RİSK DEĞERLENDİRMESİ

ATEX DİREKTİFLERİ - PATLAYICI ORTAMLAR
BÜYÜK ENDÜSTRİYEL KAZALARIN ÖNLENMESİ
VE ETKİLERİNİN AZALTILMASI - KANTİTATİF
RİSK DEĞERLENDİRME

SEVESO II VE SEVESO III DİREKTİFİ (COMAH DİREKTİFİ)

Özlem ÖZKILIÇ

TİSK
TÜRKİYE İŞVEREN SENDİKALARI KONFEDERASYONU

RİSK DEĞERLENDİRMESİ

ATEX DİREKTİFLERİ - PATLAYICI ORTAMLAR
BÜYÜK ENDÜSTRİYEL KAZALARIN ÖNLENMESİ VE ETKİLERİNİN AZALTILMASI - KANTİTATİF RİSK DEĞERLENDİRME

SEVESO II VE SEVESO III DİREKTİFİ (COMAH DİREKTİFİ)

Özlem ÖZKILIÇ

TİSK
TÜRKİYE İŞVEREN SENDİKALARI KONFEDERASYONU

TÜRKİYE İŞVEREN SENDİKALARI KONFEDERASYONU

15 Mayıs 2014
Yayın No: 338

Haberleşme Adresi:
TİSK
Hoşdere Cad. Reşat Nuri Sokak No: 108
Çankaya - ANKARA

Tel : (0312) 439 77 17 (Pbx)
Faks : (0312) 439 75 92-93-94
E-mail : tisk@tisk.org.tr
Web Sitesi : http://www.tisk.org.tr

ISBN: 978-605-9994-01-9

Baskı
Ajans-Türk Gazetecilik Matbaacılık İnşaat Sanayi A.Ş.
İstanbul Yolu 7. Km İnönü Mahallesi Necdet Evliyagil Sokağı No: 24 Batıkent-ANKARA
Tel: 0 312 278 08 24 • www.ajansturk.com.tr • **Email:**info@ajansturk.com.tr

İÇİNDEKİLER

SUNUŞ 9
GİRİŞ 11
1. BÖLÜM: TEHLİKE VE RİSK KAVRAMLARI
1.1. Terminoloji…….. 13
1.2. Teknoloji ve Tehlike Kavramı 14
1.3. Risk ve Belirsizlik Kavramı 16
2. BÖLÜM: GÜVENLİK KÜLTÜRÜ
2.1. Teknoloji ve Güvenlik Kültürü 23
2.2. Öğrenen Organizasyonlar 26
3. BÖLÜM: RİSK DEĞERLENDİRME METODOLOJİLERİNİN DOĞUŞU
3.1. Tarihçe 29
3.2. Emekleme Dönemi 30
3.3. Güvenilirlikle İlgili Doktrinlerin Oluşumu 32
3.4. Olasılık Kuramlarının Oluşumu 33
3.5. Nükleer Tesisler İçin Çalışmaların Artışı 34
3.6. Tüm Endüstriler İçin Disiplinlerin Oluşturulması 36
4. BÖLÜM: ÜLKEMİZDEKİ MEVZUAT
4.1. Risk Değerlendirme Yaptırma Yükümlülüğü 39
4.2. Dokümantasyon 41
4.3. Risk Değerlendirmesinin Yenilenmesi 42
4.4. Risk Değerlendirmesi Ekibi 42
4.5. Risk Değerlendirmesi Aşamaları 43
4.6. Büyük Kaza Önleme Politika Belgesi veya Güvenlik Raporu Hazırlanması Gereken İşyerlerinde Risk Değerlendirmesi 47
5. BÖLÜM: TEKNOLOJİK RİSK KAVRAMI
5.1. Kaza Modelleri ve Teknolojik Risk Arasındaki İlişki 50
5.2. Kritik Sistemler ve Güvenilirlik Kavramı 54
6. BÖLÜM: GÜVENİLİRLİK TEORİSİ
6.1. Güvenilirlik 59
6.2. MTTF, MTTR, MTBF ve Kullanılabilirlik 65

7. BÖLÜM: RİSK YÖNETİM KAVRAMI

7.1. Risk Yönetim Süreci 74

7.1.1. Yetki ve Sorumluluklar 74

7.1.2. Risk Yönetim Prosesi (Risk Management Prosses –RMP) 76

7.1.3. Kimyasallarla Çalışmada Meslek Hastalığı Risk Yönetim Prosesi 90

8. BÖLÜM: RİSK DEĞERLENDİRMESİ MEDOLOJİLERİNİN SEÇİM KRİTERLERİ

8.1. Kaynakların Kullanılabilirliği 99

8.2. Belirsizliğin Niteliği ve Düzeyi 99

8.3. Güçlük Düzeyi.....99

8.4. Kullanım Süresi Evreleri Boyunca Risk Değerlendirmesinin Uygulanması 100

9. BÖLÜM: RİSK DEĞERLENDİRMESİ UYGULAMA ADIMLARI

9.1. Kapsamı Oluşturma (Tehlike Kaynakları ve Tehlikelerin Tanımlanması) 103

9.2. Risk Değerlendirmesi 105

9.3. Risk Analizi.....105

9.4. Olasılık Tayini veya Hesaplaması.....109

9.5. Risk Değerleme (Kabul Edilebilirlik Kriterini Belirleme) 110

9.6. Sonuç Analizi 117

9.7. Risk Müdahalesi (Kontrol Önlemlerinin Belirlenmesi) 120

9.8. Belgelendirme 122

9.9. İzleme ve Gözden Geçirme (Güncelleme) 124

10. BÖLÜM: RİSK DEĞERLENDİRME METODOLOJİLERİNİN SINIFLANDIRILMASI 125

11. BÖLÜM: RİSK DEĞERLENDİRME METODOLOJİLERİNİN İNCELENMESİ

11.1. Beyin Fırtınası Tekniği (Brainstorming) 143

11.2. Yapılandırılmış veya Yarı Yapılandırılmış Görüşmeler (Structured or semi-structured interviews) 146

11.3. Delphi Tekniği (Delphi Technique).....148
11.4. Ön Tehlike Analizi (Preliminary Hazard Analysis – PHA) 149
11.5. İş Güvenlik Analizi – JSA (Job Safety Analysis) 164
11.6. Çeklist Kullanılarak Birincil Risk Analizi
-(Preliminary Risk Analysis (PRA) Using Checklists) 172
11.7. Güvenlik Denetimi (Safety Audit) 179
11.8. Risk Matrisleri (L Tipi Matrisler) 182
11.9. Makine Risk Değerlendirme (Machine Risk Asessment).....195
11.9.1. Makine Risk Değerlendirmesi Nasıl Yapılmalı? 199
11.9.2. Makine Sınırlarının Tayini 199
11.9.3. Tehlikenin Tanımlanması 199
11.9.4. Risk Tahmini 200
11.9.5. Makinenin Kategorisinin Bulunması 204
11.9.6. Her Parçanın Tehlikeli Hata Yapma Ortalama Zamanı (Mean Time to Dangerous Failure of Each Channel - $MTTF_d$) 206
11.9.7. B_{10d}'den Hareketle, Komponentler (Parçalar) İçin $MTTF_d$'in Hesaplanması 206
11.9.8. Hata Tespit Kapsamı (Diagnostic Coverage –DC).....207
11.9.9. Ortalama DC'nin Tahmin Edilmesi 208
11.9.10. Donanımın Güvenirliği Yoluyla Tehlikelere Maruz Kalmanın Sınırlanması 208
11.9.11. Koruyucuların ve Güvenlik Tertibatlarının Seçimi.....209
11.9.12. Kontrol Önlemi 211

11.10. Tehlike Analizi ve Kritik Kontrol Noktaları (Hazard Analysis and Critical Control Points - HACCP) 212
11.11. ……Olursa Ne Olur? (What If..? SWIFT Tekniği) 214
11.12. Tehlike ve İşletilebilme Çalışması Metodolojisi (Hazard and Operability Studies- HAZOP) 219
11.13. Tehlike Sınıflandırma ve Derecelendirme 230
11.13.1. Güvenlik Ölçümleme Sistemi (SIS) – Güvenlik Bütünlük Derecesi (SIL) 232
11.13.2. Risk Grafiği ile SIL; (IEC 61508) 233
11.13.3. Kantitatif Analiz 239
11.13.4. Kollektif Zorunlu Seçim 240
11.13.5. Kontrol Önlemleri Önerilmesi 242
11.13.6. Aynı Prosedürün Prosesin Diğer Ekipmanlarına Uygulanması 242
11.14. İş Etki Analizi (Business Impact Analysis -BIA) 242
11.15. Kök Neden Analizi (Root Cause Analysis -RCA) 245
11.16. Hata Ağacı Analizi (Fault Tree Analysis-FTA) 247
11.16.1. Ağaç Yapısı ve Semboller 252
11.16.2. FTA Diyagramının Yapılandırılması 253
11.16.3. Kantitatif Analiz 255
11.16.4. Güvenirlik ve Hata Olasılık Bağlantıları 255
11.16.5. Boolean Matematiği 258
11.16.6. Mantık Matematiğinde İşlem Basitleştirilmesi 259
11.16.7. "Azaltılmış" Hata Ağacı- Mantık Eşiti Hata Ağacı 264
11.17. Hata Modu ve Etkileri Analizi (Failure Mode and Effects Analysis- Failure Mode and Critically Effects Analysis- FMEA/FMECA) 272
11.18. Neden – Sonuç Analizi (Cause-Consequence Analysis) 286
11.18.1. Olay Ağacından Hata Ağacına Transformasyon 295
11.19. Neden – Sonuç Analizi (Cause-Consequence Analysis) 295
11.20. Neden ve Etki Analizi (Cause and Effect Analysis) 302
11.21. Senaryo Analizi (Scenario Analysis) 305

11.22. Koruma Katmanları Analizi (Layers of Protection Analysis - LOPA) 307
11.23. Karar Ağacı Analizi (Decision Tree Analysis) 312
11.24. İnsan Güvenilirlik Değerlendirmesi (Human Reliability Assessment - HRA) 314
11.25. Papyon Analizi (Bow - Tie Analysis) 319
11.25.1. Kantitatif Risk Tahmini 320
11.25.2. Güvenlik Fonksiyonlarının Karakteristikleri 322
11.26. Güvenilirlik Merkezli Bakım (Reliability Centred Maintenance - RCM) 324
11.27. Gizlilik Analizi (Sneak Analysis -SA) ve Gizlilik Devre Analizi (Sneak Circuit Analysis -SCI) 328
11.28. Markov Analizi (Markov Analysis) 330
11.29. Monte Carlo Simülasyonu (Monte Carlo Simulation) 333
11.30. Bayes İstatistiği ve Bayes Ağları (Bayesian Statistics and Bayes Nets) 335
11.30.1. Bayesgil Çıkarsama (Bayesian Inference) 337
11.30.2. Bayes Ağları 338
11.31. F-N Eğrileri (F-N Curves) 341
11.32. Maliyet/Fayda Analizi (Cost/Benefit Analysis- CBA) 343
11.33. Çok Kriterli Karar Analizi (Multi - Criteria Decision Analysis - MCDA) 346
11.34. Risk Endeksleri (Risk Indices) 347
11.35. Toksikolojik Risk Değerlendirme- Kimyasal Mauziyet Risk Değerlendirme (Toxicity Risk Assessment- Chemical Exposure Risk Assessment) 349

12. BÖLÜM: PATLAYICI ORTAMLAR- ATEX DİREKTİFLERİ

12.1. Patlayıcı Ortam Sınıflaması İle İlgili Standartlar ve Hukuki Düzenlemeler 353
12.2. Patlayıcı Ortam Sınıflandırma ve Patlayıcı Ortam Risk Değerlendirmesi 358
12.3. NEC 50, NFPA Kodlarına Göre Alan Sınıflandırması 359
12.4. EN 60079 Patlayıcı Gaz Ortamlarında Tehlikelerin Sınıflandırılması 360

12.5. TC31/W09 - Güvenlik Bütünlük Derecelendirme - SIL(Safety Integrity Level) 362
12.6. Yangın ve Patlama İndeksleri 363
12.6.1. Dow F&EI ve Mond F&ETI 365
12.6.2. Temel Emniyet İndeksi (Inherent Safety Index -ISI) ve Entegre Temel Emniyet İndeksi (Integrated Inherent Safety Index -I2SI) 376
12.6.3. Çevre Sağlık ve Emniyet İndeksi – Environment Health &Safety Index (EHS) 379
13. BÖLÜM: BÜYÜK ENDÜSTRİYEL KAZALARIN KONTROLÜ HAKKINDA YÖNETMELİK GEREĞİNCE RİSK DEĞERLENDİRMESİ METODOLOJİ: ARAMIS PROJESİ
13.1. SEVESO III Direktifi 387
13.2. ARAMIS Projesi Nedir? 389
13.3. SEVESO Kuruluşlarında Büyük Kaza Senaryolarının Tanımlanması....392
13.4. Büyük Çaplı Kaza Tehlikelerinin Tanımlanması (MIMAH) 392
13.4.1. MIMAH'ın Adımları....394
13.4.2. Ekipman Tipolojisi 395
13.4.3. Madde Tipolojisi 396
13.4.4. Tehlikeli Ekipmanın Seçimi 397
13.4.5. Bow-Tie (Papyon) Yaklaşımı 398
13.4.6. MIMAH Metodolojisi'nde Matrislerin Kullanımı 399
13.4.7. Hata Ağacının Oluşturulması 402
13.5. Referans Kaza Senaryolarının Belirlenmesi Metodolojisi (MIRAS) 403
13.5.1. MIRAS'ın Amaçları ve Temel Adımları....405
13.5.2. Olay Ağaçlarında Geçiş Olasılıklarının Değerlendirilmesi 408
13.5.3. Olay Ağacındaki Güvenlik Bariyerlerinin Etkileri 409
13.5.4. Risk Şiddeti Değerlendirmesi ve Haritalandırması....410
13.6. Maruziyetlerin Değerlendirilmesi 411
KAYNAKÇA 413

SUNUŞ

İş kazaları ve meslek hastalıklarının önlenmesinde işyerindeki risk faktörlerinin tespiti büyük önem taşımaktadır. Risk faktörlerinin tespiti ve söz konusu risklerin ortadan kaldırılmasına yönelik risk değerlendirmesi faaliyeti günümüzde iş sağlığı ve güvenliğinin en öncelikli konularından birini teşkil etmektedir.

4857 sayılı İş Kanunu'nun 2003 yılında yürürlüğe girmesinin ardından iş sağlığı ve güvenliği alanında önleyici yaklaşım benimsenmiş ve özellikle İş Kanunu kapsamındaki yönetmeliklerde risk değerlendirmesi hakkında düzenlemelere yer verilmiştir. Ancak 2003 ile 2012 yılları arasında risk değerlendirmesi alanında yeterli düzeyde bilgilendirme faaliyeti yapılamamıştır.

Uygulamadaki bilgi eksikliğini gidermek üzere, Konfederasyonumuz 2005 yılında Sayın Özlem Özkılıç'ın "İş Sağlığı ve Güvenliği Yönetim Sistemleri ve Risk Değerlendirme Metodolojileri" başlıklı eserini yayınlamıştır. Anılan eser, iş sağlığı ve güvenliği alanında halen Türkiye'de en önemli kaynaklardan biri olma niteliğini sürdürmektedir.

6331 sayılı İş Sağlığı ve Güvenliği Kanunu'nun yürürlüğe girmesi ile risk değerlendirmesi ayrıntılı bir yasal düzenlemeye kavuşmuştur. Bu kapsamda işverenler, iş sağlığı ve güvenliği yönünden risk değerlendirmesi yapmak veya yaptırmakla yükümlü tutulmuştur. Ancak uygulamada risk değerlendirmesi süreçleri hakkındaki kaynakların yetersizliği nedeniyle bu yükümlülüğün yerine getirilmesinde büyük güçlükler yaşanmaktadır.

Sayın Özlem Özkılıç'ın uzun yıllara dayanan tecrübesiyle hazırladığı risk değerlendirmesi alanındaki yeni yapıtının Türkiye'de iş sağlığı ve güvenliğinin gelişimine büyük katkı sağlayacağını düşünüyoruz.

Yayınımızın uygulamacılar, akademisyenler ve konuya ilgi duyan herkes için yararlı olmasını dileriz.

Saygılarımızla,

TÜRKİYE İŞVEREN SENDİKALARI KONFEDERASYONU

Teşekkür

Kitabımı hazırlamam için bana destek veren ve yüreklendiren eşim, annem ve kızlarıma sonsuz sevgi ve teşekkürlerimle.

Bu kitabın yayınlanmasında verdikleri destek ve katkılarından dolayı TİSK'e ve Sayın Genel Sekreter Bülent PİRLER ile Sayın Emel ÇOPUR'a saygı ve teşekkürlerimle.

Son olarak yine bu kitabımı da, yayınlanmasından büyük mutluluk duyacağına inandığım sevgili babamın anısına adıyorum.

Dr. Özlem ÖZKILIÇ

Kimya Yük. Müh.

ÇSGB-Emekli İş Başmüfettişi

E. İş Teftiş Kurulu İstanbul Grup Bşk. Yrd.

A. Sınıfı İş Güvenliği Uzmanı

Ocak 2014

GİRİŞ

İş sağlığı ve güvenliği son yıllarda Avrupa Birliği'nin de en çok yoğunlaştığı ve önem verdiği sosyal politika konularından birisi olmuştur. Avrupa Komisyonunun belirlediği yeni iş sağlığı ve güvenliği stratejisi, "çalışma hayatındaki değişimleri ve başta psiko-sosyal konularda olmak üzere yeni risklerin ortaya çıkması durumunu göz önünde bulundurarak global bir iş sağlığı ve güvenliği yaklaşımı" nı benimsemektedir. Tüm yeni yaklaşım direktiflerinin ekinde bulunan "Temel Sağlık ve Güvenlik Gerekleri", Avrupa Birliği ülkelerinde, 80'li yılların ikinci yarısından itibaren iş sağlığı ve güvenliği mevzuatı içerisinde yer alan risk analizi ve risk değerlendirmesi kavramları ile de yakından ilgili bulunmaktadır. Esasen, Avrupa Birliği hukukunda, iş sağlığı ve güvenliği ile ilgili olarak iki alan söz konusudur. Bunlar; ürün güvenliği ve işletme güvenliği'dir.

Yasalar ve yönetmelikler çalışma ve güvenlik şartlarına ilişkin sorumlulukları tanımlar. Ülkeler arasında yasal mevzuat ve bunun uygulanması konusunda birçok farklılıklar bulunmaktadır. Ancak bunların tümünde sistematik güvenlik çalışması yapılması tezi savunulmaktadır. Mevzuatlardaki ortak konular aşağıda verilmiştir:

- İşveren işyerinde sağlıklı ve güvenli bir çalışma ortamı sağlamakla yükümlüdür,
- İşyerindeki sağlık, güvenlik ve çevre yönetimi yeterli seviyede düzenlenmiş olmalıdır,
- Çalışanlar tehlikeler ve güvenli çalışma konusunda bilgilendirilmelidir,
- Tehlikeler tanımlanmalı ve değerlendirilmeli, gerekiyorsa azaltılmalı veya ortadan kaldırılmalıdır.

Mevzuatlarda yer alan güvenliğe dair çalışmalar ise "Risk Değerlendirmesi" yapılması vasıtası ile risklerin sistematik ve belgelenerek değerlendirilmesi şeklinde istenmektedir. Birçok farklı ülkenin mevzuatında "risk değerlendirmesi" terimi sıklıkla kullanılmakta, işverenlere yükümlülük olarak verilmekte ve risk değerlendirme tekniklerinin kullanımı giderek yaygınlaşmaktadır.

Fakat risk analizi isteyen daha detaylı mevzuatlar da bulunmaktadır. Bunlardan birisi AB'ne üye ülkelerin milli mevzuatlarına aktardıkları işyerinde makine kullanımını düzenleyen 2006/42/EEC sayılı AB Direktifidir. Bunun direktifin uygulanması, AB standartları tarafından desteklenmektedir.(IEC EN 12100, EN 13849 vb.). Tehlikeli kimyasallarla büyük endüstriyel kazaların meydana gelebileceği işyerlerinde risk yönetimi ve daha ciddi risk değerlendirmelerinin resmi olarak talep edilmesi eğilimi yüksektir. Avrupa'da, bu konular 1992

yılında değiştirilen 1982 tarihli Seveso Direktifi ile, ABD'de Temiz Hava Yasası (Çevre Kirliliği Ajansı (EPA),1990) ile düzenlenmiştir. Diğer tipteki sanayi kuruluşlarında, örneğin nükleer güç üreten ve açık deniz işletmelerinde sistematik güvenlik analizi şartları bulunmaktadır.

İlgili tarafların en önemlisi; alınan güvenlik önlemlerinin yetersiz kalması durumunda kazaya uğraması muhtemel tehlike kaynağına yakın çalışanlardır. İşletme içerisinde iyi ugulanmış bir risk değerlendirmesi, güvenlik problemlerini ortadan kaldırır, işyerindeki güven hissini ve güvenliği geliştirir. Bu türde bir analiz için önerilen çalışan temsilcilerinin de katılımını sağlamaktır. Bu analizi geliştirir, çalışanların tecrübelerinin dahil olmasını sağlar ve analizin şeffaflığını arttırır.

İşyerlerinde risklerle mücadele yöneticiler, tasarımcılar ve güvenlik uzmanları gibi çeşitli alanlardan kişilerin katılımını gerektirir. Ancak işyerlerinde sağlık ve güvenlik konusunda ana sorumluluk işverene aittir. Sorumlulukların detayları ülkeden ülkeye farklılık gösterir, fakat işverenin sorumluluğu prensibi genellikle geçerlidir. Bu sorumlulukların yerine getirilmesi için ve işyerinde güvenliğin sağlanması için birçok durumda risk değerlendirmesi etkin bir yöntemdir. Analiz sonuçlarının kayıtları, işyeri güvenliğinin yasal ve yeterli seviyede sağlandığını göstermek için kullanılır. Risk değerlendirme uygulamalarının faydalarını özet olarak sıralayacak olursak;

- İşletmede daha az kaza yaşanması,
- Kaza oluşumuna neden olabilecek faktörlerin sistematik olarak belirlenmesi ve yok edilmesi,
- Tasarım sırasında sistematik analizle hataların ve problemlerin etkin şekilde belirlenmesi, bu tip problemlerin önlenmesi ve sonradan çıkacak daha büyük maliyetlerden kurtulma,
- Büyük kaza ve yangın vb. meydana gelme olasılığının azaltılması (eğer analiz bunu amaçlamış ise), finansal olarak da daha düşük sigorta primleri.

Bu kitap özelikle risk değerlendirme kavramına yabancı olan ilk defa tanışacak olan iş sağlığı ve güvenliği mühendis ve teknik elemanları ile bu konuda oldukça bilgi birikimine sahip olan teknik elemanların ve işyeri hekimlerinin tümünün yararlanabileceği bir kaynak olması düşünülerek hazırlanmıştır.

Bu nedenledir ki bu kitapta risk değerlendirme yöntemlerinin güçlü ve zayıf yanları irdelenmiş, güvenilirlik teoremlerinin tarihçesinden başlamak üzere bir çok bilgi derlenmiştir. Tüm iş güvenliği mühendisleri ile işyeri hekimlerine bu kitabın çalışmalarında yararlı bir kaynak olmasını tüm kalbimle dilerim.

1. BÖLÜM: TEHLİKE VE RİSK KAVRAMLARI

1.1. Terminoloji

Gerek ulusal, gerek ise uluslararası düzeylerde terminoloji standardizasyonu, aynı ifade ile aynı şeyi anlamak için olmazsa olmaz koşuldur. Bir yandan global düzeyde terminoloji standardizasyonu çalışmaları devam ederken, sektör ve alanlardaki gelişmeler, yeni terimlerin ortaya çıkmasına ya da eski terimlerin farklı anlam kazanmalarına yol açtığından bir çok bilim dalında sorunun süregelmesine neden olabilmektedir.

Ülkemizde iş sağlığı ve güvenliği mevzuatı çerçevesinde getirilen en büyük ve en önemli yenilik, işverenlerin işyerlerinde risk değerlendirmesi yapması ve alınan sonuçlara göre gerekli sağlık ve güvenlik önlemlerinin belirlenmesi zorunluluğudur. Özellikle 89/391 sayılı Konsey Direktifi İş Sağlığı ve Güvenliği Yönetmeliği olarak 2003 yılında yayınlanmış, ancak Danıştay 10. Dairesi İş Sağlığı ve Güvenliği Yönetmeliği'nin yürütmesini 2004/1942 esas nolu ve 24 Mayıs 2004 tarihli kararı ile durdurmuştur.

89/391 sayılı Konsey Direktifi çerçeve direktiftir ve bu direktif daha sonradan Çalışma ve Sosyal Güvenlik Bakanlığı tarafından İş Sağlığı ve Güvenliği Kanunu Taslağı olarak hazırlanmıştır. 6631 sayılı İş Sağlığı ve Güvenliği Kanunu'nun yürülüğe girmesi ile işyerlerinde risk değerlendirme yükümlülüğünün yeniden getirilmiş olmasıyla birlikte, daha önce iş sağlığı ve güvenliği çalışmalarında etkin olarak uygulanmayan risk değerlendirmesi konusunda terminolojik olarak tanım ve kavramlarda kargaşa da yaşanmaya başlanmıştır.

Her ne kadar 29 Aralık 2012 tarih ve 28512 sayılı İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği'nin 4. maddesinde risk ve tehlike tanımı verilmiş olsa da kavram kargaşası halen devam etmektedir.

Kaynak farklılığı ya da sektörlerdeki konum farklılığı (işveren/ çalışan/ müfettiş/ mühendis/ akademisyen/ basın/ toplum), terminolojide farklılığa ya da aynı terimde farklı algılamalara yol açabilmektedir.

Standartlar kurumsal, askeri, ulusal hatta uluslararası ölçeklerde geçerliliğe sahip uygulamaları kapsamaktadırlar. Teknik terimleri kapsayan standartlarda kavramlar arasındaki uyumu sağlamak ve iletişimi kolaylaştırmak ise temel hedeftir. Bu nedenle, uluslararası standartların "Türkçe"ye çevirisinde kullanılan kelimelerin seçimine büyük bir özen gösterilmelidir. Özellikle, çok büyük bir hızla gelişen iş sağlığı ve güvenliğini ilgilendiren standartlarda dil birliğinin sağlanması, standartların "Türkçe"leştirilmesinde büyük önem arz etmektedir.

Standartlaştırma faaliyetleri ulusal, askeri ve kurumsal olmak üzere geniş ölçeklerde geçerliliğe sahip uygulamaların bütününü sağlamaktadır. Standardizasyon çalışmalarının temel amaçlarından en önemlisi varolan tipik özelliklerin her bir birey tarafından aynı anlamda kavranılmasını sağlamaktır. Bu amaçla, yaygın uygulama alanına sahip olan standartlar geliştirilirken özellikle ulusal olan standardizasyon çalışmalarında seçilen kelimeler her kişi tarafından aynı şekilde anlaşılabilecek ve kavranılabilecek bir şekilde oluşturulmalıdır.

1.2. Teknoloji ve Tehlike Kavramı

Teknoloji, insanın bilimi kullanarak doğaya üstünlük kurmak için tasarladığı rasyonel bir disiplin olarak tanımlanmaktadır. Ünlü bir eğitim teknoloğu olan James Finn (1972) teknolojiyi tanımlarken şöyle demektedir: "Teknoloji; sistemler, işlemler, yönetim ve kontrol mekanizmalarıyla hem insandan hem de eşyadan kaynaklanan sorunlara, bu sorunların zorluk derecesine, teknik çözüm olasılıklarına ve ekonomik değerlerine uygun çözüm üretebilmek için bir bakış açısıdır".

İş kazaları ve meslek hastalıklarının oluşmasında teknolojideki hızlı gelişim, makineleşme, işyerlerindeki fiziksel ve kimyasal etmenler ile üretimde kullanılan ham ve yardımcı maddelerin yanında ekonomik, sosyolojik, psikolojik, fizyolojik ve ergonomik bir çok etken rol oynamaktadır. Özellikle sanayi devrimi sonrasında teknolojik gelişmeler sonucunda üretimin yapısı oldukça karmaşıklaşmış, hızlı ve kontrolsüz sanayileşme süreci ve üretimin giderek yoğunlaşması iş kazaları ve meslek hastalıkları ile çevre kirliliği gibi sorunların önemli boyutlara ulaşmasına neden olmuştur.

Son yıllarda risk kelimesi ve risk süreci konusunda önemli çalışmalar yapılmasına karşın konu ile ilgili tanımlarda bir dil birliği sağlanamamıştır. Risk ile ilgili süreçlerin tanımını yapabilmek için riskin tanımlanması; riskin tanımını yapabilmek için de tehlike (hazard) ve zarar (harm) tanımlarının bilinmesi gerekmektedir.

Teknolojinin gelişmesine bağlı olarak tehlike kavramı da çeşitli kaynaklarda bir çok tanıma sahip olmuştur. Tehlike kavramının anlamına Türk Dil Kurumu ve Büyük Larousse Sözlük ve Ansiklopedisinden baktığımızda şu tanımlamalarla karşılaşırız;

Tehlike, büyük zarar veya yok olmaya yol açabilecek durum ya da gerçekleşme ihtimali bulunan fakat istenmeyen durumdur, diğer bir ifadeyle bir tehdit

oluşturan bir şeyin bir kimsenin varlığını ya da durumunu tehdit eden ya da kaygı uyandıran şey, çekincedir.

Dünya Sağlık Örgütü (WHO) ise tehlikeyi 1950 yılında; bir nesne ya da belli koşulların, etkenlerin insan sağlığı ve çevre için olumsuzluk içermesi şeklinde tanımlamıştır. Uluslararası Çalışma Örgütü, ILO'nun 1991 yılında yanınlanan "Büyük Endüstriyel Kazaların Önlenmesi Uygulama Kodu"nda ise canlıları çevreyi ve/veya malı, tesisleri tehdit eden, kapsamı belirlenmemiş kaza ve zarar potansiyeli olarak verilmiştir.

ISO/IEC Guide 51 (1999)'da tehlike "potansiyel zarar kaynağı olarak", zarar ise "sağlık veya varlığa gelebilecek fiziksel yaralanma ve/veya ziyan" olarak tanımlamıştır. IMO'nun Deniz Güvenliği Komitesi (MSC -Maritime Safety Committee) (2002)'nin MSC/CIRC 1023 rehberine göre; "Tehlike; insan hayatına, sağlığına, malına veya çevreye karşı olası tehditler" olarak tanımlanmaktadır.

Risk Yönetimi - Terimler ve Tarifler standartı ISO Rehber 73: 2012'ye göre tehlike, "muhtemel zarar kaynağıdır.Tehlike bir risk kaynağı olabilir".

Güvenililirlik Yönetimi ve Teknolojik Sistemlerin Risk Analizi standartı, ISO IEC 60300-3-9'da öncelikle "Zarar" tanımı verilmiştir. Standarta göre zarar; fizikî hasar veya sağlığa, mala veya çevreye olan hasardır. Tehlike ise; muhtemelel zarar kaynağı veya zarar oluşturma ihtimali bulunan bir durumdur. Standartta ayrıca "Tehlikeli Olay" tanımı da verilmiştir, buna göre tehlikeli olay; tehlikeye neden olabilecek bir olaydır. Standartta tehlikenin belirlenmesi ise, bir tehlikenin var olduğunun kabullenilmesi ve onun özelliklerinin tarif edilmesi süreci olarak verilmiştir.

Fitzpatrick ve Bonnefoy (1999)'a göre zarar ise, tehlikenin denetlenmemesi durumunda ortaya çıkan fiziksel, işlevsel ya da maddi hasar durumu olarak tarif edilmiştir.

Yine literatür araştırması yapıldığında afet bilimciler Gigliotti ve Jason (1991) tarafından tehlike; doğal veya insan eliyle oluşturulmuş çevrede, insanların hayatlarını, sosyal ve ekonomik faaliyetlerini, mal ve hizmetlerini önemli ölçüde etkileyebilecek en olumsuz ve nadir olaylar olarak tanımlanmaktadır.

OHSAS 18001'in 1999 versiyonunda tehlike; insan yaralanması ya da hastalığı, malın hasar görmesi, işyeri çevresinin zarar görmesi ya da bunların kombinasyonuna neden olabilecek potansiyel bir durum ya da kaynak şeklinde tanımlanmışken bu tanım OHSAS 18001 – 2007 versiyonunda, insan yaralan-

ması ya da hastalığına neden olabilecek kaynak, faaliyet veya durum şeklinde verilmiştir. Görüldüğü üzere yeni tanımda malın hasar görmesi tehlike kavramı içerisine alınmamıştır.

Duru ve Besbelli (1997) ise tehlikeyi, bir nesne ya da olgunun kendi yapısında olan ve etkileme koşullarında insan ya da çevreye zarar oluşturma olasılığı olarak vermişlerdir.

6331 sayılı İş Sağlığı ve Güvenliği Kanunumuz ile İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği'ne baktığımızda ise tehlike, işyerinde var olan ya da dışarıdan gelebilecek, çalışanı veya işyerini etkileyebilecek zarar veya hasar verme potansiyeli olarak tarif edilmiştir.

1.3. Risk ve Belirsizlik Kavramı

Risk kelimesi aslında Çin orjinli bir kelimedir ve diğer dillere de çinceden geçmiştir. Aslında Çince'de "Risk" kelimesini ifade eden ideogram, "tehlike" ve "fırsat" ideogramlarının birleşkesidir. Yani Çincede risk denildiği zaman iki farklı unsur birden anlaşılır. Bu unsurların birincisi "gelecekte oluşma ihtimali" bir diğeri ise "fırsat ve tehdit"dir. Diğer tüm terminolojilerde "Risk" denilince yaygın olarak tehdit anlaşılmaktadır. Oysa risk kavramının çıkış yeri olan Çin'de "Risk", meydana getirdiğimiz çalışmalar esnasında gelecekte meydana gelebilecek olan ve amaçlarımızın gerçekleştirmesini engelleyebilecek tehditler/olumsuzluklar veya amaçlara ulaşmayı kolaylaştırabilecek fırsatlar olarak tanımlanmaktadır.

Fransızca'da risk (risque) sözcüğü olası olaylara ilişkin olup çoğunlukla olumsuz anlamlar içerir. Eski İtalyanca'da risicare olarak kullanılan risk, cesaret etmek, meydan okumak anlamındadır. Bu tanıma göre risk, kaderden ziyade bir tercihtir.

Lay and Strasser (1987)'e göre risk, hedeflenen bir sonuca ulaşamama olasılığı ya da istenmeyen bir olayın oluşma olasılığıdır ve belirsizlikler potansiyel risk kaynaklarıdır. Proje Yönetim Enstitüsünde yıllarca çalışmış olan Brehmer (1994) ise riski, ortaya çıktığında proje hedeflerini olumlu veya olumsuz etkileyecek olaylar ve şartlar olarak tanımlamıştır. Yine Brehmer'e göre; hedeflenen bir sonuca ulaşamama olasılığı ya da istenmeyen bir olayın oluşma olasılığı ve oluşması durumunda yaratacağı sonucun şiddetinin bir fonksiyonu olarak tanımlanan risk karmaşık bir kavramdır.

Risk analizi disiplininde önemli bir yere sahip olan Morgan (1993) riski; tehlikeyle karşılaşanlarca daha önceden tanınmayan ve gözlenemeyen, bilimin

yeterince tanımadığı, yeni ve etkileri geç ortaya çıkabilecek şey olarak tanımlamıştır. Yine "Risk" kelimesini tanımlarken, tehlikelerin insanlar tarafından gözlenmesi ve bilinmesi zorunlu değildir demektedir. Eğer bir yerde risk varsa bunun bilinmemesinin meydana gelecek olası zararı ve hasarları ne sınırlayacağını ne de ortadan kaldıracağını iddia etmektedir. Riskin denetlenemezliği nedeniyle korkutucu, dünya çapında felaket yaratıcı, sonuçları öldürücü, hukuka uygun olmayan, kolayca azaltılamayan ve gelecek kuşaklar için çok tehlikeli potansiyel olaylar olarak açıklamış ve riskin içerdiği tehlikeyi ikiye ayırmıştır, bunlardan ilki tehlikeyle karşılaşma, ikincisi ise sonuçtur.

Morgan'a göre "Risk", her olayın doğasında olan bir durum olarak kabul görmekte ve gelecekte ortaya çıkabilecek olayları analiz ederek potansiyel riskleri belirlemek ve yönetmek için ölçülebilir kavramlar haline getirilmeye çalışılmaktadır. Belirsizlik, risk oluşma olasılığının bir ölçüsünü verir, belirsizlik arttıkça riskin oluşma olasılığı artar. Belirsizliğin negatif bileşeni risk, pozitif bileşeni de fırsat içerir. Hedeflenen bir sonuca ulaşamama olasılığı veya istenmeyen bir olayın oluşma olasılığı ve oluşması durumunda yaratacağı sonucun şiddeti olarak ifade edilen risk, karmaşık bir kavramdır.

Yine Morgan'a göre risk ve belirsizlik kavramları sıklıkla birbirine karıştırılmaktadır, ancak bu iki kavram aynı şeyi ifade etmemektedir. Risk; çoğu zaman istenmeyen bir olayın oluşma olasılığına ilişkin istatistiksel verilere dayalı olarak ölçülebilen bir kavramdır. Morgan; riskle karşılaşma ve sonuç çalışmalarının (kadroları ve uzmanları yeterli ve yetkin ülkelerde dahi) büyük ölçüde belirsizlik içerdiğini ifade etmiştir. Belirsizlik; istatistiksel verilerin mevcut olmadığı durumlarda kullanılan, ölçülemeyen bir kavramdır. Belirsizlik bir olayın oluşma olasılığının verilerle belirlenemediği durumları ifade eder. Risk, bilinen olasılık dağılımından ya da mevcut verilerden yararlanarak belirlenebilen ve ölçülebilen olayları ifade eder. Karar verme ortamındaki belirsizliğin fazla olması, daha fazla risk almayı gerektirir. Deneyimsizlik ve geçmiş verilerin bulunmaması ise belirsizliği artırır. Birçok durumda risk istatistiksel olarak çok iyi bilinmesine rağmen, olaylar tek tek ele alındığında riskin belirsizleşmekte olduğunu ve henüz çok yeni olan ya da kötü sonuçların nadiren görüldüğü teknolojilerdeki risk hesaplamalarının daha da belirsiz sonuçlar içerdiğini iddia etmiştir.

Okuyama ve Chang (2004), Coburn ve Spence (1992) ise genel anlamda riski, herhangi bir tehlikenin meydana gelme olasılığı ile bu tehlikenin neden olacağı sonuçların bileşkesi olarak tarif etmektedirler. Başka bir deyişle risk

düzeyinin, tehlikenin büyüklüğü ve etkilenen elemanların savunmasızlığıyla orantılı olduğunu ifade etmektedirler.

Kerzner (1998), insanların bir kısmı günlük yaşamlarında ve işlerinde risk alırken, bir kısmı da riskten kaçınma yolunu seçtiklerini ifade etmiştir. Bu nedenle, riskle ilgili evrensel kurallar geliştirmek zordur. Riskin başlıca üç bileşeni vardır; bir olay yani istenmeyen bir değişiklik, bu olayın ortaya çıkma olasılığı ve bu olayın ortaya çıktığında yaptığı etkidir. Yani risk kavramı tehlike ve tehdit unsurlarını da içermektedir. Bu olumsuz yönü itibariyle risk, görevin hedeflerine ulaşmayı etkileyen belirsiz olayların etkisi olarak ifade edilebilir. O halde riskin varlığı için; görevin hedefleri, belirsiz olayların varlığı ve belirsiz olayların görevin hedefleri üzerine etkisinin olması gerekmektedir.

Bir başka risk tanımını ise Andrews ve Moss (2002) yapmış ve riskin belirli bir beklenmeyen olayın, sıklığı, olasılığı ve sonucun bütünü olduğunu ifade etmişlerdir. Andrews ve Moss'un yapmış olduğu tanım Oxford Sözlüğünde yer almış ve "Risk", tehlike, kayıp, yaralanma ya da başka zararlı sonuç oluşma olasılığı olarak tanımlanmıştır.

ILO Yönetim Kurulu'nun 244. toplantısında alınan karar uyarınca hazırlanan raporda ise risk, "belli bir dönemde veya koşullar altında istenmeyen olayın ortaya çıkma olasılığı, çevre koşullarına göre sıklık ve olasılık" olarak ifade edilmiştir.

Risk Yönetimi - Terimler ve Tarifler standartı ISO Rehber 73: 2012'ye göre risk, bir olayın ve bu olayın sonucunun olasılıklarının birleşimi olarak tanımlanmaktadır. Bilgi ve diğer varlıklar, bu varlıklara yönelik tehditler, var olan sistemde bulunan korunmasızlıklar ve güvenlik sistem denetimleri mevcut riski tayin eden bileşenlerdir. Risk; hedefler hakkında belirsizliğin etkisidir. Bir etki, olumlu ve/veya olumsuz olarak, beklenenden bir sapmadır. Hedefler, (finansal, sağlık ve güvenlik, çevresel hedefler gibi) farklı hususlara sahip olabilir ve (stratejik, kuruluş çapında, proje, ürün ve süreç gibi) farklı seviyelerde uygulanabilir. Risk, genellikle muhtemel olaylara ve sonuçlarına veya bunların bir birleşimine göre karakterize edilir. Risk, genellikle bir olayın sonuçlarının ve bu olayın oluşmasına ilişkin olasılığın bir birleşimi cinsinden ifade edilir. Belirsizlik, bir olayın, sonucunun veya ihtimalinin anlaşılmasına veya bilinmesine ilişkin bilgi eksikliğinin kısmî de olabilen durumudur.

Risk Yönetimi - Prensipler ve Kılavuzlar standartı ISO 31000:2011'e göre risk; "hedefler üzerindeki belirsizlik etkisi"dir. Bir etki beklenenden bir sapma-

dır (pozitif ve/veya negatif). Hedefler farklı hususlara sahiptir (örneğin finansal, sağlık ve güvenlik, çevresel amaçlar) ve farklı seviyelerde uygulanır (örneğin stratejik, kuruluş çapında, proje, ürün ve süreç gibi). Risk genellikle muhtemel olaylar ve sonuçlara göre veya bunların bir birleşimine göre karakterize edilir. Risk genellikle bir olayın sonuçlarının (şartlardaki değişiklikler dahil) ve karşılık gelen olma ihtimalinin bir birleşimi cinsinden ifade edilir. Belirsizlik, kısmî de olsa, bir olayın, sonuçlarının veya ihtimalinin anlaşılması veya bilinmesine ilişkin bilgi eksikliği durumudur.

Güvenililirlik Yönetimi ve Teknolojik Sistemlerin Risk Analizi standartı, ISO IEC 60300-3-9'da ise risk; "belirlenen bir tehlikeli olayın sıklığının veya ihtimalinin veya oluşumunun kombinasyonu ve yol açtığı sonuçlar"dır. Risk kavramının her zaman iki elemanı vardır, bunlar: sıklık veya tehlikeli olayın oluşması ihtimali ve tehlikeli olayın yol açtığı sonuçlardır.

Cayless ve Riley (1997) ise risk için, nesne ya da olgunun bir etkileşim sonrası insan ya da çevrede can kaybı, sağlık sorunları, malzeme ve çevresel hasarlar gibi zararlı etkiler oluşturma olasılığı ve belirli bir zaman diliminde bu etkileşimin büyüklüğüdür demektedirler.

OHSAS 18001 (1999)'da ise risk; "belirlenmiş tehlikeli bir olayın oluşma olasılığı ve sonuçlarının kombinasyonu" şeklinde verilmiştir. 2007 versiyonunda ise "Tehlikeli bir olayın veya maruz kalmanın meydana gelme olasılığı ve sonuçlarının kombinasyonu" şeklinde değiştirilmiştir.

Avustralya standartı AS/NZS 4360 (1999)'a göre risk; tehlike yaratabilecek etkiye sahip bir olayın meydana gelme şansının sonuçlar ve olasılık açısından ölçülebilirliği olarak tanımlanmıştır.

AS/NZS 4804 (2001)'e göre risk ise; herhangi bir olayın potansiyel zarar meydana getirme olasılığı ve sonucudur. İki tanım arasındaki fark ise AS/NZS 4360'de risk; olabilirliği ve ölçülebilirliği ile AS/NZS 4804'de ise sonucun büyüklüğü ile anlam ifade etmektedir.

Dünya Sağlık Örgütü (WHO) 2002 yılında riski; sonucun olumsuz olma ihtimali veya bu olasılığı ortaya çıkaran faktör olarak tanımlamış ve riskin ne anlamlara gelebileceğini ifade etmeye çalışmıştır:

- Risk olasılık anlamına gelebilir,
- Risk istenmeyen sonucu ortaya çıkaran faktör anlamına gelebilir,
- Risk bir sonuç anlamına gelebilir,

- Risk potansiyel güçlük veya tehdit anlamına gelebilir.

6331 sayılı İş Sağlığı ve Güvenliği Kanunumuz ile İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği'nin 4. maddesinde risk ise; tehlikeden kaynaklanacak kayıp, yaralanma ya da başka zararlı sonuç meydana gelme ihtimali olarak tanımlanmıştır.

Görüldüğü üzere literatür araştırması ne kadar genişletilirse "Risk" ve "Tehlike" kelimelerinin anlamında da o kadar geniş bir yelpazede tanımlamalar olduğu görülmektedir.

Tehlikeyi daha belirgin bir şekilde şöyle açıklayabiliriz: İnsanın yaşam sürecinde mutlak emniyet içinde bulunması veya tehlikeden uzakta yaşaması diye bir kavramdan söz edilmesi olası değildir. Günlük yaşamlarında insanlar kendi faaliyetlerinden kaynaklanan trafik, ev kazaları, yangınlar, hastalıklar, spor faaliyetleri vb. gibi bir çok tehdit ile birlikte yaşamaktadırlar. Avcılık, dağcılık, kayak, çeşitli spor faaliyetleri ise insanların bilerek ve isteyerek yani gönüllü olarak karşılaştıkları tehlikeleri içeren faaliyetler arasında yer almaktadır.

Bu nedenle de tehlike kelimesini tanımlarken doğal veya insan eliyle oluşturulmuş bir olayın öncelikle çevreyi, insanların hayatını, sosyal ve ekonomik faaliyetlerini, mal ve hizmetlerini tehdit edici bir olaydan bahsedilmesi ve bu olayın meydana gelme olasılığından da bahsedilebiliyor olmalıdır. Yani tehlike kavramı bir anlamda olasılık da içermektedir. Örnek vericek olursak; denizde köpek balığının bulunduğunu düşünelim, eğer denizde değilseniz bu köpek balığı sizin için bir tehlike değildir. Ama bir olasılıkla denize girmeniz gerekiyorsa işte o zaman o köpek balığı sizin için tehlike oluşturuyor demektir.

Genel olarak ise tüm risk tanımlamalarında tehlike ve bu tehlikenin olabilirliğinden yani olasılığından bahsedilmektedir. Risk kavramı ile belirsizlik kavramının iç içe iki kavram olduğu konusunda ise neredeyse tüm risk analizi disiplinindeki otoritelerin hem fikir olduğunu söylebiliriz.

*Belirsizlikte mevcut olan **"bilinmezlik"** ve **"sürpriz"** şeklindeki iki boyut, risk için **"tehlike"** ve **"olasılık"** şeklindedir.*

Yaşamda sıfır risk hiçbir zaman söz konusu değildir. Her olay, her karar, atılan her adım istenmeyen bir yön, yani bir risk içermektedir. Kesinlik durumu, yalnızca karar verici tarafından kapsanan süre zarfı içinde ne olacağı kesin olarak söylenebiliyorsa mevcuttur. Belirsizlik ise bunun tersine, hiçbir tarihsel verinin veya geçmişte karar alıcı üzerinde düşünmekte olduğu, yaşanmış durum ile bağlantı taşıyan bir olayın bulunmadığı bir durum olarak tanımlanabilir.

Karar alıcı ister sezgileriyle olsun, ister akılcı yolu kullanarak olsun; belli bir olayın gerçekleşme olasılığı için bir değer belirleyebiliyorsa, alınacak kararın risk altında alındığı konusunda genel bir fikir birliği mevcuttur.

Risk, olasılık hesaplamalarında kendisine ait bir yere sahiptir ve uygun niceliksel bir ifadeyle belirtilebilir. Risk, bir ve sıfır arasında [1,0] değişen sayısal değerlerle ifade edilebilir. Bir, %100 riski, sıfır ise %0 riski gösterir. Riske sayısal olarak bir değer biçilemediği durumlarda risk, yüksek, düşük, "kabul edilebilir", "ihmal edilebilecek kadar düşük" gibi bulanık sözcüklerle tanımlanmaya çalışılır. Tüm insan etkinlikleri az ya da çok risk taşır. Bazı durumlarda söz konusu riskin ölçülebilmesi mümkün olduğu halde bu etkinliğin tamamen risksiz, yani kesinlikle güvenli olduğunu belirlemek olanaksızdır.

2. BÖLÜM: GÜVENLİK KÜLTÜRÜ

2.1. Teknoloji ve Güvenlik Kültürü

Teknoloji kelimesinin doğuş hikâyesi araştırıldığında, Yunanca sanat ve bilmek sözcüklerinin birleşiminden türediği görülür. İnsanoğlu yüzyıllar boyunca ihtiyaçlarına uygun yardımcı alet ve araçları yapmaya çalışmış ya da doğa olaylarını araştımış, bilinmeyene merak duymuş ve hep neden sorusunu sormuştur.

Her yeni icat edilen teknoloji ve bu teknolojinin kullanılması ile birlikte, çeşitli kazalar da meydana gelmeye başlamış ve teknolojik risk kavramı doğmuştur. Bilim her ne kadar insanlığın refah ve gelişmesi açısından çok hizmet etmişse de aynı zamanda insanoğluna, çevreye ve topluma karşı çeşitli tehlikeleri de beraberinde getirmiştir.

İşyerinde gerçekleşen kazaların çoğunluğunun teknik etkenlerin yanısıra, yapılan veya yapılmayan davranışlar açısından insan etkenine dayandığı çoğunluk tarafından kabul görmektedir. İşte bu aşamada kültür kavramı gündeme gelmektedir.

Kültür kelimesi genelde çok defa duyduğumuz, bazen kullandığımız, ama tam olarak ne anlama geldiğini etraflıca düşünmediğimiz kavramlardan biridir. Yüzlerce tanımı olmasına karşın sıkça kullanılan tanımlardan biri Kroeber ve Kluckhohn (1952) tarafından yapılmıştır. Kroeber ve Kluckhohn'a göre kültür, "İnsan gruplarının özgün yapılarını ortaya koyan, yaratılan ve aktarılan sembollerle ifade edilen düşünce, duygu ve davranış biçimleridir."

Kültürün temelini genellikle tarihsel süreçte oluşmuş olaylar veya değerler oluşturmaktadır. Teknolojinin birey ve toplum üzerindeki en önemli etkisi, insanların yaşam biçimlerine, yani kültürlerine olan etkisidir.

Çernobil reaktör kazası, 20. yüzyılın ilk büyük nükleer kazası olarak tarih sayfalarına yazılmıştır. Ukrayna'nın Kiev iline bağlı Çernobil kentindeki Nükleer Güç Reaktörünün 4. ünitesinde 26 Nisan 1986 günü erken saatlerde meydana gelen nükleer kaza sonrasında atmosfere büyük miktarda fisyon ürünleri salınmış ve 30 Nisan 1986 günü meydana gelen kaza tüm dünya tarafından öğrenilmiştir.

20. Yüzyılın en önemli nükleer kazası, Çernobil kazası çok önemli bir kavramı ortaya çıkarmıştır, Güvenlik Kültürü...

"Güvenlik Kültürü" kavramı ile kamuoyunun tanışması Çernobil kazasından sonra, 1986 yılında IAEA –Uluslararası Atom Enerjisi Kurumu'nun hazırladığı raporla olmuştur.

Ukrayna'daki Çernobil Nükleer güç santralindeki kazayı hatırlayacak olursak;

Ukrayna'daki Çernobil nükleer güç santralındaki kaza, reaktör güvenliği ile ilgili bir test sırasında gerçekleşmiştir. Reaktörlerin kararlı çalışamadığı çok düşük güç seviyesinde iken, reaktörün güvenlik sistemlerinin devreye girmemesi için,

sorumlu operatörler, normalde yapmamaları gerektiği halde acil durum kapama sistemini devre dışı bırakmışlar, deney sırasında reaktör kalp içi sıcaklıklar güvenli seviyenin üstüne çıkmış ve reaktörü kapatacak, soğutma sağlayacak sistemler devre dışında kalmıştır.

Bu affedilmez hata, buhar basıncının artmasına ve bu yüzden oluşan buhar patlamasıyla birlikte çatının çökmesine yol açmış, böylece, reaktör içindeki sıcak grafit doğrudan atmosferle temas eder hale gelmiş ve havada bulunan oksijenle reaksiyona giren grafitin yanmasıyla reaktör kalbi bütünlüğünü kaybetmiş, sonuçta radyoaktif maddeler dışarı salınmıştır.

IAEA tarafından Çernobil için hazırlanan raporda kurumun ***güvenlik kültürünün zayıflığından söz edilmiş*** ve bu kazanın nedenlerinden biri olarak gösterilmiştir.

Bu kavram ve önemi çeşitli şekillerde vurgulanmasına rağmen detaylı bir şekilde tanımlanmamış ve ölçülebilirliği üzerine araştırmalar yapılmamıştır. Ancak, IAEA 1991 yılında bu kavramı tanımlamıştır. Bu tanıma göre Güvenlik kültürü, "kurumun sağlık ve güvenlik programlarının yeterliliğine, tarzına ve uygulamadaki ısrarına karar veren birey ve grupların değer, tutum, yetkinlik ve davranış örüntülerinin bir ürünüdür." Diğer yandan, "güvenlik kültürü" üzerine yapılan tanımlamalar, ilgili boyutlar ve ölçümler bir çalışmadan diğer çalışmaya değişiklik göstermeye devam etmektedir.

Güvenlik kültürü denildiğinde literatürde birçok tanımla karşılaşılmaktadır, ancak genel olarak tanımlayacak olursak; "güvenliği veya emniyeti tehdit edebilecek davranış veya uygulamalarla bunların yer aldığı 'ortak kullanım ya da etki alanında' bulunan canlıların veya nesnelerin (örn, teçhizat, araç vb.) zararını en aza indirmeyi amaçlayan, güvenlik veya emniyete öncelik veren algılar, inançlar, tutumlar, kurallar, roller, sosyal, teknik ve politik uygulamalarla, yetkinlikler ve sorumluluk hislerinin bütünüdür" denilebilir.

Reiman ve Oedewald (2002) literatürde çalışmalardan elde edilen iyi güvenlik kültürünün kriterlerini;

- Güvenlik politikaları,
- Yönetimin güvenlik için görünür dirayeti, demokratik uygulamaları ve yetkinliği,
- Güvenlik yönelimli olumlu değerler, tutumlar ve bağlılık, zorunluluk ve sorumlulukların açık tanımı,
- Güvenlik öncelikli işlemler,
- Güvenlik ve üretim arasındaki denge,
- Yetkin çalışanlar ve eğitim,

- Yüksek motivasyon ve iş tatmini,
- Yönetim ve çalışanlar arasında karşılıklı güven ve adil yaklaşım,
- Kalite, kural ve düzenlemelerin güncellenmesi,
- Düzenli ekipman bakımı,
- Gerekli olay (örneğin; atlatılan kaza) ve küçük bile olsa kazaların rapor edilmesi ve etkin yorumu,
- Farklı kurumsal seviyelerden ve görevlilerden sağlıklı bilgi akışı,
- Uygun tasarım, yeterli kaynak ve sürekli iyileştirme,
- Otorite ile olan iş ilişkileri

ana başlıklarında toplamıştır.

Gelişmiş bir iş sağlığı güvenliği kültürü ile başarılı bir iş sağlığı güvenliği performansı arasında doğru bir orantı vardır. Gelişmiş iş sağlığı ve güvenliği kültürünü; her seviyede iş güvenliğine verilen önem, eğitimli yöneticiler ve çalışanlar, iyi aktarılmış prosedürler ve standartlar, çalışan grupları, iş birimleri ve müteahhitler arasında iyi bir işbirliği ve net bir şekilde bildirilmiş sorumlulukların belirlenmesi olarak tanımlayabiliriz. Farklı tanımlar kullanılmakla birlikte, güvenlik kültürü kavram özelliklerini "kültür" kavramının özelliklerinden ayrı düşünmemek gerekir. Kültürlerin gelişmesindeki en önemli öge ise öğrenmedir. Gelişmiş bir iş sağlığı ve güvenliği kültürünün oluşturulmasında ise öğrenmenin önemi yadsınamaz.

Bir organizasyon kapsamlı bir yönetim sistemi ve prosedürler geliştirmiş olabilir ancak bunlar her seviyede etkili şekilde uygulanmadığında veya iletilmediğinde dengesizdir ve fayda sağlamayacaktır. Ülkemizde özellikle sanayi kuruluşları incelendiğinde birçoğunda özellikle iş sağlığı ve güvenliği açısından yönetim sisteminin var olduğu ancak uygulamada çok da fayda getirmediği görülmektedir. Yönetim sistemi çerçevesinde geliştirilen iş sağlığı ve güvenliği politikaları, prosedür, standart ve talimatlar kağıt üzerinde kalmakta ve işyerindeki iş kazası ve meslek hastalıklarının önlenmesine bir katkıda bulunmamaktadır.

Her geçen gün görsel ve yazılı basında bir iş kazası haberlerine tanık olmaktayız, buna rağmen birçok işyerinde halen iş sağlığı ve güvenliği ile ilgili yapılan yatırımlar angarya olarak algılanmakta ve çoğu zaman da maaliyet getiren yatırımlar ertelenebilmekte ya da görmezden gelinmektedir. Teknolojinin getirdiği ve iş sağlığı ve güvenliği alanında iyileştirme sağlayacak birçok yatırım için ise genellikle mevzuatta bir zorunluluk olup olmadığı araştırması yapılmakta, mevzuat açısından bir zorunluluk olmaması durumunda ise ya hiç yapılmamakta ya da proje aşamasında kalmaktadır.

Hatta işyerlerinde birçok iş kazası veya meslek hastalığı meydana gelmesine rağmen, işletemelerdeki aynı tür hataların tekrarlandığı ve yapılan hatalardan

organizasyonların, yöneticilerin ve işçilerin ders almadıkları gözlenmektedir. Örneğin; işyerindeki işçilerin çoğunluğunda 87 db'in çok üzerindeki gürültüye bağlı olarak çalışanlarda duyma kaybı yaşanmasına rağmen işveren tarafından gürültünün 87 db altına düşürülmesi için yatırım yapılmasından kaçınılmakta ve sürekli olarak çalışanlar kurallara uymamakla, kulaklıklarını takmamakla suçlanmaktadır. Ya da metal sektöründe faaliyet gösteren bir işyerinde meydana gelen kazalar incelendiğinde kazalar hep preslerde meydana gelmesine rağmen işveren tarafından teknolojinin izin verdiği fotosel sistemi, kızak sistemi vb. yatırımlardan kaçınılmaktadır.

Bu aşamada sadece işverenlere de yüklenmemek gerekmektedir. Meydana gelen kazalar incelendiğinde, işveren tarafından teknolojinin izin verdiği önlemler alındığı halde insan davranışlarından kaynaklanan da birçok kaza olduğunu görmekteyiz. Yine örnek vermek gerekirse, yüksekte çalışan işçinin güvenliğini sağlamak için işveren tarafından güvenlik halatı gerilmiş ve işçiye uygun paraşüt tipi bir emniyet kemeri verildiği halde, işçi tarafından emniyet kemeri kullanılmamakta ya da emniyet kemeri işçi tarafından takıldığı halde emniyet kemerinin kancası güvenlik halatına takılmayıp, kanca iş elbisesinin cebine takılabilmektedir. Ya da işçi tarafından baret veya emniyet kemeri takmamanın "erkek adam olma" şeklinde görülmesi mümkün olabilmektedir.

İşyerlerindeki tehlikelerin, risk önlemlerinin, planlar ve hedefler hakkında bilgi ve talimatların yönetim kurulu toplantılarından en alt seviyedeki iş gücüne kadar iletilmesi ve bir davranış değişikliği haline getirilebilmesi gerekmektedir. İşte bu aşamada da iş sağlığı ve güvenliği kültürünün yerleştirilmesinde "Öğrenen Bir Organizasyon" olabilme kavramını gündeme getirmektedir.

2.2. Öğrenen Organizasyonlar

Yönetim biliminde ilk defa 1990 yılında Peter Senge'nin *"The Fifth Discipline"* adlı kitabında kullandığı kavram, kısa bir süre içerisinde günümüz literatüründe en sık tekrarlanan terimlerden biri olmuştur. Kitapta geçen tanımlara göre öğrenen organizasyonlar kısaca **bilen**, **anlayan** ve **düşünen** organizasyonlardır. Öğrenen organizasyon kavramı, bir işletmenin sürekli olarak yaşadığı olaylardan sonuç çıkarması, bunları aynı zamanda çalışanlarını geliştirebileceği bir sistem içinde değişen çevre koşullarına adapte edebilmesi ve tüm bunların sonucunda sürekli olarak değişen, gelişen ve kendini yenileyen dinamik bir işletme olması anlamına gelmektedir.

Öğrenen organizasyon, kavramı ilk ortaya koyan Senge'ye göre, *"Kişilerin gerçekten arzu ettikleri sonuçları elde etmek için kapasitelerini sürekli olarak geliştirdikleri; yeni, sınırları zorlayan düşünce şekillerinin ortaya atıldığı; insanların sürekli biçimde beraber öğrenmeyi öğrendikleri organizasyonlardır. Öğrenmek daha fazla bilgi edinmek anlamına gelmez. Söz konusu olan, hayatta gerçek-*

ten istediğimiz sonuçları üretme yeteneğini geliştirmektir. Bu, hayat boyu üretici öğrenmedir. Her seviyede bunu uygulayan insanlara sahip olmadıkça, öğrenen organizasyonlar da mümkün olmaz."

Senge, öğrenen organizasyonların özelliklerini tanımlarken kişisel gelişim, düşünce modelleri, takım çalışması, ortak vizyon, sistem düşüncesi gibi kavramları vurgulamaktadır. Öğrenen organizasyonları diğer organizasyonlardan ayıran temel öge öğrenme sürecine verdikleri önemdir.

Marquardt'e göre (2002) öğrenen organizasyonlar; öğrenmeyi ödüllendirici ve cesaretlendirici, kolaylaştırıcı bir iklim temin ederler. Öğrenenler kahramandır. Öğrenme, performans değerlendirildiğinde, ödül törenlerinde, ödemelerde, ödül planlarında çalışanların edindiği yeni bilgilerin bedelini ödemek şeklinde takdir edilir. Öğrenen organizasyonda öğrenme süreçleri, öğrenme içeriği kadar önemli sayılır. Öğrenmeyi tanımlama yeteneği ihtiyacı, bulunan cevaplar kadar önemlidir.

Öğrenme, bugün için iş kazaları ve meslek hastalıklarını önleme konusunda, tek olmasa da var olan en önemli üstünlüklerden birisidir. Eğitim sürecinin en önemli amacı, bireyi, içinde bulunduğu güvenlik kültürüne ve çevreye uyum yeteneği kazandıracak yeterliklerle donatarak, onu üretken kılmaktır.

Senge'ye göre Öğrenen Organizasyonlarda, çalışan her birey mevcut koşullara uyum sağlamada belirli aşamalardan geçmektedir ve süreç içerisinde edindiği bilgi ve öğrenme sonucunda çalıştığı koşullara uyum sağlamaktadır. Bu aşamaları inceleyecek olursak;

I. AŞAMA: Bilinçsiz, Farkında Olmadan ve Yetersiz Öğrenme

Kişilerin bir eylemi gerçekleştirirken hem ne yapacaklarını bilmedikleri hem de yaptıklarının doğru mu yanlış mı olduğunu bilmedikleri aşamadır. Dolayısı ile bu aşamada kişi o işi yapamadığını bilmiyordur dolayısı ile en fazla hatanın yapıldığı aşamadır.

II. AŞAMA: Bilinçli ve Yetersiz Öğrenme

Bu aşama "acı" aşamasıdır. Hangi konuda olursa olsun kişiler o konuda aslında hiçbirşey bilmediklerini, hataları olduğunu ve önlerinde uzun bir yol olduğunu farkederler ve genellikle kendilerine olan güvenlerini ve inanclarını yitirirler. Bu gerçekten acılı bir süreçtir. Hem ne kadar az şey bildiklerini farketmişlerdir hem de ne yapacakları konusunda bir fikirleri yoktur. Çevresindeki herkes kişiye çok yetenekli ve başarılı gelmeye başlar. Dikkat edilecek ve öğrenilecek pek çok konu vardır. İşte en çok öğrenilebilen aşama da bu aşamadır.

III. AŞAMA: Bilinçli ve Yeterli Öğrenme

Bu aşamada kişiler artık beyinleri ile yaptıkları arasında bir uyum sağlamışlardır. Yoğun çalışma ve eğitim sonucunda öğrenilen fiiller veya egzersizler

artık sevilen, yapılmadıkça rahatsızlık veren hayatın parçaları haline gelmiştir. Kendilerini iyi oyuncular olarak hissederler ve bu kendilerine güven verir, bir önceki aşamada yitirdikleri kendilerine olan güvenlerini kazanırlar. Dışarıdan iyi oyuncu olarak kabul edilmeye başlarlar ama onlar kendi eksiklerinin ve hatalarının farkındadırlar ve bunu düzeltecek bilgiye veya bu bilgiye ulaşma şansına sahiptirler. Yaptıkları eylemi, sorunlarını daha iyi teşhis edebilir, problemi tanımlayabilirler. Ne kadar öğrendiklerini, ne kadar öğrenmeleri gerektiğini bilirler. Neticede başarılı ve gelişen bir dönemdir ve önceki iki döneme göre çok daha uzun sürer. Pek çok çalışan bu aşamada kalmayı tercih edebilmektedir.

IV. AŞAMA: USTALIK- Bilinçsiz, Farkında Olmadan ve Yeterli Öğrenme

Bu aşamada kişilerin kafasındaki olması gerekenle hareketlerin sonuçları arasında artık bir fark kalmamıştır. Artık uygulama doğal ve düşünülmeden yapılacak kadar kişinin bir parçası olmuştur.

Öğrenme olgusu, 'etken' değil 'edilgen' karakterlidir. Geus'a göre öğrenme, algılama ile başlar, ne herhangi bir insan, ne de herhangi bir firma, çevresinde ilgisini çeken herhangi bir şey görmediği sürece öğrenmeye başlamaz.

Sürekli öğrenme ve tecrübe edinme, belli yapılara yeniden şekil verme imkanı sağlar. Hızlı öğrenip yeni gelişmelere adapte olan organizasyonlar, yeni tecrübelere açık organizasyonlardır.

Öğrenen organizasyonlar çalışanların ulaşmak istedikleri sonuçlar için sürekli olarak düşünce yapılarını geliştirdikleri ortamlardır. Çalışanların yeni ve gelişmiş düşünce ağları bu ortamda beslenir, toplu istekler serbest bırakılır ve kişiler sürekli olarak beraber nasıl öğrenmeleri gerektiğini keşfederler.

Bir organizasyonun işletme içerisinde güvenliği veya emniyeti tehdit edebilecek davranış veya uygulamaların zararını en aza indirmeyi amaçlayan, güvenlik veya emniyete öncelik veren; algıları, inançları, tutumları, kuralları, rolleri, sosyal, teknik ve politik uygulamaları yerleştirebilmesi yani GÜVENLİK KÜLTÜRÜNÜ yerleştirebilmesi için, bir organizasyon olarak, bu organizasyonda görev alan tüm yönetici, mühendis, şef, usta vb. ve işçilerle birlikte ÖĞRENEN BİR ORGANİZASYON olması gerektiği açıktır.

Ülkemiz işyerleri düşünüldüğünde, işyerlerinde verimli iş sağlığı ve güvenliği yönetim sistemlerinin kurulabilmesi ve güvenlik kültürünün bir yaşam felsefesi haline getirilebilmesi için tüm organizasyonların en üst düzeyde çalışan yöneticisinden, işvereninden tüm çalışanlarına öğrenen organizasyonlar olarak dinamik işletmeler olmaları, iş kazaları ve meslak hastalıklarının önlenmesinde büyük yararı olacağı yadsınamaz bir gerçekliktir.

3. BÖLÜM: RİSK DEĞERLENDİRME METODOLOJİLERİNİN DOĞUŞU

3.1. Tarihçe

Günümüzden yaklaşık 350 yıl önce risk değerlendirme ve yönetimi olarak nitelendirebileceğimiz bütün faaliyetler tamamıyla batıl inanışlar, içgüdüsel davranışlar veya kâhinlerin telkinleri vb. etkenlere bağlı olarak gerçekleştirilmekteydi. Modern bilim sayesinde geçmiş ile gelecek arasındaki sınır, risk değerlendirilmesinin günümüzdeki anlamıyla yapılması sonucu çizilmiştir diyebiliriz. Ancak bu gelişim sonrasında her türlü hız, güç, hareket iletişim vb. fiziksel ölçüm değerleri insanlık için bir anlam ifade eder hale gelmiştir.

Risk Değerlendirme Metodolojilerinin tarihçesine bakıldığında ilk adımların yine Sanayi Devrimi sırasında atıldığını görmekteyiz. Yeni anlayış çerçevesinde büyük önem kazanan "Risk Değerlendirmesi" kavramı 20. yüzyılın başlarında güvenilirlik teoreminin oluşturulması ve kullanılmaya başlanması sonrasında telaffuz edilmeye başlanmıştır.

1955'lerden itibaren öncelikle A.B.D.'de başlayan ve bilgisayar, ticari jet uçuşları, uzay araştırmaları ve tıp alanının getirdiği yeni ve etkili buluşlarla süratle gelişen çağdaş uygarlık dönemi, ilk on yıllık süre içinde büyük gelişme kaydetmiştir.

I. Dünya Savaşı'nın sonlarında uzay ve hava bilimciler aynı işlevi görmek üzere oluşturulmuş sistemleri nicel olarak karşılaştırma yolları aramaya başlamışlardır. Çift motorlu uçakların tek motorluIara kıyasla daha az bozulduklarını farkederek, her tip araç için bir " bozulma oranı" (uçuş saatinin bir oranı olarak bozulma sayısı) hesaplamışlardır. Bu arada, geçmiş olayları karşılaştırmak için kullanılan bu oranların, aynı zamanda gelecek olayları öngörmek amacı ile de kullanılmaya başlaması 1930'lu yıllarda gerçekleşebilmiştir. Bu şekilde; daha sonra güvenilirlik teorisi adı ile anılacak olan yeni bir disiplin ortaya çıkmıştır.

Bu şekilde "GÜVENİLİRLİK TEORİSİ" olarak anılan yeni disiplinin, Olasılık Teoremleri ile birlikte kullanılmaya başlanması ile Risk Değerlendirme çalışmalarının temeli atılmıştır.

Risk değerlendirme çalışmalarının öncülüğünü savunma sanayi ve uzay çalışmaları yapmıştır, ancak savunma sanayinin risk değerlendirmesi ile ilgili aktif uygulamalarına baktığımızda çok yakın denebilecek tarihlerde başladığını görürüz.

Risk Değerlendirmesi kavramı 20. yüzyılın başlarında güvenilirlik teoreminin oluşturulması ve kullanılmaya başlanması sonrasında telaffuz edilmeye başlanmıştır. İlk defa NASA tarafından geliştirilen MIL-STD-882 nolu standart bu alandaki gelişmelerin önünü açan ilk sistemli belge olmuştur. Ünlü analist Peter F. Drucker yöneticilere vermiş olduğu bir konferansta 18., 19. ve 20. Yüzyıllarında Batı ekonomisinin ilerlemesinde teşebbüs, girişim ve çabuk ve doğru karar verme yeteneği kadar risk değerlendirme yönetiminin de önemli bir yere sahip olduğunu vurgulamıştır. Drucker'a göre riskleri yönetme ve önlem alma çalışmaları gelişmiş ülkeler ve gelişmekte olan ülkeler arasındaki en önemli farktır.

3.2. Emekleme Dönemi

İkinci Dünya Savaşı'nın bitiminden önce Almanya, roketleri operasyonel olarak konuşlandırıp kullanabilecek bir seviyeye ulaşmıştır. Nazi Almanya'sının 1942'nin sonlarından itibaren hava hâkimiyetini kaybetmeye başlamasıyla beraber, Alman toprakları Müttefik hava bombardımanlarının hedefi haline gelmiştir. Buna karşılık Alman Hava Kuvvetlerinin bu saldırılara misilleme yapabilecek imkânlardan yoksun oluşu, Adolf Hitler'in 'İntikam Silahı' adını verdiği V1 ve V2 (Vergeltungswaffe 1 ve 2) roketlerini kullanıma sokulması sonucunu doğurmuştur.

II. Dünya Savaşı'nda Alman roket sanayinin başında bulunan Alman bilim adamı Wernher von Braun (1912 –1977), Almanya ve ABD'de roket teknolojisinin gelişmesini sağlayan önemli bir bilim adamıdır. Wernher von Braun, roketlerle uğraşmaya 17 yaşında başlamış kısa sürede yükselip Alman askeri roket geliştirme programının başına geçmiş ve ilk uzun menzilli balistik roketleri V1 ve V2 yi geliştirmiştir. 'Uçan Bomba' adı verilen V1, esasen pilotsuz bir jet uçağıdır ve günümüzdeki 'cruise' füzelerinin atası olarak değerlendirilebilir.

Alman havacılık firması olan Fiesler firmasında çalışan Robert Lusser, pilotsuz uçak çalışmalarında Fieseler Fi 103R Reichenberg'i geliştirmiş ve daha sonra Nazi Almanya'sında Wernher von Braun'ın ekibine katılarak Vergeltungswaffe-1 veya diğer bilinen adıyla V-1 füzesini dizayn edilmesine yardımcı olmuştur.

V1 ve V2 balistik füzelerinin geliştirilmesi esnasında elektronik bileşenlerde meydana gelen rastgele aksaklıklar, mekanik bileşenlerdeki yaşlanma ve aşırı stres benzeri bir şekilde hesaplanmaktaydı. Bunların arasındaki farkın anlaşılması güvenilirlik modellemelerinin geliştirilmesine yol açmıştır.

V1 balistik füzesinin ilk serisi özellikle belirlenen hedefi vurma konusunda oldukça başarısız olmuş, bu nedenle de Wernher von Braun pilotsuz uçak geliştirme projesinde çalışmaları bulunan Robert Lusser'i ekibine davet etmiştir. Alman roket takımına uzman olarak davet edilen, Robert Lusser, proje sorumlularına "bir zincirin dayanıklılığının, o zincirin tek tek ele alınan her bir parçasının dayanıklılığından daha zayıf olduğunu" açıklamıştır.

Alman uçak mühendisi ve matematikçi Robert Lusser'in günümüzde "Lusser Kanunu" olarak bilinen teoremi sayesinde V1 füzesinin hedefi vurma kabiliyeti %0' lardan %60'lara kadar geliştirilebilmiştir. Daha sonraki yıllarda Eliyahu Goldratt ve arkadaşları tarafından bu teorem sistem ve kalite uygulamalarına da uygulanmıştır ve "Kısıt Teorisi" olarak da anılmaya başlanmıştır. Ancak bu ünlü zincir anolojisi ile anılan teoremi ilk defa matematikçi Robert Lusser öne sürmüştür.

Lusser Kanunu'na göre bir sistemin başarısını sağlamak için alt sistemleri çözümlemek ve tek tek ele almak gerekmektedir. Robert Lusser'in bu teoremi daha sonra yapılacak güvenilirlik çalışmalarına temel oluşturmuştur.

1940 ve 1959'lu yıllarda, güvenilirlik yaklaşımı özellikle havacılık, askeri ve nükleer sahalarda ilerlemeler kaydetmiştir. Gerçekte, bozulmaların bilimi olarak güvenilirliğin ele alınması olayının 1950'lerde, Amerika Birleşik Devletleri'nde, özellikle elektronik alanında ortaya çıktığı söylenebilir. Bu da uzun yıllar boyunca salt nicel yaklaşımların çok sayıda olmasının nedenini açıklamaktadır. Amerikan Savunma Bakanlığı, 1 dolar eşdeğerli bir elektronik parçanın iyi durumda tutulabilmesi için yılda 2 dolarlık bir bakım masrafına gereksinim olduğunu saptadığında, daha en başta güvenilir parçalar elde etmenin önemini ortaya çıkarmıştır. Fakat sistemler çok karmaşık ve parçaları çok değişkenli olduğundan mühendislerin en kuvvetli bilgi düzeyleri bile tatmin edici bir başarı düzeyine erişilmesini engellemiştir. Bunun sonucunda, elektronik techizat alımı için yapılan her ihalede üreticilerin, uzun süreli deneyler ile ürünlerinin güveniliklerini ispat etmeleri şart koşulmuştur. Bu deneyler sonucunda güvenilirliğe ilişkin verilerden meydana gelen ünlü "Elektronik Teçhizatın Güvenilirliğinin Tahminine İlişkin 217 Askeri Standardı" elde edilmiştir.

1950'li yılların sonlarında, sistemlerin bozulmasında insan hatalarının önemini vurgulayan çok sayıda çaIışma gerçekleştirilmiştir. Uçakların kullanımında insan güvenilirliği konusunu dikkate alan çalışmalar sonucunda havacılık

yeniden öncül sektör konumuna gelmiştir. İnsan hataları da dâhil olmak üzere, sistem güvenilirliğinin tahminine ilişkin ilk çalışmalar 1957 yılından itibaren başlamıştır. Bu çalışmalar insanı "mekanik bir birim" olarak kabul etmektedirler. Güvenilirlik bilimine parallel olarak, daha az sıklıkla matematiksel destek ihtiyacına sahip olan, bozuk parçaların eski konumuna getirilmesi için bakım, onarım konusu da gündeme gelmiştir. Amerika Birleşik Devletleri'nde, ilk "Güvenilirlik ve Bakım Sempozyumu" 1954'de gerçekleştirilmiştir. Fransa'da Ulusal Telekomünikasyon Araştırma Merkezi (CNET) çalışmalarına 1955 yılında başlamış ve CNET güvenilirlik merkezi 1961 yılında kurulmuştur.

İş kazaları ve meslek hastalıklarının oluşmasında teknolojideki hızlı gelişim, makineleşme, işyerlerindeki fiziksel ve kimyasal etmenler ile üretimde kullanılan ham ve yardımcı maddelerin yanında ekonomik, sosyolojik, psikolojik, fizyolojik ve ergonomik bir çok etken rol oynamaktadır. Özellikle sanayi devrimi sonrasında teknolojik gelişmeler sonucunda üretimin yapısı oldukça karmaşıklaşmış, hızlı ve kontrolsüz sanayileşme süreci ve üretimin giderek yoğunlaşması iş kazaları ve meslek hastalıkları ile çevre kirliliği gibi sorunların önemli boyutlara ulaşmasına neden olmuştur.

3.3. Güvenilirlikle İlgili Doktrinlerin Oluşumu

1960'lı yıllarda, mekanik, hidrolik ve elektrik aksamlı sistemlerin doğru çalışması için yapılan araştırmalarda giderek güvenilirlik teorisinin kullanımı artmıştır. Ancak elektronik sistemlerin değerlendirilmesi için geliştirilmiş olan araçlar diğer tip teçhizat değerlendirmelerine iyi uyum gösterememiştir. Bunun sonucunda yeni yöntemler araştırılmaya başlanmıştır. İşte bu dönemde, BelI Laboratuarlarından H.A. Watson, Minuteman füzelerinin güvenliğini değerlendirmek üzere "Hata Ağacı" adı ile tanınan bir yöntemi ortaya koymuştur. Bu yöntem sayesinde, karmaşık sistemlerin çalışmalarında öngörülemeyen bozulmaları tanımlamak mümkün olmuştur. Birçok endüstri bu yöntemi kullanmıştır ve halen de kullanmaktadırlar. Özellikle NASA; Mercury ve Germini programlarının başlangıcından beri bu yöntemden yararlanmaktadır.

Ayrıca, AVCO olarak adlandırılan ve pompa, vana gibi elektromekanik teçhizatın, güvenilirlik değerlerine ilişkin tabloları, çalıştıkları çevrenin bir fonksiyonu olarak veren tabloların ilk olarak 1961 yılında yayınlandıklarını da bu aşamada belirtmek gerekir. Bu tablolar birçok firmada halen kullanılmaktadır. 1960'lı yılların başlarından itibaren insan güvenilirliğine ilişkin verilerden olu-

şan bir banka da ortaya konulmuştur. Bu veri bankası, vasıfsız işlerde insan hataları düzeyini vermektedir. Son olarak 1963'de THERP Yöntemi (Technique For Human Error Prediction: İnsan Hatalarının Tahmini İçin Teknik) nükleer silahların güvenliğinin değerlendirilmesi çerçevesinde, A.D. Swain tarafından geliştirilmiştir.

Bu on yıllık dönemde oldukça fazla çalışma gerçekleştirilmiştir, örneğin; PasquiII atmosferin denge şartlarını ve başlangıç hızı olmayan az sayıdaki çevre kirleticilerinin yayılımına ilişkin bir modeli 1961 ve 1962 yıllarında yayınlamıştır. Sözkonusu model birkaç düzeltme ile halen çok yoğun olarak kullanılmaktadır.

3.4. Olasılık Kuramlarının Oluşumu

Risk kavramının tanımlanmasında büyük önem teşkil eden olasılık teorisi ilk kez günümüzden yaklaşık 300 yıl kadar önce Paskal ve Pierre de Formet adındaki matematikçinin ortak çalışmaları sonucu bulunmuştur. Günümüzde risk yönetiminde kullanılan temel araçların hemen hemen tümü 1654 ile 1754 yılları arasındaki gelişmeler sonrasında ortaya konmuştur.

Olasılık teorisinin başlangıcı şans oyunlarıyla ilgili fiziksel gözlemlerde yatmaktadır. 1650 yıllarında kumar fransız toplumunda çok yaygındır ve zar, kart, para atışı, rulet gibi oyunlar oldukça gelişmiştir. Şans oyunlarına olan bu ilgi bazı formüllerle kumar şansının hesaplanabileceği düşüncesini akla getirmiştir. O dönemin Chevalier de Méré gibi etkili sözü geçen kumarbazları, Pascal, Fermat ve daha sonra d'Alembert ve De Moivre gibi zamanın önde gelen matematikçilerinin bu konuda yardımcı olabileceğini düşünmüşlerdir. Matematikçilerin problemi benimsemesiyle klasik olasılık konusu şekillenmiştir.

Olasılığın tanımı 1654 yılında Pascal ve Fermat arasındaki yazışmalarda formüle edilmiştir. Huygens 1657 yılında konuyla ilgili ilk bilimsel eseri yayınlamış ve meşhur Bernoulli teoremi ile binom dağılımı 1713 yılında ortaya atılmıştır.

Olasılıkların çarpılması kuralı başlığıyla bilinen genel teorem de Moivre tarafından 1718 yılında öne sürülmüş ve 1733'den 1738'e kadar normal olasılık dağılımı ve merkezi limit teoreminin bir özel durumu yine aynı matematikçi tarafından tartışılmıştır. Sekiz yıl sonrada ünlü İsviçreli matematikçi Jakop Bernoulli'nin yeğeni Daniel Bernoulli tarafından risk yönetimi yöntemlerinde yaygın olarak kullanılan beklenen fayda kavramının tanımı yapılmıştır.

Normal dağılışla ilgili daha ileri gelişmeler Gauss tarafından gerçekleştirilmiş, aşağı yukarı aynı zamanlarda "En Küçük Kareler" kuralı Legendre tarafından formülleştirilmiştir.

Laplace 1812 yılında şans oyunlarıyla ilgili matematiksel teorinin tam bir özetini vermiştir ancak 1812 yılından hemen sonra klasik matematikçilerin istatistik ve olasılık teoremlerine olan ilgisi neredeyse kaybolmuştur. Konuya ilişkin daha sonraki gelişmeler teorik ve uygulamalı alanlarda çalışan istatikçiler tarafından gerçekleştirilmiştir. Gaunt'ın 1662 yılında İngiltere'deki hayat ve ölüm kayıtlarını yayınlaması olasılığın ve deneysel olasılığın bugünkü biçimine dönüşmesinde ilk adım olmuştur.

Birkaç yıl sonra bu kayıtlar ve bunlarla ilgili yorumlar Halley tarafından önemli derecede geliştirilmiştir. Halley'e bazen bu nedenle istatistiğin babası bile denmektedir. Günümüzde risk yönetiminde kullanılan temel araçların hemen hemen tümü 1654 ile 1754 yılları arasındaki gelişmeler sonrasında ortaya konmuştur. İş kazaları ve meslek hastalıkları, insan hayatına maddi ve manevi zararlar vermekte, bunun yanında hem çalışanlara hem de işletmelere ve dolayısıyla ulusal ekonomiye önemli ölçüde maddi zarar ve yük getirmektedir.

3.5. Nükleer Tesisler İçin Çalışmaların Artışı

Ciddi bir kaza veya olay meydana geldiğinde, bilim adamları çeşitli sorular sormaya başlamışlar ve kazaların meydana gelme mekanizmalarını açıklamaya çalışmışlar ve çeşitli disiplinlerde Olası Hata Türü ve Etkileri Analizi (FMEA), Hata Ağacı Analizi (FTA), Olay Ağacı Analizi (ETA), Tehlike ve Çalışabilirlik Analizi (HAZOP) vb. Risk Değerlendirme Metodolojilerini üretmişlerdir.

İşyerlerinde yapılacak risk değerlendirme çalışmalarında özellikle büyük endüstriyel kazalara sebebiyet verebilecek kritik sistemlerin de irdelenmesi ve bu sistemlerde oluşabilecek, tehlikeli olarak tanımlanan sapmaların giderilmesi ile sistemlerin güvenilirliğinin arttırılması gerekliliği de ortaya çıkmıştır.

1979'lı yılların başında, Nükleer Düzenlemeler Komisyonu üyelerinden N.Rasmussen ve mühendislerden oluşan ekibi nükleer santrallerin kendi bütünlükleri içinde ilk tüm "risk analizi" çalışmalarını gerçekleştirmişler, çeşitli kaza senaryolarının oluşa gelme olasılıklarını hesaplamışlar ve sonuçlarını değerlendirmişlerdir.

Araştırma temelde Hata Ağacı yöntemine dayanarak gerçekleştirilmiştir. Rasmussen tarafından ortaya konulan metodoloji dünyadaki nükleer birimlerin

güvenliklerinin araştırılmasına büyük bir katkı sağlamıştır ve halen de sağlamaktadır. THERP yöntemi ise insan faktörünün, güvenlik üzerindeki etkisini değerlendirmek maksadı ile kullanılmıştır.

Yine 1970'li yılların başlarında "The Aerospatiale-British Aerospace Concorde" projesi için sistem güvenirliğinin değerlendirilmesi amacı ile özellikle kendi problemlerine çok iyi uyarlanmış yeni yöntemler geliştirilmiştir. Önce Concorde sonra Airbus programına sistematik olarak uygulanan bu yöntem teknik başarı ve bu araçların güvenilirlikleri üzerinde hiç şüphesiz büyük rol oynamıştır. Benzer şekilde, olasılık düzenlemeleri ilk olarak Concorde projesi sırasında ortaya atılmıştır. Bu, bir yandan hataların küçük, anlamlı, kritik ve felakete sebebiyet verici şeklinde sınıflandırılmaları öte yandan da tüm bu bozukluk türlerinin uyması gereken risk amaçlarının ortaya konması temeline dayanmaktadır. Örneğin, felakete sebep olabilecek ve dolayısı ile uçağın kaybı ile sonuçlanacak bir bozukluğun uçuş saati başına %7'den daha büyük bir olasılıkta olmaması gereklidir.

Fransa'da nükleer, askeri ve sivil alanında da güvenirlik yöntemleri, benzer şekilde 1970'li yılların başlarında kullanılmaya başlamıştır. Özellikle, Fransız elektronükleer programının öncüleri tarihte hiç rastlanmamış bir durumla karşı karşıya kalmışlardır. Proje sorumluları, Hiroşima'ya atılan atom bombası sonucu ortaya çıkan sonuçlar nedeni ile nükleer enerji kullanımına karşı yoğun protestolar ile karşılatı. Bu sorumluluk altında olarak daha inşa edilmeden sistemlerinin güvenilirliklerini, sayısal ve mantıksal birçok teknik kullanarak ispat etmek durumunda kalmışlardır.

Bu konudaki bir başka aşama 1978'de Ingiltere'de Birleşik Kraliyet Atomik Enerji Yetkili Merkezi (UKAEA - United Kingdom Atomic Energy Authority) tarafından gerçekleştirilen risk analizi çalışmaları olmuştur. Merkez, Londra'nın batısında Times nehrinin kuzey kıyısında bir ada olan Canvey Adası'ndaki petrokimyasal kompleksin büyütülmesine ilişkin risklerin değerlendirilmesi amacı ile çalışmalar gerçekleştirmiştir. Bu şekilde nükleer bir alan dışında ilk kez tam bir risk analizi gerçekleştirilmiştir. Bu çalışma, tesise ikinci bir erişim güzargahının saptanması gibi ek bir takım güvenlik önlemleri alınması halinde kompleksin büyütülmesinin risklerde farkedilir düzeyde bir artışa yolaçmayacağını saptamıştır. Söz konusu araştırma boyunca kullanılan yöntemler nükleer endüstride sürekli olarak kullanılan yöntemler olmuştur.

Son olarak, 70'li yıllara karşılık gelen on yıl içerisinde gerçekleştirilen çalışmalar güvenilirlik ve güvenlik konusundaki veri birikimlerinin oluşmasını sağlamıştır. Çalışmalar, 1970 yılında Birleşik Kraliyet Atom Enerji Ünitesi Veri Bankası'nın kurulmasına aracı olmuştur. 1975 yılında ise elektromekanik bileşenler hakkındaki RADC- TR-75-22 verilerinin yayınlanması vb. gelişmelere sebep olmuştur.

3.6. Tüm Endüstriler İçin Disiplinlerin Oluşturulması

Amerika Birleşik Devletleri'nde Tree Mil Adaları'nda meydana gelen ve ölümle sonuçlanmamakla birlikte büyük zarar ve ziyana yol açan kaza ise 1979'da meydana gelmiştir. Bu kaza güvenlik çalışmalarına yeni bir ivme vermiştir. Ancak klasik endüstriye ilişkin risk değerlendirme çalışmalarının hızla başlamasında İtalya Seveso'daki büyük endüstriyel kaza dönüm noktası olmuştur.

80'li on yıllarda ise özellikle güvenilirlik konularında daha önce belirtilen çabalarda büyük artış olmuş ve daha derinlemesine gelişmeler yaşanmıştır. Öte yandan, bu on yıllık süre aşağıdaki nedenlerden ötürü ayrı bir öneme sahiptir:

- Güvenilirlik verilerinin toplanması;
- Güvenlik konusunda yeni analiz yöntemlerinin oluşturulması;
- İnsan faktörünü dikkate alan yöntemlerin geliştirilmesi (HCR Yöntemi: Kişilerin Bilimsel Cevaplarının Saptanması Tekniği, HEART: İnsan Hatalarının Saptanması ve Azaltılması Tekniği vb.),
- Tüm endüstrilerde (otomotiv, havacılık, kimya, petrokimya vb.) bu dönemde güvenliğin sağlanmasına ilişkin teknikler ele alınmaya başlanmış,
- PC'lerde düşük fiyata, kaliteli ve hızlı hesaplayabilme olanakları sağlayan hesap mantıkları geliştirilmiştir.
- Sayısal simülasyonları uygulamaya sokup doğrulamak üzere büyük çaplı deneyler gerçekleştirilmiş,
- Salt insan güvenliğini sağlamak için değil üretim kayıplarını da enazlamak üzere techizat bozulmalarının daha büyük sıklıklarla dikkate alınması sağlanmıştır.

1981 yılında A.B.D. savunma müsteşarı Frank C. Carlucci tarafından tedarik uygulamalarının iyileştirilmesine yönelik 32 maddeden oluşan bir rapor

yayınlanmıştır. Bahis konusu raporun 11. maddesinde Savunma Bakanlığınca (Defence of Department - DoD) hazırlanan sistem tedarik programları bütçelerinde teknik risklerin etkilerinin daha iyi bir biçimde ele alınmasının gereği belirtilmiştir.

Bir yerde bir kaza veya ciddi bir olay meydana geldiğinde, benzer sistemleri inceleyen endüstriciler çeşitli sorular sormaya yönelmiştir. Kazanın meydana geldiği tesis veya en azından yüksek riskli sektörler için, uygun tesislerin sahip olduğu güvenli risk düzeyine erişebilmek üzere risk değerlendirmesi gerçekleştirmenin önemli bir fırsat olduğu düşünülmeye başlanmıştır. Kazalar çok ciddi olduğunda veya daha büyük anormalliklerin göstergesi oldukları düşünüldüğünde, güvenlik otoriteleri endüstricilerden risk değerlendirme istemeye yönelmiştir. Üç Mil Adası'ndaki ve Çernobil'deki kazalardan sonra nükler alanda bu enerjinin işletilmesi ile ilgili farklı ülkelerin güvenlik otoritelerinin isteği üzerine büyük ölçüde araştırmalar gerçekleştirilmiştir. Klasik endüstriye ilişkin olarak ise Seveso'da (İtalya) meydana gelen kaza kesin bir dönüm noktası olmuştur.

İtalya'nın Seveso şehrinde 1976 yılında meydana gelen büyük endüstriyel kaza sonucunda, büyük risk kaynağı olarak kabul edilen tesislerin risk olasılıklarının sistematik olarak araştırılmasının empoze edilmesi konusunda yetkililerin eğilimlerinde artış olmuştur. Bu eğilimler sonucunda ise 24 Haziran 1981 tarihli 82/501/EEC Seveso yönergesi yayınlanmıştır. Salt insan, proses veya sistem hatalarını veya olasılıklarını değerlendirmek yerine, bu hataların hangi şartlarda gerçekleştiğinin anlaşılması ve en aza indirilmesi hususunda risk değerlendirme çalılanmalarının yapılması gerektiği anlaşılmıştır. Bir sistemin tüm yaşam eğrisi boyunca karşılaştığı her çeşit teknolojik risk durumu dikkate alınmaya başlanmıştır.

Nihayet 1986 yılında ABD Genelkurmay Başkanlığı (United States General Accounting Office) tarafından "Teknik Risk Değerlendirmesi" (Tecnical Risk Assesment – The Status of Current DoD Efforts) adında bir rapor yayınlanmıştır. Sözkonusu rapor 25 proje ofisinde teknik risklerin incelenmesine yönelik yürütülen uygulamaları içermektedir, ayrıca yine bu raporda risk değerlendirmesinde kullanılan metodolojiler incelenmiştir.

İngiltere Savunma Bakanlığı, 1986 yılında yaptığı bir çalışma neticesinde 12 savunma projesinde yürüttüğü incelemeler çerçevesinde risklerin sistematik olarak ele alınmaması ve süre- maliyet tahminlerinin risk analiz sonuçlarını dik-

kate almadan yapılmasının projelerde yaklaşık %90'na varan maliyet getirdiğini saptamıştır. Bunun üzerine yapılan tüm projelerde planlama aşamasında risk değerlendirme faaliyetlerinin "Risk Kayıt Dökümanı" ile raporlanmasına karar verilmiştir.

1989 yılı Mart ayında Savunma Sistemleri Yönetim Koleji (Defence Systems Management College) tarafından "Risk Yönetimi Konsepti ve Kılavuzu" (Risk Management Concept and Guidance) isimli diğer bir referans kaynak yayınlanmıştır. 1991 yılı Nisan ayında da yine "Teknik Risk Değerlendirmesi" isimli yeni bir referans kaynak basılmıştır.

4. BÖLÜM: ÜLKEMİZDEKİ MEVZUAT

4.1. Risk Değerlendirme Yaptırma Yükümlülüğü

Resmi Gazete'de 30.06.2012 tarihinde yayımlanmayan "6331 sayılı İş Sağlığı ve Güvenliği Kanunu", işyerlerinde iş sağlığı ve güvenliğinin sağlanması, mevcut sağlık ve güvenlik şartlarının iyileştirilmesi için işveren ve çalışanların görev, yetki, sorumluluk, hak ve yükümlülüklerini düzenlemektedir. İş Sağlığı ve Güvenliği Kanunumuzu incelediğimizde, Avrupa Birliğinin 89/391 sayılı Konsey Direktifinin gerekliliklerinin kanun kapsamında yer aldığını ve çerçeve direktifin ana unsurlarının yeni kanun çerçevesinde yasalaştırıldığını görmekteyiz. Söz konusu Direktif tüm çalışanların sağlığı ve güvenliği konusundaki gelişmeleri teşvik edecek önlemler sunmakta ve tüm işyerlerindeki riskleri kontrol altına almak için geniş kapsamlı bir strateji belirlemektedir. Direktif, iş sağlığı ve güvenliğini sağlamada genel önleme ilkelerini, risk değerlendirmesini ve risk yönetimini esas almaktadır.

6331 sayılı İş Sağlığı ve Güvenliği Kanunu çerçevesinde işverenler; çalışanların işle ilgili sağlık ve güvenliğini sağlamakla yükümlüdür. Bu çerçevede işverenler aşağıda verilen yükümlülükleri yerine getirmek zorundadırlar;

- Mesleki risklerin önlenmesi, eğitim ve bilgi verilmesi dâhil her türlü tedbirin alınması, organizasyonun yapılması, gerekli araç ve gereçlerin sağlanması, sağlık ve güvenlik tedbirlerinin değişen şartlara uygun hale getirilmesi ve mevcut durumun iyileş-tirilmesi için çalışmalar yapmak,
- İşyerinde alınan iş sağlığı ve güvenliği tedbirlerine uyulup uyulmadığını izlemek, denetlemek ve uygunsuzlukların giderilmesini sağlamak,
- Risk değerlendirmesi yapmak veya yaptırmak,
- Çalışana görev verirken, çalışanın sağlık ve güvenlik yönünden işe uygunluğunu göz önüne almak,
- Yeterli bilgi ve talimat verilenler dışındaki çalışanların hayati ve özel tehlike bulunan yerlere girmemesi için gerekli tedbirleri almak.

Risk değerlendirmesinin işyerlerinde ne şekilde yapılacağı, değerlendirme yapacak kişi ve kuruluşların nitelikleri, gerekli izinlerin verilmesi ve iptal edilmesi ile ilgili usul ve esaslar ise 29 Aralık 2012 tarih ve 28512 sayılı İş

Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği'nde verilmiştir. Bu Yönetmeliğin amacı, işyerlerinde iş sağlığı ve güvenliği yönünden yapılacak risk değerlendirmesinin usul ve esaslarını düzenlemektir. Yönetmelik 30/12/2012 tarihinde yürürlüğe girmiştir ve 20/6/2012 tarihli ve 6331 sayılı İş Sağlığı ve Güvenliği Kanunu kapsamındaki tüm işyerlerini kapsamaktadır.

Risk değerlendirmesi yönetmeliğimize göre; tüm işyerleri için tasarım veya kuruluş aşamasından başlamak üzere tehlikeleri tanımlama, riskleri belirleme ve analiz etme, risk kontrol tedbirlerinin kararlaştırılması, dokümantasyon, yapılan çalışmaların güncellenmesi ve gerektiğinde yenileme aşamaları izlenerek gerçekleştirilmesi gerekmektedir. Çalışanların risk değerlendirmesi çalışması yapılırken ihtiyaç duyulan her aşamada sürece katılarak görüşlerinin alınması sağlanması zorunludur. İşveren; çalışma ortamının ve çalışanların sağlık ve güvenliğini sağlama, sürdürme ve geliştirme amacı ile iş sağlığı ve güvenliği yönünden risk değerlendirmesi yapmak veya yaptırmak zorundadır.

Risk değerlendirmesinin gerçekleştirilmiş olması; işverenin, işyerinde iş sağlığı ve güvenliğinin sağlanması yükümlülüğünü ortadan kaldırmamaktadır. İşveren, risk değerlendirmesi çalışmalarında görevlendirilen kişi veya kişilere risk değerlendirmesi ile ilgili ihtiyaç duydukları her türlü bilgi ve belgeyi temin etmekle yükümlü kılınmıştır.

Aynı çalışma alanını birden fazla işverenin paylaşması durumunda, yürütülen işler için diğer işverenlerin yürüttüğü işler de göz önünde bulundurularak ayrı ayrı risk değerlendirmesi gerçekleştirilmesi gerekmektedir. İşverenler, risk değerlendirmesi çalışmalarını, koordinasyon içinde yürütmek, birbirlerini ve çalışan temsilcilerini tespit edilen riskler konusunda bilgilendirmek zorundadırlar.

Birden fazla işyerinin bulunduğu iş merkezleri, iş hanları, sanayi bölgeleri veya siteleri gibi yerlerde, işyerlerinde ayrı ayrı gerçekleştirilen risk değerlendirmesi çalışmalarının koordinasyonu yönetim tarafından yürütülür. Yönetim; bu koordinasyonun yürütümünde, işyerlerinde iş sağlığı ve güvenliği yönünden diğer işyerlerini etkileyecek tehlikeler hususunda gerekli tedbirleri almaları için ilgili işverenleri uyarır. Bu uyarılara uymayan işverenleri Bakanlığa bildirir. Bir işyerinde bir veya daha fazla alt işveren bulunması halinde:

- Her alt işveren yürüttükleri işlerle ilgili olarak, bu Yönetmelik hükümleri uyarınca gerekli risk değerlendirmesi çalışmalarını yapar veya yaptırır.
- Alt işverenlerin risk değerlendirmesi çalışmaları konusunda asıl işverenin sorumluluk alanları ile ilgili ihtiyaç duydukları bilgi ve belgeler asıl işverence sağlanır.
- Asıl işveren, alt işverenlerce yürütülen risk değer-lendirmesi çalışmalarını denetler ve bu konudaki çalışmaları koordine eder.
- Alt işverenler hazırladıkları risk değerlendirmesinin bir nüshasını asıl işverene verir. Asıl işveren; bu risk değerlendirmesi çalışmalarını kendi çalışmasıyla bütünleştirerek, risk kontrol tedbirlerinin uygulanıp uygulanmadığını izler, denetler ve uygunsuzlukların giderilmesini sağlar.

4.2. Dokümantasyon

Yönetmeliğimize göre risk değerlendirmesi asgari aşağıdaki hususları kapsayacak şekilde dokümante edilmesi gerekmektedir;

- İşyerinin unvanı, adresi ve işverenin adı,
- Gerçekleştiren kişilerin isim ve unvanları ile bunlardan iş güvenliği uzmanı ve işyeri hekimi olanların Bakanlıkça verilmiş belge bilgileri,
- Gerçekleştirildiği tarih ve geçerlilik tarihi,
- Risk değerlendirmesi işyerindeki farklı bölümler için ayrı ayrı yapılmışsa her birinin adı
- Belirlenen tehlike kaynakları ile tehlikeler,
- Tespit edilen riskler,
- Risk analizinde kullanılan yöntem veya yöntemler,
- Tespit edilen risklerin önem ve öncelik sırasını da içeren analiz sonuçları,
- Düzeltici ve önleyici kontrol tedbirleri, gerçekleştirilme tarihleri ve sonrasında tespit edilen risk seviyesi.

Risk değerlendirmesi dokümanının sayfaları numaralandırılarak; gerçekleştiren kişiler tarafından her sayfası paraflanıp, son sayfası imzalanıp ve işyerinde bu şekilde saklanması gerekmektedir. Risk değerlendirmesi dokümanı elektronik ve benzeri ortamlarda hazırlanıp arşivlenebilir.

4.3. Risk Değerlendirmesinin Yenilenmesi

Yapılmış olan risk değerlendirmesi; tehlike sınıfına göre çok tehlikeli, tehlikeli ve az tehlikeli işyerlerinde sırasıyla en geç iki, dört ve altı yılda bir yenilenir. Risk değerlendirme yenilenme süreleri aşağıda belirtilen durumlarda ortaya çıkabilecek yeni risklerin, işyerinin tamamını veya bir bölümünü etkiliyor olması göz önünde bulundurularak risk değerlendirmesi tamamen veya kısmen yenilenir.

- İşyerinin taşınması veya binalarda değişiklik yapılması,
- İşyerinde uygulanan teknoloji, kullanılan madde ve ekipmanlarda değişiklikler meydana gelmesi,
- Üretim yönteminde değişiklikler olması,
- İş kazası, meslek hastalığı veya ramak kala olay meydana gelmesi,
- Çalışma ortamına ait sınır değerlere ilişkin bir mevzuat değişikliği olması,
- Çalışma ortamı ölçümü ve sağlık gözetim sonuçlarına göre gerekli görülmesi,
- İşyeri dışından kaynaklanan ve işyerini etkileyebilecek yeni bir tehlikenin ortaya çıkması.

4.4. Risk Değerlendirmesi Ekibi

Risk değerlendirmesi işi bir tek kişinin işi değildir. İş Sağlığı ve Güvenliği Kanunu'nun Risk Değerlendirmesi Yönetmeliği'nin 6. maddesi'nde açıkça belirtildiği gibi "Risk Değerlendirmesi" işlemi ekip tarafından gerçekleştirilmelidir. Risk değerlendirmesi ekibi aşağıdakilerden oluşur;

- İşveren veya işveren vekili,
- İşyerinde sağlık ve güvenlik hizmetini yürüten iş güvenliği uzmanları ile işyeri hekimleri,
- İşyerindeki çalışan temsilcileri,

- İşyerindeki destek elemanları,
- İşyerindeki bütün birimleri temsil edecek şekilde belirlenen ve işyerinde yürütülen çalışmalar, mevcut veya muhtemel tehlike kaynakları ile riskler konusunda bilgi sahibi çalışanlar.

İşveren, ihtiyaç duyulduğunda bu ekibe destek olmak üzere işyeri dışındaki kişi ve kuruluşlardan hizmet alabilir. Risk değerlendirmesi çalışmalarının koordinasyonu işveren veya işveren tarafından ekip içinden görevlendirilen bir kişi tarafından da sağlanabilir.

İşveren, risk değerlendirmesi çalışmalarında görevlendirilen kişi veya kişilerin görevlerini yerine getirmeleri amacıyla araç, gereç, mekân ve zaman gibi gerekli bütün ihtiyaçlarını karşılar, görevlerini yürütmeleri sebebiyle hak ve yetkilerini kısıtlayamaz. Risk değerlendirmesi çalışmalarında görevlendirilen kişi veya kişiler işveren tarafından sağlanan bilgi ve belgeleri korur ve gizli tutar.

4.5. Risk Değerlendirmesi Aşamaları

Risk değerlendirmesi; tüm işyerleri için tasarım veya kuruluş aşamasından başlamak üzere tehlikeleri tanımlama, riskleri belirleme ve analiz etme, risk kontrol tedbirlerinin kararlaştırılması, dokümantasyon, yapılan çalışmaların güncellenmesi ve gerektiğinde yenileme aşamaları izlenerek gerçekleştirilir. Çalışanların risk değerlendirmesi çalışması yapılırken ihtiyaç duyulan her aşamada sürece katılarak görüşlerinin alınması sağlanır. İşyerinde çalışanlar, çalışan temsilcileri ve başka işyerlerinden çalışmak üzere gelen çalışanlar ve bunların işverenleri; işyerinde karşılaşılabilecek sağlık ve güvenlik riskleri ile düzeltici ve önleyici tedbirler hakkında bilgilendirilir.

a) Tehlikelerin Tanımlanması

Tehlikeler tanımlanırken çalışma ortamı, çalışanlar ve işyerine ilişkin ilgisine göre asgari olarak aşağıda belirtilen bilgiler toplanır;

- İşyeri bina ve eklentileri,
- İşyerinde yürütülen faaliyetler ile iş ve işlemler,
- Üretim süreç ve teknikleri,
- İş ekipmanları,
- Kullanılan maddeler,

- Artık ve atıklarla ilgili işlemler,
- Organizasyon ve hiyerarşik yapı, görev, yetki ve sorumluluklar,
- Çalışanların tecrübe ve düşünceleri,
- İşe başlamadan önce ilgili mevzuat gereği alınacak çalışma izin belgeleri,
- Çalışanların eğitim, yaş, cinsiyet ve benzeri özellikleri ile sağlık gözetimi kayıtları,
- Genç, yaşlı, engelli, gebe veya emziren çalışanlar gibi özel politika gerektiren gruplar ile kadın çalışanların durumu,
- İşyerinin teftiş sonuçları,
- Meslek hastalığı kayıtları,
- İş kazası kayıtları,
- İşyerinde meydana gelen ancak yaralanma veya ölüme neden olmadığı halde işyeri ya da iş ekipmanının zarara uğramasına yol açan olaylara ilişkin kayıtlar,
- Ramak kala olay kayıtları,
- Malzeme güvenlik bilgi formları,
- Ortam ve kişisel maruziyet düzeyi ölçüm sonuçları,
- Varsa daha önce yapılmış risk değerlendirmesi çalışmaları,
- Acil durum planları,
- Sağlık ve güvenlik planı ve patlamadan korunma dokümanı gibi belirli işyerlerinde hazırlanması gereken dokümanlar.

Toplanan bilgiler ışığında; iş sağlığı ve güvenliği ile ilgili mevzuatta yer alan hükümler de dikkate alınarak, çalışma ortamında bulunan fiziksel, kimyasal, biyolojik, psikososyal, ergonomik ve benzeri tehlike kaynaklarından oluşan veya bunların etkileşimi sonucu ortaya çıkabilecek tehlikeler belirlenir ve kayda alınır. Bu belirleme yapılırken aşağıdaki hususlar, bu hususlardan etkilenecekler ve ne şekilde etkilenebilecekleri göz önünde bulundurulur;

- İşletmenin yeri nedeniyle ortaya çıkabilecek tehlikeler,

- Seçilen alanda, işyeri bina ve eklentilerinin plana uygun yerleştirilmemesi veya planda olmayan ilavelerin yapılmasından kaynaklanabilecek tehlikeler,
- İşyeri bina ve eklentilerinin yapı ve yapım tarzı ile seçilen yapı malzemelerinden kaynaklanabilecek tehlikeler,
- Bakım ve onarım işleri de dahil işyerinde yürütülecek her türlü faaliyet esnasında çalışma usulleri, vardiya düzeni, ekip çalışması, organizasyon, nezaret sistemi, hiyerarşik düzen, ziyaretçi veya işyeri çalışanı olmayan diğer kişiler gibi faktörlerden kaynaklanabilecek tehlikeler,
- İşin yürütümü, üretim teknikleri, kullanılan maddeler, makine ve ekipman, araç ve gereçler ile bunların çalışanların fiziksel özelliklerine uygun tasarlanmaması veya kullanılmamasından kaynaklanabilecek tehlikeler,
- Kuvvetli akım, aydınlatma, paratoner, topraklama gibi elektrik tesisatının bileşenleri ile ısıtma, havalandırma, atmosferik ve çevresel şartlardan korunma, drenaj, arıtma, yangın önleme ve mücadele ekipmanı ile benzeri yardımcı tesisat ve donanımlardan kaynaklanabilecek tehlikeler,
- İşyerinde yanma, parlama veya patlama ihtimali olan maddelerin işlenmesi, kullanılması, taşınması, depolanması ya da imha edilmesinden kaynaklanabilecek tehlikeler,
- Çalışma ortamına ilişkin hijyen koşulları ile çalışanların kişisel hijyen alışkanlıklarından kaynaklanabilecek tehlikeler,
- Çalışanın, işyeri içerisindeki ulaşım yollarının kullanımından kaynaklanabilecek tehlikeler,
- Çalışanların iş sağlığı ve güvenliği ile ilgili yeterli eğitim almaması, bilgilendirilmemesi, çalışanlara uygun talimat verilmemesi veya çalışma izni prosedürü gereken durumlarda bu izin olmaksızın çalışılmasından kaynaklanabilecek tehlikeler.

Çalışma ortamında bulunan fiziksel, kimyasal, biyolojik, psikososyal, ergonomik ve benzeri tehlike kaynaklarının neden olduğu tehlikeler ile ilgili işyerinde daha önce kontrol, ölçüm, inceleme ve araştırma çalışması yapılmamış ise risk değerlendirmesi çalışmalarında kullanılmak üzere; bu tehlikelerin,

nitelik ve niceliklerini ve çalışanların bunlara maruziyet seviyelerini belirlemek amacıyla gerekli bütün kontrol, ölçüm, inceleme ve araştırmalar yapılır.

b) Risklerin Belirlenmesi ve Analizi

Tespit edilmiş olan tehlikelerin her biri ayrı ayrı dikkate alınarak bu tehlikelerden kaynaklanabilecek risklerin hangi sıklıkta oluşabileceği ile bu risklerden kimlerin, nelerin, ne şekilde ve hangi şiddette zarar görebileceği belirlenir. Bu belirleme yapılırken mevcut kontrol tedbirlerinin etkisi de göz önünde bulundurulur. Toplanan bilgi ve veriler ışığında belirlenen riskler; işletmenin faaliyetine ilişkin özellikleri, işyerindeki tehlike veya risklerin nitelikleri ve işyerinin kısıtları gibi faktörler ya da ulusal veya uluslararası standartlar esas alınarak seçilen yöntemlerden biri veya birkaçı bir arada kullanılarak analiz edilir.

Maddenin metninden anlaşıldığı üzere işyerlerinde yapılan risk değerlendirme çalışmalarında ulusal veya uluslararası standartlar kullanılması istenilmektedir. İşyerinde birbirinden farklı işlerin yürütüldüğü bölümlerin bulunması halinde birinci ve ikinci fıkralardaki hususlar her bir bölüm için tekrarlanır.

Analizin ayrı ayrı bölümler için yapılması halinde bölümlerin etkileşimleri de dikkate alınarak bir bütün olarak ele alınıp sonuçlandırılır. Analiz edilen riskler, kontrol tedbirlerine karar verilmek üzere etkilerinin büyüklüğüne ve önemlerine göre en yüksek risk seviyesine sahip olandan başla-narak sıralanır ve yazılı hale getirilir.

c) Risk Kontrol Adımları

Yönetmeliğe göre risklerin kontrolünde şu adımlar uygulanır;

i. Planlama:

Analiz edilerek etkilerinin büyüklüğüne ve önemine göre sıralı hale getirilen risklerin kontrolü amacıyla bir planlama yapılır.

ii. Risk kontrol tedbirlerinin kararlaştırılması:

Riskin tamamen bertaraf edilmesi, bu mümkün değil ise riskin kabul edilebilir seviyeye indirilmesi için aşağıdaki adımlar uygulanır;

- Tehlike veya tehlike kaynaklarının ortadan kaldırılması,

- Tehlikelinin, tehlikeli olmayanla veya daha az tehlikeli olanla değiştirilmesi,
- Riskler ile kaynağında mücadele edilmesi.

iii. Risk kontrol tedbirlerinin uygulanması:

Kararlaştırılan tedbirlerin iş ve işlem basamakları, işlemi yapacak kişi ya da işyeri bölümü, sorumlu kişi ya da işyeri bölümü, başlama ve bitiş tarihi ile benzeri bilgileri içeren planlar hazırlanır. Bu planlar işverence uygulamaya konulur.

iv. Uygulamaların izlenmesi:

Hazırlanan planların uygulama adımları düzenli olarak izlenir, denetlenir ve aksayan yönler tespit edilerek gerekli düzeltici ve önleyici işlemler tamamlanır. Risk kontrol adımları uygulanırken toplu korunma önlemlerine, kişisel korunma önlemlerine göre öncelik verilmesi ve uygulanacak önlemlerin yeni risklere neden olmaması sağlanır.

Belirlenen risk için kontrol tedbirlerinin hayata geçirilmesinden sonra yeniden risk seviyesi tespiti yapılır. Yeni seviye, kabul edilebilir risk seviyesinin üzerinde ise bu maddedeki adımlar tekrarlanır.

4.6. Büyük Kaza Önleme Politika Belgesi veya Güvenlik Raporu Hazırlanması Gereken İşyerlerinde Risk Değerlendirmesi

6331 sayılı İş Sağlığı ve Güvenliği Kanunun 29 uncu maddesi gereğince büyük kaza önleme politika belgesi veya güvenlik raporu hazırlanan işyerlerinde; bu belge ve raporlarda değerlendirilmiş riskler, bu Yönetmeliğe göre yapılacak risk değerlendirmesinde dikkate alınarak kullanılır.

30 Aralık 2013 tarihli Mükerrer Resmi Gazetede yeni yayınlanan Büyük Endüstriyel Kazaların Önlenmesi ve Etkilerinin Azaltılması Hakkında Yönetmelik'in 8. maddesi kapsamındaki alt ve üst seviyeli kuruluşlarda büyük endüstriyel kaza tehlikelerinin belirlenmesi ve bu tehlikelerden kaynaklanacak risklerin değerlendirilmesi amacıyla kantitatif metotlarla risk değerlendirmesi yapılır.

Kantitatif risk değerlendirmesinde, büyük kazaya yol açabilecek tehlikeler ve aşağıda belirtilen hususlar dikkate alınır:

- Tehlikeli kimyasalların sınıflandırılması, bu kimyasalların miktarları ve karşılıklı etkileşimleri.
- Kimyasal maruziyetin insan ve/veya çevre açısından değerlendirilmesi.
- Patlayıcı ortamlar ve bu ortamların kalıcılığı, patlayıcı ortam sınıflandırması ve bu alanlarda kullanılacakekipmanların uygunluğu.
- Proses içerisindeki tehlikeli ekipmanların belirlenmesi ve gruplandırılması.
- Proses tehlikeleri ile proses ekipmanlarının ve/veya enstrümanlarının karşılıklı etkileşimleri.
- Proses enstrümanlarının ve acil durum kapatma sistemlerinin güvenilirlik değerlendirmesi ve sertifikasyonu.
- Bakım ve onarım işlerinde güvenilirlik verisi.
- Güvenilirlik merkezli gerçekleştirilecek bakım ve risk temelli kontrol yöntemleri.
- Büyük kaza senaryolarının kök neden ve sonuç analizi.•Geçmişte yaşanan kazalar ve bu kazaların nicel tekrarlanma olasılıkları.
- İnsan hataları ve güvenilirlik analizi.

5. BÖLÜM: TEKNOLOJİK RİSK KAVRAMI

Bütün iş ve işlemler çeşitli riskler taşır, özellikle endüstriyel tesislerdeki kazalar ise bize sıfır riskin mevcut olmadığını hatırlatmaktadır. Bu tür endüstriyel kazlar teknolojideki hızlı gelişme sonucu giderek daha sık gerçekleşmekte ve gerçekleştiklerinde de sonuçları az veya çok "felaket" olmaktadır. Bu durum doğal olarak riski iki boyutlu bir büyüklük yani olasılık ve sonuçlar şeklinde dikkate almaya yönlendirmektedir. Riskin bu tanımı son derece geneldir ve tesis güvenliğine ilişkin olayları; olma olasılığı yüksek, sonuç - zarar düşük şeklinde karakterize edebildiği gibi olma olasılığı düşük, sonuç - zarar büyük ifadesiyle ortaya koyan "FELAKETLERİ" de tanımlamaktadır.

"Teknolojik Riskten" bahsedildiğinde genelde ilk akla gelen onun "güvenlik" yönüdür, çünkü insan hayatı söz konusudur. Buna karşın "üretim" yönü de en az o denli önemlidir; aksi takdirde tesisin kendisinin varlığını veya çevresini tehlikeye sokabilecek boyutta ekonomik kayıplara yol açabilir. Saptanmış bir teknolojik riski azaltmak için iki yol bulunmaktadır;

- Riskin meydana gelme olasılığını düşürmek veya
- Şiddeti azaltmaya yönelik sistemler kurmak suretiyle sonuçların etkisini küçültmek.

Güvenlik analizinin birçok faydası sayılabilir, analizin tipine bağlı olarak bunlar çeşitlilik göstermekte, ve daha detaylı tanımlar bu kitabın ilerleyen bölümlerinde verilmektedir. Güvenlik analizinin sonuçlarına dair örnekler aşağıda verilmiştir:

- İşyerindeki risklerin genel gözden geçirmesi,
- İşyerindeki tehlikelerin listesi ve bunların değerlendirmeleri,
- İşyeri için alınacak güvenlik önlemleri,
- Belli kazaların nasıl meydana gelebileceğinin detaylı açıklaması, bunların meydana gelme ihtimali, ve muhtemel sonuçları,
- Bir kazanın incelenmesi, teknik, insani ve organizasyonel faktörlerin olaya etkisinin irdelenmesi,
- İşyerinde alınmış güvenlik önlemlerinin özeti ve bunların etkinliğinin değerlendirmesi
- Katılımcıların üretim ve güvenlik sisteminin işleyişine dair daha kapsamlı bilgilendirilmesi.

- Teknolojik riskte güvenliğin yanında güvenilirliğe ilişkin çalışmalar da büyük önem arz etmektedir. Nükleer endüstri bugün artık güvenilirliğe ilişkin olarak olasılık araştırmalarını yoğun şekilde yürütmektedir.

Petrol sahalarında sık sık risk değerlendirmesinden başka sahalarda güvenilirliğe dayalı olasılık veya tehlike analizi teriminden bahsedilmektedir. Özellikle bu tür tesislerde kazaların açıklanması geniş değişkenlik gösterir ve düzenli ya da yaygın kullanımlı bir teori yoktur. Fakat çeşitli kaza analiz yöntemlerinde kazaların nasıl oluştuğuna dair açık modeller mevcuttur.

Meydana gelen kazayı sadece bir nedenin ortaya çıkardığını ve yanlızca bir açıklamasının olduğunu düşünmek en fazla rastlanılan bakış açısıdır. Ancak bu bakış açısı ne yazıkki kazaların asıl nedeni veya nedenlerinin ele alınmasını zorlaştırmakta ve problemlerin etkili şekilde çözümünü engelleyebilmektedir. Bu nedenle, açıklama ve teoriler, genellikle kazaların neden meydana geldiği ve nasıl önlenebileceği hakkında yeterli anlayış sağlaması nedeniyle yararlıdır.

5.1. Kaza Modelleri ve Teknolojik Risk Arasındaki İlişki

Kazaları açıklamak üzere çok sayıda değişik model geliştirilmiştir. Özellikle insan hataları konusunda, insan davranışı ve karakteristiği ile ilgili uzun zamandır araştırma yapılmaktadır. "Domino Teorisi" olarak adlandırılan teori ise ilk olarak 1930'larda Heinrich tarafından ortaya atılmıştır ve uzun zaman boyunca güvenli çalışma için büyük önem görmüştür. Bu teoride kaza; ardışık olaylar, güvensiz davranış ve fiziksel tehlikeler açısından tanımlanmaktadır. Teoride kazalar şayet bu elemanlar ortadan kaldırılabilirse önlenebilir. Fakat Domino teorisi kazaları çok basit bir biçimde açıkladığı için aynı zamanda birçok eleştirye de maruz kalmıştır. Niçin çalışan insan tarafından güvensiz hareketlerin yapıldığını veya neden mekanik ve fiziksel tehlikelerin oluştuğunu bu teori açıklayamamaktadır.

Daha geniş ya da dar kapsamda sistemleri merkez alan birkaç değişik model vardır ancak bu modellerin çoğu belirli sonuçları elde edebilmek maksadıyla birbirini etkilemesi gereken teknoloji, insan ve organizasyonel kaynaklar ile şirketi bir sistem olarak görür. Bu sistemlerde oluşabilecek hata veya kusurların da her zaman kazaya katkısı olan nedenler olduğu görüşü üzerine kuruludurlar. Bunlar anormal sistem etkileri olarak ifade edilir ve sistemin tek tek bileşenlerinin (insan hatası da dahil olmak üzere) veya onlar arasındaki ilişkinin bozulması nedeniyle kazaların oluştuğu fikri üzerinde durulur.

Kaza, ani istenmeyen ve planlanmamış, genellikle ölüm, yaralanma veya maddi hasarla sonuçlanan bir olay olarak tanımlanabilir ya da önceden bilinmeyen istem dışı bir olgu sonrası aniden meydana gelip kontrol dışına çıkan ve kişinin bedensel bütünlüğüne zarar verebilecek yada maddi hasara neden olabilecek nitelikteki olaylardır. Bize bir bakış açısı kazandırması açısından kaza ile ilgili bazı teorilere kısaca değineceğiz;

- **Tek Faktör Teorisi:**

Bu teori, bir kazanın tek bir nedenin sonucu olarak ortaya çıktığını ileri süren görüşten doğar. Eğer bu tek neden tanınabilir ve ortadan kaldırılabilir ise kaza tekrar etmeyecektir. Bu teori genellikle temel sağlık ve güvenlik eğitimi almış kişilerce kabul edilmemektedir.

- **Domino Etkisi Teorisi:**

Bu teoride olaylar beş domino taşının arka arkaya sıralanarak, birbirini düşürmesine benzetilerek açıklanmıştır. Her kaza beş tane temel nedenin arka arkaya dizilmesi sonucu meydana gelir, buna "Kaza Zinciri" de denir. Şartlardan biri gerçekleşmedikçe bir sonraki gerçekleşmez ve dizi tamamlanmadıkça kaza meydana gelmez.

- **Enerji Teorisi:**

Bu teoriye göre (William Haddon tarafından ortaya atılmıştır) kazalar daha çok Muhtemelen enerji transferinde ya da enerji transferi esnasında meydana gelir.

Bu enerji boşalmasının oranı önemlidir çünkü enerji boşalması ne kadar büyükse, hasar potansiyeli de o kadar büyüktür. Tehlikelerin tanınmasında bu kavram çok sınırlandırılmış ve bu haliyle tek etken teorisine benzemektedir. Tek faktör teorisinden farklı olarak enerji boşalması önemlidir.

- **İnsan Faktörleri Kuramı:**

Bu teori kazaları, eninde sonunda insan hatasından kaynaklanan olaylar zincirine bağlar. Teori, insan hatasına yol açan üç önemli faktörü içerir: Aşırı yük, uygun olmayan tepki ve yerinde olmayan faaliyetler. Bu teorileride kaza sebepleri teorileri üç geniş kategori altında sınıflandırılmıştır: Kaza-yatkınlık teorileri, işçi kabiliyetlerine karşılık iş talebi teorileri ve psikososyal teoriler.

Kazaların insan hatalarından kaynaklanması bir çok faktöre dayanır. Kuşkusuz, kaza yapan işçinin eğitimsizliği, işe uygun olmayışı, uyumsuzluğu, eğitim ve bilgi eksikliği, tecrübesizliği, yorgunluğu, heyecanlı veya üzüntülü

oluşu, dalgınlığı, dikkatsizliği, ilgisizliği, düzensizliği, meleke noksanlığı ve hastalıkları vb. nedenler; ya da işçinin her şeye karşın kurallara uymamış olması da insan faktörüne bağlı temel sebepler arasındadır.

- **Kaza/Olay Kuramı:**

Bu teori insan faktörleri teorisinin genişletilmiş bir halidir. Ek olarak; ergonomik yetersizlikleri, hata yapma kararı ve sistem hataları gibi yeni elemanları ortaya çıkarır.

- **Sistem Kuramı:**

Teori bir kazanın oluşabileceği herhangi bir durumu, üç parçadan oluşan bir sistem olarak görür: İnsan, makine ve çevre.

- **Kombinasyon Kuramı:**

Bir tek teorinin tek başına bütün hadiseleri açıklayamayacağını savunur. Teoriye göre kazaların gerçek sebebi iki veya daha fazla modelin kombinasyonu ile elde edilebilir.

- **Epidemiyoloji Kuramı:**

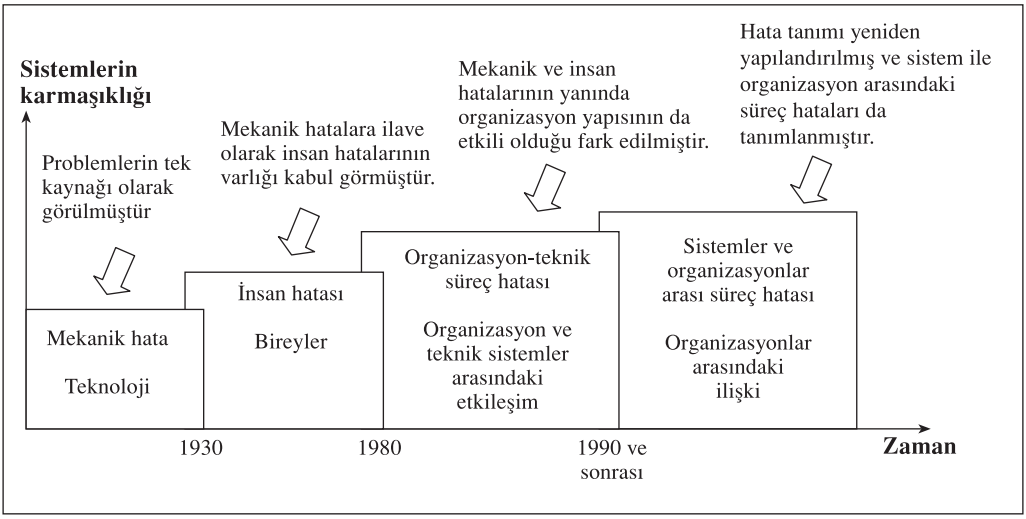
Teori, çevre faktörleri ve hastalık arasındaki ilişkiyi belirleme ve çalışma için kullanılan modellerin, çevre faktörleri ile kazalar arasındaki sebepsel ilişkinin açıklanmasında da kullanılabileceğini savunur.

- **Çok Etken Teorisi:**

Kaza birçok etken ile birlikte değerlendirilerek analiz edilir. Bu teori ve analiz yöntemleri birçok deneyimli sağlık ve güvenlik uzmanları tarafından da kabul edilip uygulanmaktadır. Kazalar çok etkenlidir, standart altı uygulamalar, standart altı şartların oluşması sonucu bir hatalar zinciri sonucu meydana gelir.

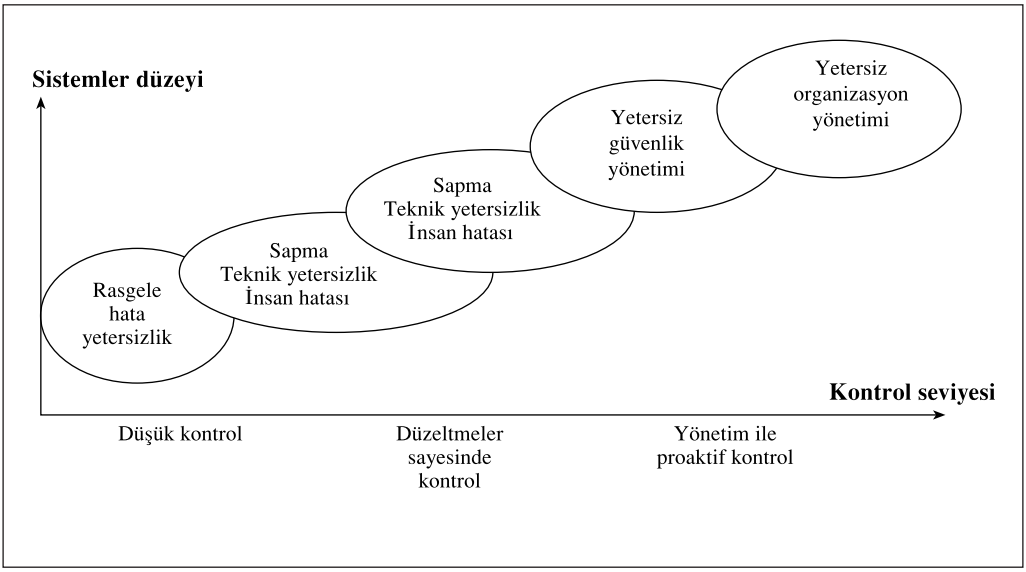
Kaza nedenlerine bakış açısının zamanla nasıl değiştiği **Şekil 1**'de verilmiştir. Teknolojik sistemler daha gelişmiş güvenlik özelliklerine sahip olma eğilimindedir ve kazanın teorik olasılığı sık sık aşırı düşük olarak görünmektir. Güvenlik sistemlerinin başarısız olması ihtimali kaza modellemelerinin ilk yıllarında pek düşünülmemekte sadece teknik aksam üzerinde olabilecek arızalar kaza nedeni olarak görülmekte idi. Perrow, 1984; Reason, 1990, 1997'de sistemlerin planlandığı gibi çalışmaması veya zamanla kötüleşmesi durmunun ve güvenlik sitemlerinin tüm tehlike olasılıklarını kapsamaması durumlarının da düşünülmesi gerektiğini ifade etmişlerdir. İşte bu aşamada işin içine organizasyonlardaki sosyal yapının bunu analiz yapabilme yeteneğinden yoksun olmasının ve hatta sistem ile organizasyon arasındaki süreç hatalarının da kaza nedeni olduğunu öne sürmüşlerdir.

Şekil 1: Kaza Kaynakları Üzerine Uzun Dönemli Bakış



Başka bir bakış açısı da **Şekil 2**'de verilmiştir. Şekilden de görüleceği üzere önceleri kazaların nedenlerinin, insan hatası veya yetersizliği nedeni ile meydana gelen rasgele hatalar sonucunda ortaya çıktığı değerlendirilmiştir. Kaza nedenlerinin organizasyonun küçük derecede de olsa kontrolünde olan rasgele olaylar nedeniyle meydana geldiği ifade edilmiştir. Daha sonraları ise kaza nedeni, organizasyonun yönetim siteminin yetersizliği olarak görülmüştür. Organizasyon tarafından yürütülen yönetim sistemi, kazaların engellenmesi için yeteri kadar etkili değildir. Bu açıklama daha çok bağımsız çalışan sistemler için uygun olabilir ancak özellikle büyük tehlike potansiyeli olan sistemler için geçerli değildir. Çünkü bu tür sistemlerde birbiri ile bağıntılı birçok alt sistemler ve karışık ilişki ağları (insan da dahil olmak üzere) bulunmaktadır. İşte bu sistemlerin ve bu ilişki ağlarının da gözden geçirilmesi gereklidir aksi takdirde bu karmaşık ilişki ağlarının ortaya çıkardığı yüksek risk yani "Teknolojik Risk" fark edilemez. Bu kaza modellemesi bakış açısında o nedenle de özellikle sistem düzeyinin artması ve karmaşık sistemler içermesi durumunda, bu sistemler arasındaki ilişki ağının incelenmemesi ve sistemde bulunan güvenlik sistemlerinin yeterli olup olmadığının değerlendirilmemesi durumunda "Teknolojik Risk" nedeni ile kazanı doğduğu belirtilmektedir. Bu nedenle de söz konusu değerlendirmeyi yapmayan organizasyon yönetimini kaza nedeni olarak belirtmektedir.

Şekil 2: Şirketteki Kontrolün Seviyesi ile İlişkili Olarak Kazaların Açıklaması



Son zamanlarda kazaların ve özellikle de "Teknolojik Risk" nedeni ile ortaya çıkan kazaların önlenmesine yönelik yeni bir kavram ortaya atılmıştır, bu da "Çalışma Güvenliği"dir. Çalışma güvenliğini sağlayabilmek için ise tesisteki tüm sistemlerin birbiri ile uyum içerisinde çalışmasından fazlası gerekmektedir. Bu bağlamda, güvenilir sistemlere, alt sistemlere, birimlere, eleman ve ekipmanlara ihtiyaç vardır ve bu elemanlardan en önemlilerinden birisi de insandır. İşte bu aşamada "Kritik Sistemlerde Güvenilirlik" kavramı ortaya çıkmaktadır. Güvenilirliği yüksek bir sistem, kendisinden bekleneni veya verimliliği hakkında şüpheye yolaçabilecek olaylara ve emniyet düzeyini tehlikeye atabilecek kazalara meydan vermeden çalışan bir sistemdir; dolayısı ile bir sistemin emniyetli çalışması durumu farklı bakış açılarından değerlendirilmektedir.

5.2. Kritik Sistemler ve Güvenilirlik Kavramı

Bir tesis veya proseste meydana gelebilecek hatanın önem derecesini belirlemek ve bu önem derecesine göre önlemleri planlamak gerekmektedir, ancak bu hataları belirleyebilmek için öncelikle sistem kavramı ve tanımına göz atmamız ve "Kritik Sistem" tanımını yapmamız gerekmektedir.

Uluslararası Sistem Mühendisliği Konseyi INCOSE (International Council on Systems Engineering), sistemi ortak bir hedefe doğru çalışan birbirleri ile ilişkili parçalar bütünü olarak tanımlamıştır. Sistemin özelliklerini ise aşağıdaki gibi vermiştir;

- Karmaşık bir bütün oluşturan, birbirlerini etkileyen, birbirine bağlı ve/veya birbirleriyle ilişkili parçalar (öğeler) grubudur,
- Parçaların her biri aynı süreç, işlem ve/veya yapı ile ilişkilidir,
- Parçalar birbirlerinden farklı biçim ve/veya işleve sahiptir,
- Parçaların kendilerine özgü nitelikleri(özellik ve işlevi) vardır,
- Sistem sınırlandırılabilir/sınırı çizilebilir bir yapıdadır,
- Parçalar birbirlerini ilişkiler ile etkiler,
- Parçalar da birer sistem olabilir.

Sistem bilimci olan Ian Sommerville (2004), sistemleri açıklarken aşağıdaki gibi bir ayrım vermiştir;

- **Emniyet -Kritik Sistemleri (Safety-critical systems);** hatası yaralanma, ölüm veya büyük çevresel hasarlara yol açabilen sistemler olarak tanımlamıştır. Örneğin; tren rotaları ve saatlerini düzenleyen sistemler.
- **Amacı Kritik Olan Sistemler (Mission-critical systems);** hatası sistemin amacını gerçekleştirememesine neden olan sistemler. Örneğin uzaya fırlatılan bir aracın rotasını belirleyen sistemler gibi.
- **İşi (Kullanıcısı) Kritik Olan Sistemler (Business-critical systems);** hatası kullanan şirketin hata yapmasına yol açan sistemler. Örneğin bir bankanın müşteri hesap sistemi gibi.

MIL-HDBK-189 Military Handbook'da ise sistemler çökme bazlı ele alınarak tanımlama yapılmıştır;

- **Güvenliği-Kritik Sistemler (Safety-critical systems);** çökmesi hayat kaybına, sakatlığa veya çevrenin zara görmesine neden sistemlerdir.
- **Görevi-Kritik Sistemler (Mission-critical systems);** sistemin çökmesi belirlenmiş hedeflerin başarısızlığa uğramasına neden olur.
- **İşi-Kritik Sistemler (Business-critical systems);** sistem çökmesi büyük ekonomik kayba neden olur.

Sistem tanımlarının genellikle aynı yaklaşımda verildiği görülmektedir. İki ayrı kaynaktaki en önemli fark; bir bakış açısının kritik hata bazlı bakarken, diğer bakış açısının sistemin çökmesi üzerine bakmasıdır. Ancak her iki tanımda da sonuç değişmemekte ve sistemin hata yapması veya çökmesi aynı sonucu doğurmaktadır.

Tüm sistemler, prosesler ve ekipmanlar için ise bir yaşam döngüsü söz konusudur. Yaşam döngüsü içerisinde güvenilirliği ne kadar yüksek bir sistem tasarlamaya çalışırsanız bu seferde karşınıza maliyet kavramı gelmektedir. %100 güvenilirlik sağlanmış bir sistemin maliyetinin çok yüksek olacağı aşikardır, işte bu aşamada gündeme yaşam döngüsü maliyeti (life-cycle cost concept of management) boyutlarından birkaçı olan İngilizce dependability, reliability, avaliability ve security fonksiyonlarının analitik olarak tanımlanması gelmektedir.

Literatürde güvenilirlik analizi konusunda yapılmış birçok çalışma mevcuttur. Bunlardan, bir kısmı güvenilirlik analiz yöntemlerinin geliştirilmesine yönelik çalışmalar olup, diğerleri ise farklı sistemlerin güvenilirliklerinin belirlenmesine yönelik çalışmalardır. Yine literatür taraması yapıldığında güvenilirlik analizinde geçen terimlerin tanımlarında da bazı farklılıklar olmasına rağmen birbirine yakın ifadeler içerdikleri görülmektedir. Bu terimlerden bazılarını inceleyecek olursak;

Dependability ve reliability kelimeleri ingilizcede eş anlamlıdır ve Türkçe karşılıkları güvenilirlik olarak verilmektedir, bu nedenle de bu iki İngilizce kelimenin anlamı büyük kafa karışıklıklarına neden olabilmektedir. Özellikle de yeni sistemlerin veya makinelerin güvenilirlik hesaplamaları yapılırken eskiden reliability hesaplanmasının önemi vurgulanırken artık dependability'nin bilinmesinin daha önemli olduğu otoritelerce kabul edilmektedir. Bu nedenle de özellikle bu iki kelimenin arasındaki farkı iyi ayırt etmek gerekmektedir.

ASHRAE Aplications Handbook'ta verilen tanımlara göz attığımızda; Dependability için bir sistemin durumunun ölçüsü olarak tanım yapıldığı görülmektedir. Sistemin, hizmet ömrünün başlangıcında çalışır durumda olduğunu kabul ederek, dependability hizmet ömrünün içindeki herhangi bir anda çalışabilir durumda olma olasılığıdır. Tüm bu tanımlar ışığında Dependability'i, Türkçe'de teknik terim olarak dayanaklılık olarak karşılık vermek daha doğru olacaktır.

ASHRAE Aplications Handbook'ta Reliability; tanımlanmış bir zaman periyodunun öngörülen bir dilimi içerisinde sistemin çalışacağının göstergesi olarak verilmiştir. Yine Reliability için makine emniyeti ile ilgili EN standartlarına bakıldığında EN ISO 292'de, bir makine veya elemanın veya donanımın belirli şartlar altında ve verilen bir zaman süresi içerisinde arızalanmaksızın istenen bir fonksiyonu yerine getirebilme kabiliyeti şeklinde tanımlandığını görürüz. ISO/IEC 27001-27002'de ise sistemin herhangi bir zaman dilimi içinde gerekli hizmetleri doğru bir biçimde verebilmesi olasılığı olarak verilmiştir. Söz konusu bu tanımlar ışığında Reliability'in Türkçede teknik terim olarak güvenilirlik olarak karşılık bulduğunu söylemek doğru olacaktır.

Yine özellikle sistem, proses, makine ve ekipmanların güvenilirlik çalışmalarında sıklıkla duyduğumuz avaliability, safety ve security kelimelerini de inceleyecek olursak;

EN ISO 292 'de avaliability için, amaçlanan kullanma şartları altında fonksiyonunu yerine getirebilmeye muktedir tutulabilme veya belirli uygulamalara göre ve belirli vasıtalar kullanarak yürütülen gerekli işlemlerle yeniden eski durumuna getirilebilme kabiliyeti şeklinde tanım verilmiştir. EN ISO 12100'de ise; bir makinenin diğerleri ile birlikte fonksiyonunun/fonksiyonlarının kolayca anlaşılabilir olmasını sağlayan özellikleri veya karakteristiği sayesinde kolayca kullanılabilme özelliği olarak verildiği görülmektedir. Yine sistem güvenilirliği ile ilgili bir standart olan ISO/IEC 27001-27002'de avaliability için, herhangi bir zamanda sistemin çalışır durumda olması ve istenilen hizmetleri verebilmesi olasılığı şeklinde tanım yapılmaktadır. Standartlardaki tanımlamalar incelendiğinde avaliability için Türkçede teknik terim olarak kullanılabilirlik şeklinde karşılık vermek yerinde olacaktır.

Yine aynı Dependability ve reliability kelimeleri gibi safety ve security kelimeleri de İngilizcede eş anlamlıdır ve Türkçe karşılıkları güvenlik olarak verilmektedir. Ancak yine standartlar araştırıldığında bu iki kelimenin anlamlarının birbirinden tamamen farklı anlamlar içerdiği görülür. EN ISO 12100- EN ISO 13849 –EN ISO 13850 standartlarında safety için makine dâhilinde veya çevresinde bulunan herhangi bir alan çerçevesinde bulunanlara zarar verebilme ölçüsü şeklinde tanımlama yapıldığı, ISO/IEC 27001-27002 standardında ise sistemin insanlara veya çevresine zarar verme ölçüsü olarak verildiği görülmektedir. Bu tanımlamalar çerçevesinde safety için Türkçe teknik terim olarak hatasızlık olarak karşılık vermek daha doğru olacaktır.

EN ISO 12100- EN ISO 13849 –EN ISO 13850 standartlarında ingilizce security için; makine dahilinde veya çevresinde bulunan fonksiyonların kasti ya da kazara yapılan etkilere dayanabilme ölçüsü olarak verilmişken, ISO/IEC 27001-27002 standardında otomasyon sisteminin kötü niyetli müdahalelere karşı kendini koruyabilme kabiliyeti şeklinde tanımlanma yapılmıştır. Bu tanımlar çerçevesinde security için Türkçe teknik terim olarak güvenlik kelimesini kullanmak yerinde olacaktır.

Bir başka deyişle günümüzde bu değerler niteliksel değil sayısal olarak ifade edilmekte, sistemlerin, makinelerin ve ekipmanların değerlendirmeleri de bu sayısal değerlere bakılarak yapılmaktadır. Ekonomik sistemlerin kurulması, maliyetleri minimize eden optimum işletme koşullarının (doğru yapılmış tasarım değerlerinde) sağlanması veya işletme sürecinde yaratılması, etkin ve sürekli hizmet verebilmek için bu değerlerin bilinmesi gerekmektedir.

Modern işletme ve bakım mühendisliği sistemlerinin önemli unsurlarından biri olmakla birlikte, söz konusu uygulamaların yapılabilmesi için gerekli olan, sistem ve ekipmanların durumlarının gözlenmesini gerektirmektedir. Gözlem (monitoring), hem ilgili sistem şartlarının (sıcaklık, debi, basınç vs) ve ekipmanlarının şartlarının (titreşim, yük, ses vs) gözlenmesini ve kayıt edilmesini (test raporları) hem de değerlendirilmesi süreçlerini içermektedir. Bu süreçlerin sonunda, işletme ve bakım planları gerçekleştirilebilmektedir. Aynı zamanda yine aynı sistemlerin veya makine ekipmanlarının risk değerlendirmelerini veya makine emniyeti ile ilgili mevzuat hükümleri ile standartlarına uygunluğunun sağlanabilmesi için de yine aynı değerlerin sayısal olarak ifade edilmesine ihtiyaç bulunmaktadır.

6. BÖLÜM: GÜVENİLİRLİK TEORİSİ

Güvenilirliği mühendislik bazında ele alacak olursak; modern toplumumuzda mühendislerin sorumluluğunda olan muhtelif makinelerin veya sistemlerin planlanması, üretimi ve işletimi konularını içeren bir tanımlama yapmamız gerekir. Bu sistemlerden ve makinelerden yararlanan kullanıcılar öncelikle bunların güvenilir olmasını isterler. Bu anlamda güvenilirliği bir karşılaştırma kavramı olarak kullanırlar. Dolayısıyla lojik olarak güvenilir veya güvenilmez nitelemeleri büyük bir anlam taşımaz. Önemli olan "ne derece güvenilir?" sorusunun yanıtıdır. Böyle bir sorunun yanıtı ise % 0 ile %100 arasındaki gerçek sayılarla verilebilir.

Başlangıçta deneyimlere dayanarak değerlendirilen güvenilirlik, bugün artık mühendisliğin ve işletmeciliğin her alanında uygunabilen bir bilim dalı haline gelmiştir. Bir dizi indisler tanımlanarak sistemlerin/makinelerin hangi koşullarda devre dışı kalacağı ve bu durumların yolaçacağı olumsuzluklar belirlenmeye çalışılmaktadır. Diğer yanda ise tasarım maliyeti hesaplanmakta ve güvenilirlik-maliyet arasındaki ekonomik denge kurulmaya çalışılmaktadır.

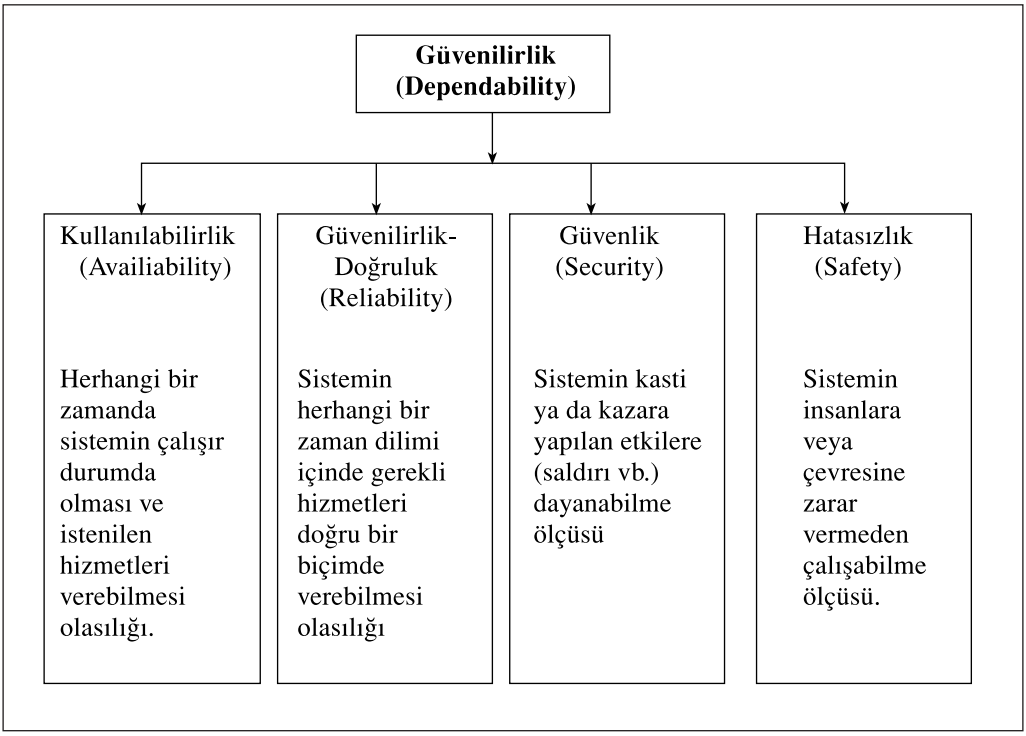
Beşinci bölümde belirtildiği gibi risk değerlendirmesinin temel aşamalarından biri, ele alınan sisteme ait deneyime ve geçmiş bilgiye sahip olmaktır, kuşkusuz geçmişte kazanılmış bilgi ve deneyim temel bir bilgi kaynağıdır. Fakat yeni veya az bilinen bir sistem sözkonusu olduğunda bu amaçla geliştirilmiş bir veya birkaç risk analizi yöntemi uygulamak gerekir.

Sistem güvenliğinin analizi için güvenirlik teorisi ve olasılık hesaplamaları çoğu risk değerlendirme yöntemi uygulamaları için büyük önem taşır. Risk değerlendirme çalışmalarını yaparken ve sistemlerin güvenlik özelliklerini değerlendirirken bu temel bilgiye mutlaka tüm İş Güvenliği Uzmanlarının sahip olması gerekmektedir.

6.1. Güvenilirlik

Güvenirliğin genel tanımı, belirli bir zaman aralığında belirlenmiş durumlarda bir bileşenin istenen fonksiyonu yerine getirme ihtimalidir. Güvenilirlik analizi, basit anlamda bir sistemin parçalarının ve birimlerinin bozulma oranlarının analizidir. Bu analizlerde kullanılan genel modeller vardır. Örneğin elektronik parçalar için MIL-HDBK-217 veya Telcordia ve mekanik parçalar için NSWC gibi. Bu modeller bize parçaların hata oranlarının hesaplanması için gerekli prosedürleri sağlarlar. Güvenililirlik analizinin temel prensipleri aşağıdaki **Şekil 3**'de verilmiştir;

Şekil 3: Güvenilirlik ve Bileşimi



Sistem, birbiri ile etkileşim halinde bulunan alt bileşenlerin oluşturduğu bir ağdır. Her sistemde bütünü oluşturan parçalar birbirlerini etkilediği gibi bütünü de etkilemektedir. Alt sistemlerden herhangi birinde aksaklık, bütüne de yansımaktadır. Sistemdeki bir durumu anlayabilmek, onu oluşturan alt sistemleri ve bu sistemlerin birbirleriyle olan ilişkilerini inceleyerek mümkün olabilmektedir. Lusser Teorisi olarak bilinen bu teoriye göre; bir sistemin başarısı onu oluşturan alt sistemlerin başarı olasılılarının çarpımına eşitir. Sistemin herhangi bir bölümünü geliştirmeden önce sistemin bütünsel amacı ve bu amacın üzerinde etkili olabilecek alt sistemler ile kararları tanımlamak gereklidir. Teorem, aşağıdaki gibi formüle edilmektedir;

$R(x) = R1 .R2. R3.....Rn$

Tüme varım kuralı da denilebilecek bu teoremin, sistemlerdeki süreç iyileştirmelerinde genel olarak kabul edilen yedi varsayımı vardır, bunlar;

1. Sistemin performansının çok iyi olması, sistemin parçalarının her birinin performansının iyi olduğunu göstermez,

2. Bir zincirin en zayıf halkasında olduğu gibi, sistemin performansını kısıtlayan elemanın belirlenmesi gerekir. Bu bir makine olabileceği gibi, yönetim politikası veya benzeri de olabilir,

3. Sistemi küçük parçalara bölerek iyileştirmek ve sonra iyileştirilmiş parçaları birleştirerek sistemin bütününü iyileştirmek mümkündür,

4. Sistemde zayıf olanın dışında herhangi bir halkayı güçlendirmeye yönelik yapılan işlemlerin, sistemin bütününü geliştirmeye bir etkisi olmaz,

5. Sistem içerisindeki istenmeyen etkilerin çoğuna birkaç ana sorun neden olmaktadır,

6. Bu ana sorunlar çoğunlukla görünür değildir. Sorunlar, "sonuç-neden-sonuç" ağıyla bağlı, istenmeyen etkiler yoluyla kendilerini göstermektedirler,

7. Sistemin her kademesinin performansını en üstte tutmak, sistemin genel performansını en üst düzeyde tutar.

Bir sistemde veya makinede ortaya çıkan arızalar, zamanında müdahale edilmezse, ikincil arızalara neden olur ve daha sonra sistemin katastrofik bir şekilde devre dışı kalmasıyla gelişir. Sistemlerde hataların ne kadar ciddi boyutta insani ve ekonomik sonuçlar doğurabileceğini ancak güvenilirlik analizi yaparak anlayabiliriz. Bir sitemin güvenilirliği ise, sistemin oluşturulması sırasındaki hatalardan kaçınmak, sistem kullanımda iken hataları belirleyip düzeltmek ve işlevsel hataların vereceği zararı kısıtlamak ile başarılabilir. Sistem güvenilirlik analizleri ile;

- Güvenilirlik ölçütlerinin belirlenmesi ve değerlendirilmesi,
- Ölçütlerin öngörülen düzeye çıkarılması için sistemin zayıf halkalarının saptanması,
- Sistemin gereksiz fazlalıklardan arındırılması,
- Farklı tasarım seçeneklerinin karşılaştırılması,
- Gerekli ek koruma ve gözetim donanımının saptanması,
- Koruyucu bakım ve ölçmelerin peryodunun belirlenmesi sağlanır.

Güvenilirlik; bir sisteme ait belirlenmiş standartlara göre verilen bir zaman aralığında amaçlanan fonksiyonlarını yapabilme olasılığıdır. Güvenilirlik fonk-

siyonu R(t), t zamanında bir sistemin (veya bileşenlerinin) kendi görevlerini yapabilme olasılığı olarak tanımlanır. Bu (t) zamanında elde edilen güvenilirlik fonksiyonu yalnızca bir olasılıktır. Güvenirlik, çoğunlukla R(t) ile ifade edilir. Burada R güvenirliği ve t ise zaman aralığını göstermektedir. Hata olasılığı F(t), sistemin veya sisteme ait bir ekipmanın bir zaman aralığının (t) aşılmasından önce bozulması ihtimalidir. Bunlar:

$$F(t) = 1 - R(t)$$

formülü ile bağıntılıdır.

Birikmiş dağılım fonksiyonu F(t), t'den daha büyük olmayan rastgele değişkenlerin rastgele deneylerdeki olasılığı olarak şu şekilde tanımlanabilir :

$$F(t) = \int_{-\infty}^{t} f(t)\, dt$$

Bu formülde olasılık yoğunluk fonksiyonu olarak verilen f(t) ise hata olasılığının negatif zaman türevidir. Hata yoğunluğu t=0 zamanından sonra ilk hatanın oluşma olasılığıdır.

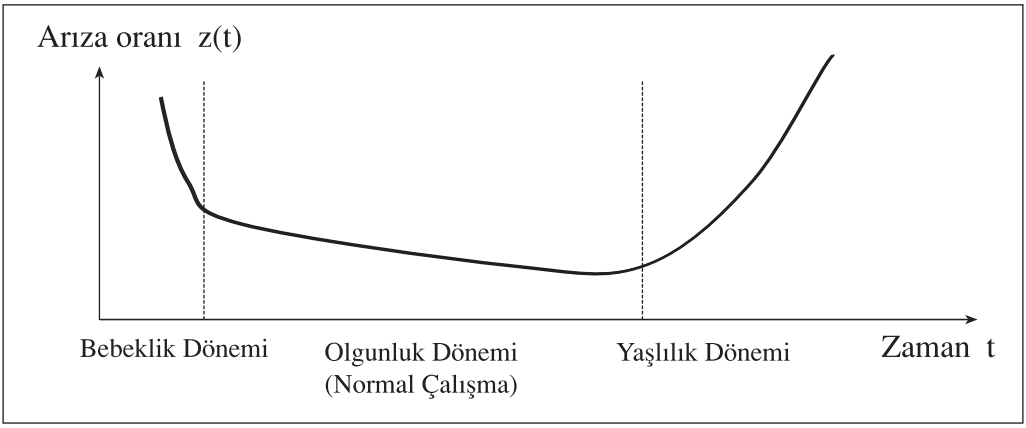
$$f(t) = -\frac{dR(t)}{dt}$$

Sistemin zamana bağlı olarak hata vermesi olarak ifade edilen bir başka önemli değişken ise, hata oranı veya arıza oranı z(t)'dir.

$$z(t) = -\frac{f(t)}{R(t)}$$

Hata oranı güvenilirlik değerlendirme çalışmaları için önemli veri sağlar, sistemin bir ömür boyunca fonksiyonunu nasıl gerçekleştirdiğini gösterir. Özellikle sistemin alt bileşenleri veya ekipmanları yeni iken; kusurlu bileşenler hızlı şekilde bozulacağı için başlangıçta hata oranı daha büyüktür. Bu aşamaya çocukluk ya da bebeklik çağı adı verilir. Bu aşamada sistemde var olan altsistem veya ekipmanların hatası izlenir ve normal çalışan bileşenler ile değiştirilir, böylece daha iyi çalışan bir sistem ve oldukça sabit hata oranı elde edilir. Zaman aralığının sonundaki hata oranının artması sistemin ömrünün bitmesinin habercisidir, bu aşamaya ise yaşlılık dönemi denir. Bu tip bozulmalar aynı zamanda "küvet eğrisi" olarak bilinir.

Şekil 4: Elektrik-Elektronik Komponentler İçin Küvet Arıza Oranı Eğrisi

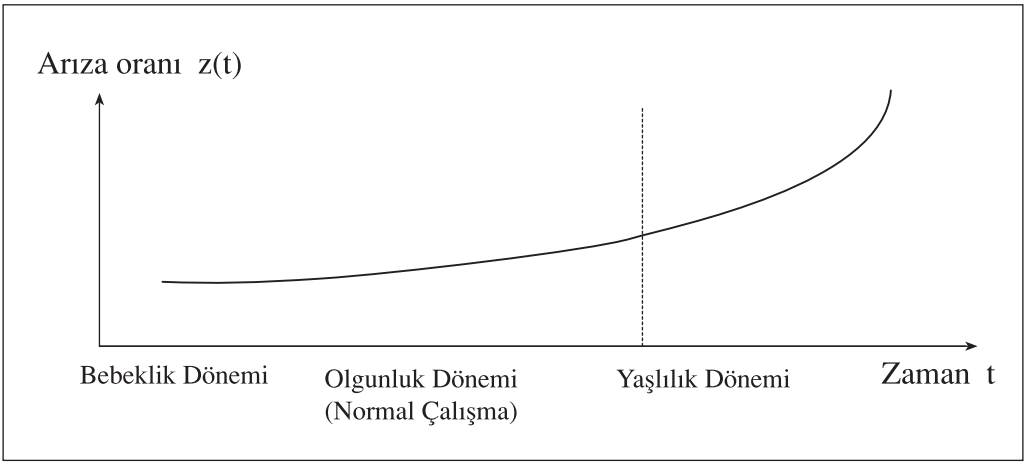


Banyo küveti eğrisi üç bölgede incelenir. Birinci bölge "bebeklik dönemi veya çocukluk dönemi" adını alır; ekipmanın kurulduğu andan itibaren yüksek bir arıza oranı gösterdiğini ve bu oranın zamanla sabitlendiğini belirtir. Bu bölge, en fazla birkaç hafta sürer ve arızalar; hatalı aksam ve parçalar, kötü lehim, bağlantı hatası vb. gibi nedenlerden kaynaklanır. İmalatçılar, ekipmanı kullanıcıya sevketmeden önce bu arızaların önceden belirlenmesi için sistemi test ederler. Tamamen hassas ölçü aletleri (enstrümantasyon) ve işlem kontrol sistemlerinde, bu arızların açığa çıkması normal bir durumdur; çünkü tasarım mühendislik hataları ve yazılım hataları genellikle bu evrede açığa çıkar.

Ortadaki bölge "Olgunluk Dönemi" adını alır, düşük değerde ve sabit bir arıza oranı gösterir. Bu süre içerisinde arızalar, rastgele meydana gelir. Sistem veya ekipmanın en verimli çalıştığı dönemdir. Genellikle "Yaşlılık Dönemi" denilen son dönem ise, giderek artan bir arıza oranı ile karakterize edilir. Bu artan güvensizlik genelde bağlantıların oksitlenmesi ve elastikiyetlerini kaybetmesi, elektrolitik kondansatörlerin kuruyup bozulması, ısıl çevrim nedeniyle endüklenen gerilim sonucunda ortaya çıkan kısa devreler gibi yapısal yaşlanma (eskime) nedeniyle meydana gelir.

Mekanik ekipmanlar, banyo küveti eğrisinden farklı bir karakteristik sergiler. Malzeme yorulması, mekanik ekipmanların arıza oranının artmasının en önemli nedenlerinden biridir. Erken dönemlerde ekipman tamamen yenidir ve arıza görülme olasılığı oldukça düşüktür. Sonraki dönemlerde yorulma ve diğer yaşlanma belirtileri ortaya çıkmaya başladıkça arıza oranı önemli ölçüde artma eğilimindedir.

Şekil 5: Mekanik Komponentler İçin Arıza Oranı Eğrisi



Eğer sabit bir aksaklık hızı λ olarak düşünülürse güvenilirlik fonksiyonu şu şekli alır. Bu denklem, güvenilirlik fonksiyonunun genel bir ifadesidir.

$z(t) = \lambda$

$R(t) = e^{-\lambda t}$

- **Seri Sistemler**

Teknik sistemler çoğunlukla birtakım bileşenlerden oluşur. Bir seri sistemden, bütün bileşenler çalışır durumda ise söz edilebilir. R1(t), R2(t), R3(t), vb. değişik alt sistemlerin güvenirlik olasılığı olarak kabul edilirse bütün sistemin güvenirliği $R_{sitem}(t)$ aşağıdaki şekilde ifade edilir:

$R_{sitem}(t) = R1(t).R2(t).R3(t)....$

Seri sistemler için, bütün sistemin hata fonksiyonu aşağıdaki şekilde ifade edilir:

$F_{sitem}(t) = 1-R_{sitem}(t)=F1(t)+ F2(t)+ F3(t).....$

- **Paralel Sistemler**

Paralel sistem bütün bileşenlerin bozulması durumunda işlemeyen sistemdir. Örneğin; birkaç lambadan oluşan ışık tesisatın aydınlatmaması için bütün lambaların bozulmuş olması gerekir. Bütün sistemin hata fonksiyonu:

F_{sitem} (t) = F1(t).F2(t).F3(t)....

Güvenilirlik tekniklerinin kullanımı, bileşenler ve sistem hata verileri ve aynı zamanda onarımı ayrılan zamanlar hakkında bilgi sahibi olmayı gerektirir. Ayrıca belirli insan tipleri hakkında veriye ihtiyaç olabilir. Veri, veri bankalarından veya teknik literatürden veya direk olarak toplanabilir. Veriye ulaşılamaması durumunda tahminler kullanılabilir. Doğruluğun düzeyi, önemli ölçüde analizin uygulamasında bağlıdır.

Hesaplamalar ileri matematiksel tekniklerin uygulanmasını gerektirebilir. Zaten, birçok zorluk verinin toplanmasında ve değerlendirilmesinde ortaya çıkar. Bir problem de teknolojinin hızlı oranda gelişmesidir. Bileşenlerin yeni versiyonları o kadar kısa zaman aralıklarında ortaya çıkar ki onların güvenirlikleri hakkında yeterli bilgi elde etmek için gereken süre yetersizdir. Sistemin kurulumuna ve hata oluşum tiplerine bağlı olarak değişik istatistiksel modeller uygulanabilir. Bazen üssel dağılımlar kullanılır, örneğin; normal dağılım veya Weibull dağılımı gibi.

Diğer anahtar kavramlar ise Arızalar Arası Ortalama Süre (MTBF) ve Arızaya Kadar Geçen Ortalama Süre (MTTF)'dir. İki kavram birbirine benzerdir ama aynı değildir. MTBF, onarım yapılan malzeme grubuna veya sisteme uygulanır. Bu, toplam operasyon süresinin gerçekleşmeme sayısına bölünmesinden türetilmiş ortalama zamandır. Bundan farklı olarak, MTTF onarılamayacak durumdaki sistemlere uygulanır.

6.2. MTTF, MTTR, MTBF ve Kullanılabilirlik

Sistemlerin veya makinelerin gelecekteki davranışlarının belirgin olmayışı nedeniyle, güvenilirliğe ilişkin indisler ancak olasılık yöntemleri kullanılarak değerlendirilebilir. Güvenilirlik ve kullanılabilirlik şeklinde tanımlanan olasılıklar güvenilirlik analizlerinin temel büyüklükleridir. Güvenilirlik analizlerinde, genellikle arızaya kadar geçen ortalama süre (ortalama çalışma süresi) MTTF, onarıma kadar geçen ortalama süre (ortalama arıza süresi) MTTR, arızalar arası ortalama süre MTBF, belirli bir zaman dilimindeki arıza sayısı, arızanın bedeli vb. temel güvenilirlik ölçütleri kullanılır. Güvenilirlikteki raslantı değişkeni zamandır, daha doğrusu arızalanma zamanıdır (x =t).

• MTTF - Arızaya Kadar Geçen Ortalama Süre (Mean Time To Failure)

Arızaya Kadar Geçen Ortalama Süre; sistemin gerekli fonksiyonlarının hepsini yerine getirdiği zamandır. Bu zaman sistemin elde edilebilirliğini ve güvenilirliğini artırır. Arıza yoğunluk fonksiyonunu grafik olarak gösterirsek,

$$MTTF = E(t) = \int_0^\infty f(t)\,dt = \int_0^\infty R(t)\,dt \text{ ile ifade edilir.}$$

• MTTR - Ortalama Tamir Süresi (Mean Time To Reapair)

Aksaklıklar yüzünden sistemin kullanılmadığı ortalama zamanı ifade eder. Bu zaman tamir için geçen süreyi ve tamircinin sistemin yanına gelmesi ile parçaları değiştirme süresini de kapsar. Diğer taraftan, arızalanan bir birimin onarım süresi de tipik çalışma süresi gibi raslantısaldır. Dolayısıyla onarım sürecine ilişkin raslantı değişkeni onarım süresi, fr(t) Onarım Yoğunluk Fonksiyonu ve Fr(t) Onarım Dağılım Fonksiyonu ile temsil edilir.

$$MTTR = E(t) = \int_0^\infty t\, fr(t)\,dt \text{ ile ifade edilir.}$$

• MTBF - Arızalar Arası Ortalama Süre (Mean Time Between Failure)

Arızalar arası ortalama süre (MTBF) verilen bir zaman aralığında, sistemin bütün parçalarının belirlenmiş görevleri yerine getirmeleri sırasında, çalışma sürelerinin ortalamasıdır. MTBF kavramına güvenilirlik literatüründe çok sık karşılaşılır; tamir edilebilir ve bozulan parçaları değiştirilerek çalıştırılabilir sistemlere tatbik edilir. MTBF aşağıdaki şekilde ifade edilir;

T(t) = toplam işletim zamanı,

r = aksaklıkların sayısıdır.

$$MTBF = \frac{T(t)}{r} \text{ Burada,}$$

MTBF= MTTF + MTTR'dir.

MTBF'nin tamir edilebilir sistemlere uygulanabilir olduğu unutulmamalıdır. Bu durumda MTBF, tam olarak ortalama ömrü temsil eder.

• **Kullanılabilirlik (Availability)**

Kullanılabilirlik bir sistemin belirlenmiş özelliklerini karşılamak suretiyle çalışacağı zamanın bir ölçüsüdür. Sistem sürekli çalıştırılacağı zaman yüksek kullanılabilirliğe sahip bir şekilde tasarlanmalıdır. Kullanılabilirlik kavramı sürekli olarak çalıştırılacak ve tamir edilebilir sistemler için geliştirilmiştir. Bir sistem, iki mümkün sürede düşünülür: işletim süresi ve tamir süresi. Kullanılabilirlik herhangi bir t zamanında bir sistemin bütün fonksiyonlarını yerine getirecek şekilde çalıştırılma olasılığı olarak tanımlanır. Yani kullanılabilirlik, güvenilirlik ve sürekliliğin bir birleşimidir. Zaman akışı içinde kullanılabilirliğin gelişimi veya ortalama kullanım düzeyi ile ilgilenilmesine bağlı olarak, iki kullanılabilirlik kavramından yararlanılmaktadır:

• Öngörülebilir anlık kullanılabilirlik,

• Ortalama kullanılabilirlik.

Tablo 1: Sistem Çalışma ve Arıza Çevrimi

	Çalışma Süresi (MTTF)	← Arıza Süresi (MTTR) →				
Sistemin Test Edilmesi	Sistemin Normal Çalışması	Arıza ve Bakımcının Çağrılması	Arıza Araştırması	Yedek Parçanın Temini	Arızanın Giderilmesi	Sistemin Test Edilmesi
	← İki Arıza Arasında Geçen Süre (MTBF) →					

Sistem gerçek bir işletim durumunda iken, salt ortalama kullanılabilirlik istatistiki olarak tahmin edilebilir. Bu değer, veri bir işletim süresi için etkin işleyiş süresi ile veri sürenin oranına eşittir. Bir sistemin kullanılabilirliği, sistemin atıl zamanı ve faal zamanı cinsinden,

$$A(t) = \frac{MTBF}{MTBF + MTTR}$$ burada,

$$A(t) = \frac{\text{Faal Zaman}}{\text{Faal Zaman + Atıl Zaman}}$$ ifadesiyle verilir.

Korunabilirlik (Maintainability):

Korunabilirlik; sistem arızalandığı zaman, arızanın giderilerek en kısa sürede tekrar işletmeye geçebilme olasılığıdır. Korunabilirlik arıza giderme süresi (MTTR) ne göre aşağıdaki bağıntıya göre hesaplanır. Sistemin korunabilirliği ile ilgili bilgilerin, sistemin tasarımcısı tarafından hazırlanan bakım prosedürlerinde yer alması gerekmektedir.

$$M(t) = 1 - e^{-t/MTTR}$$

Arıza süresi yukarıda belirtildiği gibi beş temel aşamadan oluşmaktadır. Aktif tamir ve arızanın tespit süresi, tamiri yapan kişinin eğitimi ve yeteneğine bağımlıdır. Malzemenin temini ve bakımcının bulunması gibi etkenlerden kaynaklanan gecikme, işletmenin yönetsel organizasyonuna bağımlıdır. Örneğin %90 korunabilirlik hedefi için 8 saatlik çalışma süresinde, sistemin arıza giderme süresinin (MTTR) 3,48 saat olması gerekir.

7. BÖLÜM: RİSK YÖNETİM KAVRAMI

Risk yönetimi kavramı ilk olarak 1950'lerin başlarında kullanılmaya başlanmıştır. İlk başlarda sigortacılık kavramı içerisinde değerlendirilen risk yönetimi kavramı, risk yönetiminin akademik bir disiplin olma sürecine paralel olarak değişmiş ve günümüzde kullanılan anlamını almıştır. Geçmişte risk yönetimi, sistem mühendisliğinin bir fonksiyonu olarak ele alınmaktaydı. Zaman içerisinde akademik anlamda da gelişen bu kavram şu anda mühendislik uygulamaları, askeri ve havacılık programları, finans ve sigortacılık alanlarında sıklıkla kullanılmakta ve uygulama alanı bulmaktadır.

Risk yönetim kavramı, belirsizlikleri ve belirsizliğin yaratacağı olumsuz etkileri daha kabul edilebilir bir düzeye indirmeyi amaçlayan bir disiplin ve problemlerin oluşmadan önlenmesini sağlayan proaktif bir yaklaşımdır. Avustralya standartı AS/NZS 4360:1999 (Risk Management to Managing Occupational Health and Safety Risks)'a göre risk yönetimi, iş sağlığı ve güvenliği risklerinin idare edilebilirliğidir.

ISO 17666: 2006'e göre risk yönetimi, belirlenmiş proje risk yönetimi politikasına göre yapılmış ve proje kaynaklarının sistematik ve tekrarlayan bir biçimde en iyi şekilde kullanılmasıdır. Risk yönetim politikası ise, risklere karşı kuruluşun tümünü, risk yönetiminin nasıl yürüttüğünü, kabul etmeye hazır olduğu risklerin neler olduğunu tanımlayan ve risk yönetim planının temel şartlarını tarif eden dokümandır.

IEC 60300-3-9: 2003'e göre risk yönetimi, yönetim politikalarının, prosedürlerin ve risklerin analizi, değerlendirilmesi ve kontrolü görevleri ile ilgili usullerin sistematik uygulamasıdır. IEC 62198:2003'e göre ise, yönetim politikalarının, prosedürlerin ve uygulamaların riskin tanımlanması, yol açabileceği sonuçların belirlenmesi, analiz edilmesi, değerlendirilmesi, iyileştirilmesi, izlenmesi ve iletişimine sistematik olarak uygulanmasıdır.

Risk Yönetimi - Terimler ve Tarifler standartı ISO Rehber 73: 2012'ye göre risk yönetimi, bir kuruluşu, riske ilişkin olarak yönlendirmek ve kontrol etmek için koordineli faaliyetlerdir. Risk yönetim çerçevesi ise, kuruluş çapında risk yönetimini tasarımlama, gerçekleştirme, izleme, gözden geçirme ve sürekli olarak iyileştirme ile ilgili temelleri ve kuruluşa yönelik düzenlemeleri sağlayan bileşenler kümesidir. Temeller, riski yönetmek için siyasa, hedefler, zorunluluk ve taahhüdü içerir. Kuruluşa yönelik düzenlemeler; planları, ilişkileri, sorumlulukları, kaynakları, süreçleri ve faaliyetleri içerir. Risk yönetim çerçevesi, kuru-

luşun tüm stratejik ve operasyonel siyasaları ve uygulamaları içine yerleştirilir. Risk yönetim süreci ise, işlemlerin ve uygulamaların, iletişim, danışma ve kapsam oluşturma faaliyetlerine ve riski tanımlama, analiz etme, değerlendirme, işleme, izleme ve gözden geçirilmesine sistematik olarak uygulanmasıdır.

IEC ISO 31010: 2009 standartına göre, çeşitli sektör ve büyüklükteki işyerleri, hedeflerinin gerçekleştirilmesini etkileyebilecek bir takım risklerle karşı karşıyadırlar. Organizasyonların tüm faaliyetleri, baş edilmesi gereken bazı riskler içermektedir. Risk yönetim süreci, belirsizlikler ile gelecekte yaşanabilecek olay ve durumları (planlanmış veya planlanmamış), bunların belirlenen hedefler üzerindeki etkilerini göz önünde bulundurarak karar verme sürecine yardımcı olmaktadır. Standarta göre risk yönetimi, aşağıda listelenen hususlara yönelik akılcı ve sistematik yöntemlerin uygulanmasını içermektedir:

- Söz konusu süreç boyunca iletişim ve danışmaya açık olunması;
- Herhangi bir faaliyet, süreç, fonksiyon veya ürüne yönelik bir riskin saptanması, analiz edilmesi, değerlendirilmesi ve ele alınması için belirli bir kapsamın oluşturulması;
- Risklerin izlenmesi ve incelenmesi;
- Sonuçların uygun şekilde rapor ve kayıt edilmesi.

Risk değerlendirmesi, hedeflerin olası riskten nasıl etkilenebileceğinin saptanması ve daha fazla müdahalenin gerekip gerekmediğine karar vermeden önce sonuç ve olasılıklar bakımından riskin analiz edilmesine olanak tanıyan yapılandırılmış bir risk yönetim sürecidir. ISO 31010: 2009 standartına göre risk değerlendirmesi, aşağıdaki temel sorulara yanıt bulma eğilimindedir:

- Hangi hususlar hangi sebeplerden ötürü meydana gelebilir?
- Olası sonuçlar nelerdir?
- Riskin gelecekte tekrarlanma olasılığı nedir?
- Riskin sonuçlarını hafifletebilecek veya risk olasılığını düşürebilecek herhangi bir tedbir var mı?
- Riskin düzeyi kabul edilebilir bir nitelikte midir veya daha fazla müdahale gerektirir mi?

Standartta risk yönetim çerçevesi ise, risk yönetiminin organizasyon çapında tüm düzeylere entegre edilmesini sağlayacak olan politika, prosedür ve kurumsal düzenlemeleri ortaya koymak olarak ifade edilmiştir. Organizasyon

ise, söz konusu çerçevenin bir parçası olarak risklerin ne zaman ve nasıl değerlendirileceği hususunda karar alınmasına yönelik bir politika veya stratejiye sahip olmalıdır. Genel hatlarıyla, risk değerlendirmesi faaliyetlerini yürüten kimselerin şu hususlar hakkında bilgi sahibi olmaları gerekmektedir:

Organizasyonun kapsamı ve hedefleri;

- Kabul edilebilir risklerin düzeyi ve türü ile kabul edilemez risklerin nasıl ele alınacağı,
- Risk değerlendirmesinin kurumsal süreçlere nasıl entegre edileceği,
- Risk değerlendirmesi doğrultusunda kullanılan yöntem ve teknikler ile bunların risk yönetim sürecine katkıları,
- Risk değerlendirmesinin gerçekleştirilmesi için hesap verebilirlik, sorumluluk ve yetki,
- Risk değerlendirmesini gerçekleştirilmesi için mevcut olan kaynaklar,
- Risk değerlendirmesinin nasıl rapor edilip inceleneceği.

Risk yönetimi; istenmeyen olayların ya da etkilerinin oluşma olasılığını azaltmak için risklerin planlanması, risk alanlarının değerlendirilmesi, risk azaltma faaliyetlerinin yürütülmesi, risklerin izlenmesi ve tüm risk yönetim programının dokümante edilmesi faaliyetlerini kapsar. Risk yönetimi, başka bir deyişle belirsizliklerin yönetimi olarak da adlandırılabilir.

Risk yönetimi gelecekte olması muhtemel ve sonuçları tam olarak bilinmeyen olaylarla ilgilenir. Genel olarak olayların neticesi olumlu ya da olumsuz olarak sınıflandırılabilir. Bu anlamda risk yönetimi, gelecekte olacak olayların sonuçlarının olumlu olması için, bunları planlama, değerlendirme ve yönetme sanatı olarak tanımlanabilir. Başarılı bir risk yönetiminin anahtarı erken tanımlama, planlama ve kararlı bir uygulamadır. İyi planlama; kapsamlı ve yinelenen bir yaklaşımla risk tanımlama, değerlendirme ve tepki geliştirmeyi mümkün kılar. Risk yönetimi başlı başına bir yönetim disiplinidir, ancak belirsizlikleri ve riskleri tamamen ortadan kaldıracak sihirli bir yönetim disiplini değil, potansiyel risklerin sistematik olarak değerlendirilerek, olası zararlarının etkisini azaltıcı yönde, verilere dayalı karar vermeyi sağlayan bir disiplindir ve diğer disiplinlerle bir bütünlük içerisinde uygulanması gerekir.

İşletmelerde sistemlerinin inşaa edilmesi, işletilmesi, bakımı ve yeniden yapılanması süreçlerinde başarısızlıkla karşılaşılması herzaman ihtimal dâhilin-

de olduğundan bu süreçler daima risk içermektedir. Bu sistemlerle çalışmak durumunda olan kişiler, hem operasyonel seviyede hem de yönetim seviyesinde risk yönetimine hazır olmalı ve risk yönetim kültürünü taşımalıdır. Buradan hareketle, tehlikelerin ve risklerin doğru tanımlanması, iyi ölçülmesi, doğru bir sistematik yaklaşım ile izlenmesi, sonucu ve etkisine yönelik isabetli kararların alınması için etkin bir risk yönetimi prosesi gerektirmektedir.

İş Sağlığı ve Güvenliğinde risk yönetimi, yalnızca üst yönetimin sorumluluğunda olmayıp, müdürleri, mühendisleri, formenleri, firma danışmanlarını, İşyeri Hekimi ve İş Güvenliği Uzmanları ile tüm çalışanları işin içine sokar. Organizasyonel öncellikleri belirleyen üst yönetimden, bir kazayı veya potansiyel tehlikeyi gözlemleyebilecek işçiye kadar herkesi kapsar ve taahhüdünü gerektirir.

Risklerin incelendikleri durumlar karmaşıklaştıkça ve kriterler arttıkça, karar vermek güçleşir. Karar verme mekanizmalarının çoğu, karar verme sürecinde başlangıç noktası olarak sezgi ve yargılarını kullanırlar; önemli riskler içeren kararlarda ise yargı ya da sezginin ötesine gidebilmek, ancak risk yönetiminin sistematik olarak uygulanması ile mümkündür. Riskin kritiklik derecesi ve sonuca etkisi bilinmelidir. Risk, tüm işin aksamasına neden olacaksa, kabul edilmemeli ve riskleri zararsız hale getirecek ya da tamamen ortadan kaldıracak risk azaltma planları ya da önlem planları geliştirilmelidir.

Etkin bir risk yönetimi kültürüne sahip olmak demek, insanların içinde birlikte çalışabilecekleri ve herhangi bir kayıp olmadan önce potansiyel problemleri tanıyabilecekleri ve bunları ortadan kaldırabilecekleri proaktif bir yaklaşıma sahip olmaları demektir.

Etkin bir "İş Sağlığı ve Güvenliği Risk Yönetim Kültürü" için herkesin buna gerçekten inanması gerekir. İş emniyeti önceliği hakkında yönetimden gelen istikrar sinyalleri, tehliklerin ve risklerin kontrol edilmesi ve tanınması için önemlidir. Uygun bir "Güvenlik Kültürü" nü başarmak için, bir organizasyonun risklere karşı sahip olacağı genel davranış biçiminin büyük önemi vardır.

Risk yönetimi bir organizasyonun bütün seviyelerinde uygulanabilir. Uygulama stratejik ve operasyonel seviyede yapılır.

(a) Stratejik Seviyede:

Stratejik seviyede risk yönetimi prosesi ile, iş sağlığı ve güvenliği riskerinin bir organizasyonu nasıl etkileyeceğini tespit edebiliriz. İş sağlığı ve güvenliği risk yönetiminin stratejik seviyede uygulanması ile;

- Organizasyonun iş sağlığı ve güvenliği politikasının yaratılması veya güncellenmesi,
- Bir risk temeline dayanan yaklaşımla, organizasyon için stratejik planlamanın geliştirilmesini,
- Risk yönetim kavramı içinde risk değerlendirme yönteminin belirlenmesini,
- İş Sağlığı ve Güvenliği risk kabülü kriterlerinin ayarlanması (Örneğin, ALARP mı? Yoksa ALARA mı? vb.)
- Toplum beklentilerinin karşılanabilirliği sağlanır (Toplumsal risk konturü).

(b) Operasyonel Seviyede:

Operasyonel risk yönetimi ile, bir organizasyonun sürekliliğe dayanan kararların verilmesini ve organizasyonun aktivitelerinin sonuçları konusunda bilgi verir. İş sağlığı ve güvenliği risk yönetiminin operasyonel seviyede uygulanması ile;

- Organizasyonun öncelikle dikkat gerektiren alanlarını veya iş sağlığı ve güvenliği risklerinin genel alanlarını tanımlamak için iş sağlığı ve güvenliği risklerinin bir ön incelemesinin yapılması,
- İşçilerin katılımı ile belli risklerin yönetimi,
- Belirli bir proje veya alan içinde iş sağlığı ve güvenliği risklerinin yönetimi,
- İş sağlığı ve güvenliği temeli üzerinde değişik yöntemler ve ekipmanlar arasında seçim yapılabilmesi,
- Amaçları başarmak için iş sağlığı ve iş güvenliği risklerini minimize ederek yeni projelerin planlanması,
- İstenmeyen bir kazanın muhtemel yansıması ile ilgili acil planların yapılmasının sağlanması,
- Prosedürler veya organizasyonel risk kabul kriterleri veya standartlarına uygunluğun belirlenmesi,
- İş sağlığı ve güvenliği ile ilgili faaliyetlerin performasına dair bilgilerin raporlamasına yardım için bilgi sağlanır.

7.1. Risk Yönetim Süreci

Risk yönetim süreci; planlama ve yürütme safhalarından oluşur. Planlama sürecinde, risk yönetiminin program boyunca, nasıl uygulanacağı planlanır. Risk yönetiminin yürütme aşamasında, risk yönetim planına ve risk azaltma planına göre, risk değerlendirme, azaltma, izleme ve kontrol faaliyetleri gerçekleştirilir. Bir organizasyonun tüm bölümlerinde Risk Yönetiminin uygulanması, her seviyedeki riskleri yönetecek programların tesis edilmesini gerektirir. Organizasyon içinde, "İş Sağlığı ve Güvenliği Riskleri" ile diğer risklerin karşılıklı etkileştiği ve yönetildiği bu yol göz önüne alınmalıdır. Genel olarak bir İş Sağlığı ve Güvenliği yönetim sistemine uygunluk için şu unsurlar gerekir: İş Sağlığı ve Güvenliği Politikası, Planlama, Uygulama ve Operasyon, Kontroller ve Kusur Giderici Eylemler, Yönetimce Gözden Geçirme ve Sürekli Geliştirme.

Büyük teknolojik kazaların çevre üzerindeki uzun vadeli etkileri ile neden oldukları akut saglık sorunları ve maddi hasarlar ile ilgili risklerin tamamen ortadan kaldırılması mümkün değildir, ancak iyi bir risk yönetimi ile bu olumsuz etkiler daha gerçekleşmeden engellenebilir veya sonuçlar en aza indirilebilir. Risk yönetimi süreklilik arz eden bir döngüdür. Bu yüzden her bir yeni tehlike tanımlanmasında aynı işlemler tekrar yapılmalıdır. Ayrıca alınan tedbirlerin sonuçları geri beslenerek maliyet-fayda oranının dengesi sağlanmalıdır.

Örneğin; AS/NZS 4804;2001'de tanımlanan İş Sağlığı ve Güvenliği yönetim elemanları şu anlamda tamınlanır;

- Politika ve taahhüt
- Planlama
- Uygulama
- Ölçme ve değerlendirme
- Gözlemleme ve gözden geçirme

Politikanın ve programların uygulanması ve iletişimi için yöntemler gereklidir.

7.1.1. Yetki ve Sorumluluklar

Bir organizasyonun "İş Sağlığı ve Güvenliği Yönetim Sistemi" nispeten gayri resmi veya resmi olabilir. Buna rağmen İş Sağlığı ve Güvenliği Risk Yönetimini etkileyen işlerle uğraşan personelin, yetkileri, sorumlulukları ve otoriteleri ile karşılıklı ilişkileri tanımlanmalı ve dökümante edilmelidir. Bu orga-

nizasyon içinde aşağıdakilerden birini veya birkaçını yapmakta olan kişilerin özellikle yetkileri, sorumlulukları ve otoriteleri tanımlanmalı ve dökümante edilmelidir;

- Riskin zararlı, etkilerini azaltan veya önleyen eylemleri başlatanlar,
- Risk seviyesi kabul edilir sınıra gelene kadar bir risk davranışı usulünü kontrol edenler,
- Risk yönetimi ile ilgili problemleri anlayıp kaydedenler,
- Belirlenen kanallar yoluyla çözümleri sağlayan, tavsiye eden ve başlatanlar,
- Çözümlerin uygulanmasını tasdik edenler,
- Uygun olduğunda dahili ve harici danışma ve iletişimde bulunanlar.

Dünya havacılık ve uzay endüstrisi risk yönetim kültürünün oluşmasında ve diğer endüstrilerde de uygulanmasında büyük öncülük etmiştir. Özellikle havacılıkta risk yönetimi hususunda önemli gelişmeler kaydedilmiştir. FAA, NASA ve başta A.B.D olmak üzere gelişmiş ülkelerin silahlı kuvvetleri ve sivil havacılık şirketleri, tüm uçuş faaliyetlerinde risk yönetim kültürünü faaliyetlerine yerleştirmiştir. A.B.D Federal Havacılık Otoritesinin, Sistem Güvenliği El Kitabında (Federal Aviation Authorities- System Safety Handbook,2000) özellikle risk yönetim kültürünün işyerlerinde yerleştirilebilmesi maksadıyla nasıl bir sorumluluk alınması gerektiği konusunda şu şekilde bilgi verilmektedir, buna göre;

- İşyeri Yönetim Kadrosu: Etkin risk yönetiminden, planlayıcılar tarafından önerilen risk azaltıcı tedbirler arasından tercih yapmaktan, elde edilecek faydaya göre riski kabul veya reddetmekten, risk yönetimi tekniklerini kullanmada personelin eğitilmeleri ve teşvik edilmesinden, yetkisini aşan risk kararlarını daha üst seviyelerdeki karar vericilere iletmekten sorumludurlar.
- Planlayıcılar: Riskleri değerlendirmek ve risk azaltıcı tedbirleri geliştirmekten, risk kontrol tedbirlerini planlamalara ithal etmekten ve gereksiz risk kontrollerini tespit etmekten sorumludurlar.
- Denetim Görevlileri: Risk yönetim sürecini uygulamaktan, etkili risk yönetimi yöntemlerini operasyonlara dahil etmekten ve yetkilerini aşan risk konularını, çözüm için bir üst kademeye iletmekten sorumludurlar.

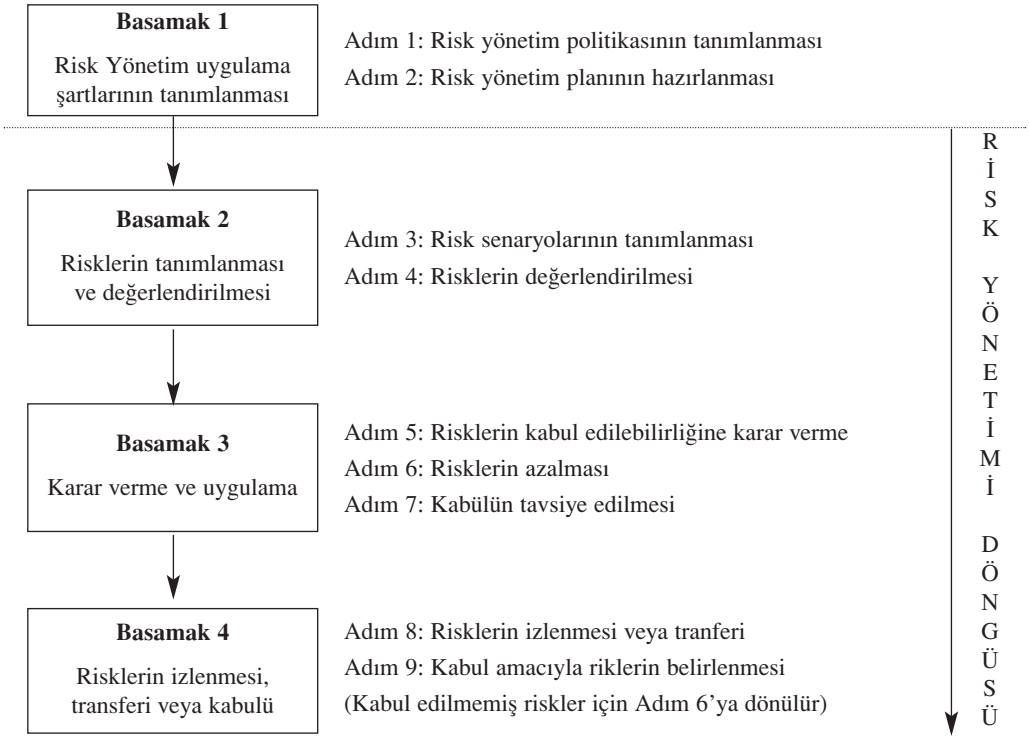
- Çalışanlar: Risk yönetimi sürecini anlamak, kabul etmek ve uygulamaktan, operasyonlara ilişkin olarak değişen risklerden her zaman haberdar olmaktan ve gerçekçi olmayan risk kontrol tedbirleri veya yüksek risk uygulamalarından yöneticileri haberdar etmekten sorumludurlar.

7.1.2. Risk Yönetim Prosesi (Risk Management Prosses –RMP)

Avustralya standartı AS/NZS 4360:1999 (Risk Management to Managing Occupational Health and Safety Risks)'a göre Risk Yönetim Prosesi; risk tanımlaması, analizi, değerlendirmesi, muamelesi, izlenmesi ve iletişimi çerçevesinin tesisi görevlerine yönetim politikalarının, prosedürlerinin ve tatbikatlarının uygulanmasıdır.

IEC 60300-3-9: 2003 standartına göre, risk yönetiminin amacı; kontrol etmek, hayat yitirilmesini, hastalık veya yaralanmaları, mala olan zararları ve önemli boyuttaki kayıpları ve çevreye olacak olumsuz etkileri önlemek veya azaltmaktır.

Şekil 6: EN ISO 17666: 2006'ya göre Risk Yönetim Döngüsü



EN ISO 17666: 2006'ya göre ise risk yönetim prosesinde, risk iletişimini ve yönetimin karar vermesini kolaylaştıracak kullanılabilir risk bilgisi üretilir ve yapılandırılır. Risk değerlendirme ve riskin azaltılmasına ilişkin sonuçlar ile artık riskler konusunda proje ekibi, bilgilendirme ve izleme amacıyla haberdar edilir.

En temel risk yönetim süreci **Şekil 6**'da gösterilmektedir. Süreç, bir sürekli geliştirme PUKO döngüsü içerecek şekilde, ilave veya değiştirilmiş risk değerlendirme kriteri ile birçok kez tekrar edebilmektedir. Risk yönteminin her bir adımı, izlenebilirliği garanti altına almak adına sonuçlar, veri kaynakları, metotlar ve kabulleri de ihtiva ederek dökümante edilmelidir.

Risk yönetim süreci; planlama ve yürütme safhalarından oluşur. Planlama sürecinde, risk yönetiminin program boyunca, nasıl uygulanacağı planlanır. Risk yönetiminin yürütme aşamasında, risk yönetim planına ve risk azaltma planına göre, risk değerlendirme, azaltma, izleme ve kontrol faaliyetleri gerçekleştirilir.

İş sağlığı ve güvenliği yönetim sisteminin temel amacı işyerlerindeki çalışma koşullarından kaynaklanan her türlü tehlike ve sağlık riskini azaltarak insan sağlığını etkilemeyen seviyeye düşürmektir, bu amaç çerçevesinde "Risk Yönetim Prosesi" iş sağlığı ve güvenliği yönetim sisteminin temel taşını teşkil eder.

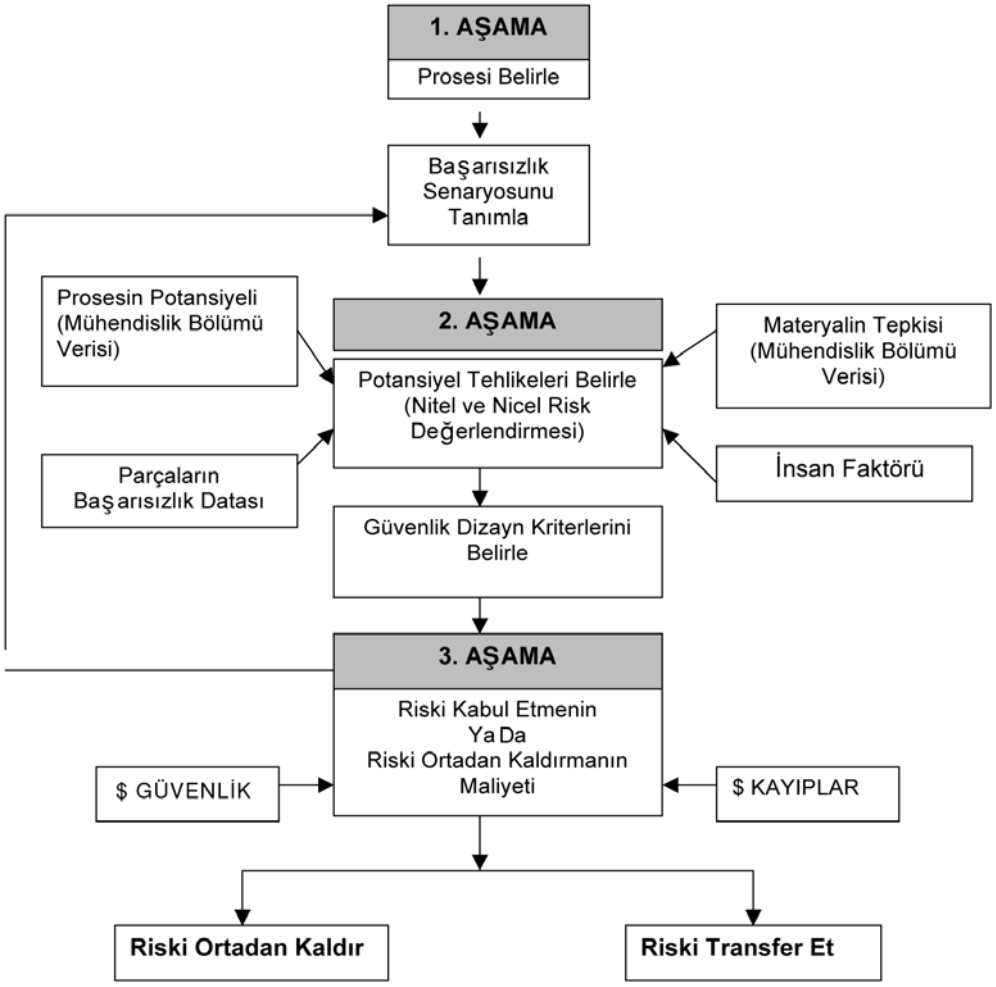
Risk Yönetim Prosesi, çok amaçlı olarak sağlık ve güvenlik yönetim sistemine biçim vermeli ve yönetim sisteminin diğer ögeleri ile tümleştirilmelidir. "Risk Yönetim Prosesi" mutlak suretle "Proses Güvenlik Yönetimi "ni dikkate almalı, böyle bir sistemde, risk yönetim prosesi işlemler veya örgütün etkinliklerindeki risklerin güncel denetimi ile uğraşan bir risk yönetim prosesi olmalıdır.

"Risk Yönetim Prosesi" ortamdaki tehlikeleri belirleyen, onların kritik değişkenler ve fonksiyonlar üzerindeki etkilerini araştıran ve koruma amaçlı mekanizma veya stratejiler geliştiren bir tekniktir. Risk yönetim Prosesinin oluşturulmasının amacı işletmelerin amaçlarına ve hedeflerine ulaşmaları için en etkin, en hızlı ve en güvenilir yolları araştırmaktır.

Risk yönetim prosesi kavramı, sistematik tanımlamayı vurgulamalı, analiz ve tehlikelerin kontrolü ise etkili ölçümler içermelidir. Risk kontrolünün neye ihtiyacı olduğunu anlamaksızın uygulanan bir risk yönetim prosesi, sağlık ve güvenlik problemleri ile savaşta doğru eylemleri içermez.

Risk Yönetim Prosesi; yönetim politikası, prosedürler ve görev tanımlarını kurma bağlamında, içerik, tanımlama, inceleme, değerlendirme, muamele, izleme ve haberleşme uygulamalarının sistematik uygulamasıdır. Risk yönetim kavramı, kazaların önlenmesi için sistematik ve gerçekçi bir çatı kurulmasını sağlar.

Şekil 7: Risk Yönetim Proses Akım Şeması



(a) İletişim ve Danışma:

ISO 31010: 2009'a göre başarılı bir risk değerlendirmesi, paydaşlar arasında etkili iletişim ve danışmaya bağlıdır. Risk yönetim sürecinde yer alan paydaşlar aşağıdaki hususlara yardımcı olacaklardır:

- İletişim planı geliştirme,
- Kapsamı uygun şekilde tanımlama,

- Paydaşlara ait menfaatlerin anlaşıldığından ve göz önünde bulundurulduğundan emin olma,
- Riski saptama ve analiz etme sürecinde farklı uzmanlık alanlarını bir araya getirme,
- Riskler değerlendirilirken farklı bakış açılarının uygun şekilde dikkate alındığından emin olma,
- Risklerin yeterli bir şekilde saptandığını güvence altına alma,
- Müdahale planı için onay ve desteği güvence altına alma.

Paydaşlar, risk değerlendirme sürecinin değişiklik yönetimi, proje ve program yönetimi ve finansal yönetim gibi diğer yönetim disiplinleri ile entegre edilmesine katkıda bulunmalıdırlar.

Çerçeveyi oluşturan alışılmış yöntemler; riskleri tanımlama, analiz etme, değerlendirme, muamele etme, izleme ve gözden geçirme sistematik olmalı ve çalışanlar, alt işverenler (belli koşullar taşımalı) ile diğer menfaat guruplarının da danışmanlığını içermelidir. Böylece herkes sonuçlara güven duyar. İş sağlığı ve güvenliği risk yönetimi ile ilgili olarak, bu adım genel olarak kanunlarla zorunlu kılınmıştır.

Etkin ve iki taraflı iletişim, zamanında raporlama iş sağlığı ve güvenliği yönetimi için önemlidir. Bunlar, risk yönetimi süreci içinde her bir adımın en önemli parçalarıdır ve bir çok davada (yargılamada) kanunen ihtiyaç duyulabilir.

Bir organizasyon, ilgili iş sağlığı ve güvenliği bilgilerinin ihtiyaç duyan herkes tarafından paylaşıldığını kanıtlamak için prosedürlere sahip olmalıdır. Bu bilgi ihtiyaçlarını belirlemek ve bu ihtiyaçların karşılandığını kanıtlamak için düzenlemeler gereklidir. Bu aşamada danışma kavramı ortaya çıkar, danışma ile çalışanlar ve diğer ilgililer bu konulara direk girmiş olurlar. Çalışanlar ve diğer ilgilerle danışmanın yararları;

- Sağlık, emniyet ile ilgili bilginin çalışanlar, müteahhitler ve ziyaretçiler ile paylaşılması,
- Çalışanlara İş Sağlığı ve Güvenliği risklerinin çözümü konularında, katkılarını ve görüşlerini belirtmek için fırsat sağlanması,
- İlgililerin görüşlerinin değerlendirilerek bu görüşlerden yararlanılması.

Çalışanlara danışma şu durumlarda mutlaka olmalıdır;

- İşyerinde, iş metodu veya sisteminde, kullanılan maddelerde değişiklik olduğunda,
- Sağlık ve emniyet riskleri değerlendirildiğinde,
- Riskleri indirgeyen veya elimine eden tedbirler hakkında kararlar verildiğinde,
- Risklerin izlenmesi için prosedürlerde değişiklik veya yenileme olduğunda,
- Çalışanların refahı için tesisler ile ilgili kararlar verildiğinde,
- Danışma prosedürleri hakkında kararlar verildiğinde,
- Yeni bilgiler gündeme geldiğinde danışma yapılmalıdır.

Danışma mekanizması;

- İş Sağlığı ve Güvenliği Kurulu,
- İş Güvenliği Uzmanı veya İşyeri Hekimi,
- İş Sağlığı ve Güvenliği İşçi temsilcileri vasıtasıyla oluşturulabilir.

(b) Çerçevenin Tesisi:

Bu adım, organizasyonun genel stratejik pozisyonunu göz önüne alarak riskin yönetimi yolu için şartları ayarlar. Bir organizasyonun, risk yönetimini neden kabul ettiğini stratejik bir bakış açısından tanımlar. Riskleri organizasyonun çerçevesi olan kültür, değerler, iş ihtiyaçları vs. bakımından izleyerek, çalışma yeri içinde iş sağlığı ve güvenliği riskinin alt yapısını ihtiva eder.

Çerçevenin tesisi ile iletişim ve danışma politikaları tanımlanır. Çalışanların iş sağlığı ve güvenliği riskleri, organizasyonun yönetmesi gereken birçok çeşit riskten biri olacaktır. İş sağlığı ve güvenliği riskleri ile diğer risk alanları arasındaki bağların tespitine ihtiyaç vardır. Bu ön adımda bilgiler tanımlanır ve "İş Sağlığı ve Güvenliği Risk Yönetim Programı" planlanır.

Riskin yönetimindeki ilk adım, organizasyonun bütünü ile ilgili bilgilerin toplanması ve kararların verilmesidir. Bu bilgiler stratejik, organizasyonel ve risk yönetimi meseleleri olarak ele alınır. Çerçevenin tesisi; organizasyonun ve işletmenin güçlü ve zayıf yönlerinin, tehlikelerinin, fırsatlarının ve tehditlerinin tanınması ve organizasyonla çevresi arasındaki ilişkinin tanımlanması ile oluşturulur.

ISO 31010: 2009'a göre çerçevenin oluşturulması; risklerin üstesinden gelinmesi ve sürecin geri kalanına yönelik kapsam ve kriterlerin belirlenmesi konusunda temel parametreleri ortaya koymaktadır. Çerçevenin oluşturulması,

bütünüyle organizasyona ilişkin olan iç ve dış parametreler ile ve geçmişte değerlendirilmesi yapılmış belirli risklere ait arka planının göz önüne alınmasını içerir.

Çerçeve oluşturulurken; risk değerlendirme hedefleri, risk kriterleri ve risk değerlendirme programı belirlenir ve kararlaştırılır. Belirli bir risk değerlendirmesi için çerçeve oluşturulması, iç ve dış kapsam ile risk yönetim kapsamının ve risk kriterleri sınıflandırmasının tanımlanmasını gerektirmektedir:

a) Dış kapsamın oluşturulması, organizasyon ve sistemin faaliyet gösterdiği çevre ile aşina olunmasını gerektirir. Bu unsurlar arasında:

- Uluslararası, milli, bölgesel ya da yerel tabiata bakılmaksızın kültürel, siyasi, yasal, düzenleyici, finansal, ekonomik ve rekabetçi çevre,
- Organizasyonun hedefleri üzerinde etkili olan başlıca faktör ve eğilimler,
- Dış paydaşların algı ve değerleri bulunmaktadır.

b) İç kapsamın oluşturulması, aşağıdaki unsurların anlaşılmasını gerektirmektedir:

- Kaynak ve bilgi bakımından organizasyonun yeterlilikleri,
- Bilgi akışı ve karar verme süreçleri,
- İç paydaşlar,
- Başarılması gereken mevcut hedef ve stratejiler,
- Algılar, değerler ve kültür,
- Politika ve süreçler,
- Organizasyonca benimsenmiş standartlar ve referans modeller,
- Yapılar (örn; yönetim, roller ve sorumluluklar).

c) Risk yönetim sürecinin kapsamının oluşturulması, aşağıdaki unsurları kapsar:

- Hesap verilebilirliğin ve sorumlulukların tanımlanması,
- Devreye alma ve kapsam dışı bırakma hususundaki özel faaliyetler de dahil olmak üzere yürütülecek risk yönetim faaliyetlerine ait düzeyin belirlenmesi,

- Süre ve yer bakımından proje, süreç, fonksiyon ya da faaliyet düzeyinin belirlenmesi,
- Organizasyonun belirli bir proje ya da faaliyeti ile diğer proje ve faaliyetleri arasındaki ilişkinin saptanması,
- Risk değerlendirme yöntemlerinin belirlenmesi,
- Risk kriterlerinin belirlenmesi,
- Risk yönetim performansının nasıl değerlendirileceğinin saptanması,
- Atılması gereken adımlara yönelik karar ve faaliyetlerin tanımlanması ve belirlenmesi,
- İhtiyaç duyulan kapsam belirleme veya çerçevenin düzeyinin, hedeflerin ve bu tür çalışmalar için gereken kaynakların tanımlanması.

d) Risk kriterlerinin tanımlanması şu hususlar hakkında karar verilmesini gerektirmektedir:

- Karşı karşıya kalınacak sonuçların tabiatı, türü ve nasıl ölçüleceği,
- Olasılıkların ifade edilme yöntemi,
- Risk düzeyinin nasıl saptanacağı,
- Riske müdahale edilmesi gerektiğini ifade eden kriterler,
- Riskin hangi koşullar altında kabul edilebilir ve/veya tahammül edilebilir olduğuna karar verilmesini sağlayan kriterler,
- Risk kombinasyonlarının hesaba katılıp katılmayacağı ve nasıl ele alınacağı.

Söz konusu kriterler, şu kaynaklara dayalı olabilir:

- Kararlaştırılan süreç hedefleri,
- Şartnamelerde tanımlanan kriterler,
- Genel veri kaynakları,
- Güvenlik bütünlüğü düzeyleri gibi genellikle kabul gören endüstri kriterleri,
- Özel bir donanım veya uygulamaya yönelik yasal ve diğer gereklilikler.

(c) Tehlikelerin Tespiti ve Risklerin Tanımlaması:

İş Sağlığı ve Güvenliği risklerinin tanımlaması, kayıp veya zarara neden

olacak potansiyele sahip her şeyin tanımlanmasını gerektirir. Zararın esas kaynağının da (Tehlike Kaynağı) tanınması yani hastalık ve sakatlanma neticesine nelerin sebeb olabileceğinin tanınması gerekmektedir.

ISO 31010: 2009'a göre risk tanımlaması, risklerin saptanması, farkına varılması ve kayıt altına alınması sürecidir. Risk tanımlamasının amacı, sistem veya organizasyona ilişkin hedeflerin gerçekleştirilmesini etkileyebilecek ne gibi durumların baş göstereceğini ve nelerin yaşanabileceğini saptamaktır. Risk tanımlandığında organizasyonun yapması gereken şey, tasarım özellikleri, insanlar, süreçler ve sistemler gibi mevcut kontrolleri belirlemektir. Risk tanımlama yöntemleri arasında:

- Kontrol listeleri ve geçmiş verilerin incelenmesi gibi delile dayalı yöntemler,
- Yapılandırılmış bir dizi ipucu veya sorular yoluyla uzman ekibinin riskleri tanımlamaya yönelik sistematik bir süreç izlediği ekip yaklaşımları,
- Örneğin; HAZOP gibi tümevarımsal sorgulama teknikleri bulunmaktadır.

Risk tanımlama sürecinde doğruluk ve bütünlüğü geliştirmek adına beyin fırtınası ve Delphi yöntemi gibi birçok destekleyici teknik kullanılabilmektedir. Risk tanımlanırken uygulanan edimsel tekniklere bakılmaksızın, zamanında farkına varma hususunun insanlara ve kurumsal faktörlere bağlı olduğu üzerinde durulması gereken önemli bir konudur. Dolayısıyla, insan ve kurumsal faktörlerde beklenenin dışında gerçekleşen sapmalar, "donanım" ve "yazılım" vakaları ile birlikte risk tanımlama sürecine dahil edilmelidir.

ISO 31010: 2009'a göre risk değerlendirmesi; risk tanımlaması, risk analizi ve risk tespitine yönelik geniş kapsamlı bir süreci ifade eder. Riskler; projeler, bireysel faaliyetler veya özel riskler için kurumsal düzeyde ve bölüm bazında değerlendirilebilir. Farklı bağlamlarda farklı araç ve teknikler uygun olabilir. Risk değerlendirmesi; risklerin ve söz konusu risklere ilişkin neden, sonuç ve olasılıkların kavranmasına olanak tanır. Ayrıca aşağıdaki hususlar çerçevesindeki kararlara çeşitli veriler sunar:

- Herhangi bir faaliyet yürütmenin gerekli olup olmadığı,
- Olanakları en üst düzeye çıkama yolları,
- Risklere müdahale etmenin gerekli olup olmadığı,

- Farklı türde riskler söz konusu olduğunda seçenekler arasından tercih yapma,
- Risk müdahale seçeneklerini öncelik sırasına koyma,
- Olumsuz riskleri kabul edilebilir düzeye getirecek risk müdahale stratejilerinden en uygun olanlarını seçme.

Risk yönetim sürecinde risklerin tanınması temel olarak beş adımdan oluşur:

- Risk tanımlaması,
- Risk analizi,
- Risk değerlendirmesi,
- Risk azaltma kararının verilmesi ile kontrol tedbirlerinin uygulanması,
- Denetleme ve değerlendirme.

Bu sürecin ilk iki aşamasında tehlike tanımlama ve risk analizi yapılır. Birinci aşamada, görevin icrasında karşılaşılabilecek her türlü tehlikeli durum tespit edilir ve her tehlikenin işleyişe tesiri saptanır.

Risklerin tanımlaması aşaması, risk yönetiminin en önemli adımıdır ve diğer aşamalardan farklıdır. Sistem veya organizasyon içerisindeki potansiyel zarar veya hasar yaratabilecek etkilerin objektif olarak analiz edilmesidir. Risklerin tanımlanması aşaması için birçok analitik metod geliştirilmiştir. Uygun metod ya da çeşitli metodların birlikte kullanımı prosesteki tehlikelerin kapsamının sistematik olarak daha iyi anlaşılmasını sağlar. Tehlikelerin belirlenmesi, risklerin değerlendirilmesi ve gerekli kontrol ölçümlerinin yapılması için işletmede; ölüme, hastalığa, yaralanmaya, hasara veya diğer kayıplara sebebiyet verebilecek tüm istenmeyen olaylar tanımlanır.

Öncelikle işletmenin/işyerinin risk haritasının çıkartılması gerekmektedir. Risk haritası oluşturulurken işyeri sağlık ve güvenlik biriminde çalışan tüm mühendis ve tekniker kadro, İş Güvenliği Uzmanı ve İşyeri Hekiminin birlikte çalışması, meslek hastalığı ile iş kazaları için iki ayrı risk haritasının çıkartılması gerekmektedir.

Tehlikelerin belirlenmesi için tipik girdiler;

- İş Sağlığı ve İş Güvenliği'ne ilişkin hukuki ve diğer şartlar (mevzuat),
- Ön gözden geçirme sonuçları,

- Çalışanlar ve diğer ilgili taraflardan alınan bilgiler,
- Çalışanlardan elde edilen İSG bilgileri, işyerindeki gözden geçirme ve iyileştirme faaliyetleri (bu faaliyetler özelliği itibariyle reaktif yada proaktif olabilir)
- İSG politikası ,
- Kaza ve olay kayıtları,
- Uygunsuzluklar,
- Denetim sonuçları,
- İletişim belgeleri,
- En iyi uygulamalar hakkındaki bilgiler,
- Kuruluşa özgü tipik tehlike riskleri, benzer kuruluşlarda olmuş olan kaza ve olaylar,
- Elektrik kullanımı,
- Kuruluşun tesisleri, prosesleri ve faaliyetleri hakkında bilgiler,
- Saha planları,
- Radyasyon kaynakları,
- Yangın,
- Proses akış şemaları,
- Makina, ekipman v.b. bilgiler,
- Malzeme envanterleri (ham maddeler, kimyasallar, atıklar, ürünler ve alt ürünler),
- Toksikoloji ve diğer sağlık ve iş güvenliği verileri,
- Verilerin izlenmesi,
- Kimyasal ve biyolojik maddeler,
- Malzeme Güvenlik Bilgi Formları (MSDS),
- Yöntemler, görevler,
- İnceleme Raporları,
- Profesyonel destek, uzmanlık
- Tıbbi/ilk yardım raporları,
- Sağlık Riskleri taramasıdır.

Yukarıda verilen tipik girdiler tehlikelerin belirlenmesi amacıyla değerlendirilir. Bu değerlendirme sonucunda yaralanma, kayma, düşme, ölüm, malzeme düşmesi, meslek hastalığı, makine - ekipman zararları, kimyasal maddelerle temaslar, yangın, patlama v.b. tehlikeler tanımlanır ve bu tanımlamalara göre işyerinin "Risk Haritaları" ve "Bilgi Bankaları" oluşturulur.

(d) Risklerin Analizi:

Tehlikelerin tanımlanmasından sonra, tehlikelerin doğasının, mekanizmasının ve dikkate değer tehlikelerin sonuçlarının anlaşılması için de çeşitli metodlara ihtiyaç vardır. Bu bilgiler ışığında çeşitli tehliklerle karşı karşıya kalabilecek çalışanların korunması sağlanabilir.

Mevcut kontroller çerçevesi içinde, olasılık ve sonuç bakımından riskler analiz edilir. Bu aşamada bir risk seviyesi tahmini üretmek için olasılık ve sonuç tahmini yapılır. Risk analizi yapmak için birçok metedoloji mevcuttur, bunlardan en uygun olanı seçilir. Risk analizi, kalitatif, kantitatif veya yarı kantitatif metedolojilerin kullanımı ile gerçekleştirilir.

Risk analiz aşamasının değişkenleri olasılık ve etki yani şiddettir. Daha sonraki adımlarda risklerin etkin yönetimi gerçekleştirilir. Yürütme aşamasında da uygulamada olduğu gibi, devamlı olarak işleyişe etki edecek riskler değerlendirilmelidir. Tehlikenin insan, ekipman veya teşkilat üzerinde gösterebileceği potansiyel etkinin büyüklüğünün tespiti son derecede önemlidir. Etki değerlendirmesi, gerçekçi olarak, beklenebilecek en kötü sonuç temeline dayandırılarak yapılmalıdır.

(e) Riskleri Değerlendirme:

Risk seviye kabul edilebilirliğinin önceden tesis edilmiş kriterleri ile kıyaslaması yapılır. Uygulama prosedürlerinde veya standartlar içinde bulunan kriterler kullanılır ve eylem gerektirip gerektirmediği hakkında karar verilir. Tedbir alınmasını gerektiren riskler, tedbir alınmak üzere önceliğinin tanınması için sıralanır.

Riskler değerlendirilir, derecelendirilir ve gerekli kontrol ölçümlerinin yapılması için prosedürler oluşturulur, risk seviyelerinin kabul edilebilirliğinin önceden tesis edilmiş kriterler ile kıyaslaması yapılır. Kalan riskin katlanılabilirliğinin değerlendirmesi, ihtiyaç duyulan her ilave risk kontrol önleminin belirlenmesi, risk kontrol önlemlerinin riski katlanılabilir bir seviyeye indirmeye yetip yetmeyeceğinin değerlendirilmesi yapılır. Risk değerlendirmesi aşamasın-

da, riskin kabul edilebirliğine karar vermek için, riskin önemi üzerinde kapsamlı olarak karar verilir.

Riski tahmin etmenin temelinde, risk değerlendirmesi, riskin kabul edilebilir düzeyde olup olmadığını belirleme yada ilave risk ölçümleri ile riski kabul edilebilir düzeye indirgemek maksadıyla uygulanır. Risk değerlendirmesi, çok fazla sübjektif yargılara dayanır. Risk değerlendirmesi aşamasında, olayların ortaya çıkma olasılığı ve ortaya çıktığında maruz kalınabilecek sonuçlar belirlenir.

(f) Risk Azaltma Kararının Verilmesi, Kontrol Tedbirlerinin Uygulanması:

ISO 31010: 2009'a göre risk düzeyi, mevcut kontrollerin yeterliliği ve verimliliğine dayalı olacaktır. Yönlendirilmesi gereken sorular arasında şunlar bulunmaktadır:

- Belirli bir riske yönelik mevcut kontroller nelerdir?
- Söz konusu kontroller riskin kabul edilebilir bir düzeye getirilebilmesi için riske yeterli şekilde müdahale edebiliyor mu?
- Uygulama bakımından kontroller planlandığı şekilde mi uygulanıyor ve başvurulduğunda etkili olduğu kanıtlanabiliyor mu?

Yukarıdaki sorular, yalnızca düzenli bir dokümantasyon ve süreçler mevcut ise güvenli bir şekilde yanıtlanabilir.

Belirli bir kontrolün verimlilik düzeyi veya ilgili kontrollerin uygunluğu niteliksel, yarı niceliksel ya da niceliksel şekilde ifade edilebilmektedir. Çoğu durumda yüksek bir kesinlik düzeyi garanti edilememektedir. Ancak, herhangi bir kontrolün geliştirilmesi veya farklı bir risk müdahalesinin benimsenmesi adına tüm çabanın sarf edildiğine yönelik yargılarda bulunmak için risk kontrol verimliliğinin düzeyini açıklayıp kayıt altına almak önemli bir adım olabilir. Bu aşama, risk ile alakadar olmak için alınacak tedbirlerin seçeneklerini tanımlamayı, en iyi eyleme kadar vermeyi, bir plan hazırlamayı ve bunun nasıl izleneceğini tanımlamayı ihtiva eder. İş sağlığı ve Güvenliği çerçevesi içerisinde, makul uygulanabilir bir "Kontrol Hiyerarşisi" takip edilerek riskler en düşük seviyeye getirilmelidir.

Değerlendirilen risklerle ilgili alınacak önlemler tartışılır. Riskin ortaya çıkma ihtimalinin önlenmesi, azaltılması veya hasarın potansiyel şiddet derecesinin azaltılması yada tehlikenin transfer edilmesinin maliyet analizi yapılır. Riskler, normalde bir yada birkaç güvenlik ölçümü ile azaltılabilirler. Risklerdeki

azalma, ya sonucu üzerinde, yada gerçekleşme olasılığı üzerinde olur. Kontrol ölçümleri, "Mühendislik Kontrolü" veya "Yönetimle İlgili Kontroller" vasıtasıyla yapılabilir. "Mühendislik kontrolleri" korunma yolları, bariyerler ve diğer tesisatlar gibi donanımlara başvurur. "Yönetimle İlgili Kontroller" ise güvenli çalışma prosedürleri, güvenlik sistemleri gibi yazıların yayımlanması yoluna başvurur. Kontrol önlemlerini tespit etme aşamasında "Riskleri Ortadan Kaldırma Planı" hazırlanır, bu plan kontrol önlemlerinin hiyerarşisi izlenerek yapılır.

(g) İzleme ve Gözden Geçirme:

Risk yönetiminin işlemi yukarıda belirtilen aşamalar çerçevesinde gerçekleşir. Ancak bazı tehlikeler gözden kaçırılabilir veya yeniden tanımlamaya ihtiyaç duyulabilir, yeni tehlikeler zaman içinde ortaya çıkabilir ve tüm işlemlerin tekrarlanması gerekebilir. Pek az iş sağlığı ve güvenliği riski değişim göstermez, zaman içerisinde ilave bilgilerin gün ışığına çıkması ile risk yönetim döngüsünün düzenli olarak gözden geçirilmesine ihtiyaç vardır. Uygun kontrol ölçümleri uygulandıktan sonra, daha önceden tespit edilmiş tehlikelerin artan risk değerlerinin kabul edilebilirliklerini değerlendirmek için yeniden değer biçmeye ihtiyaç duyulabilir.

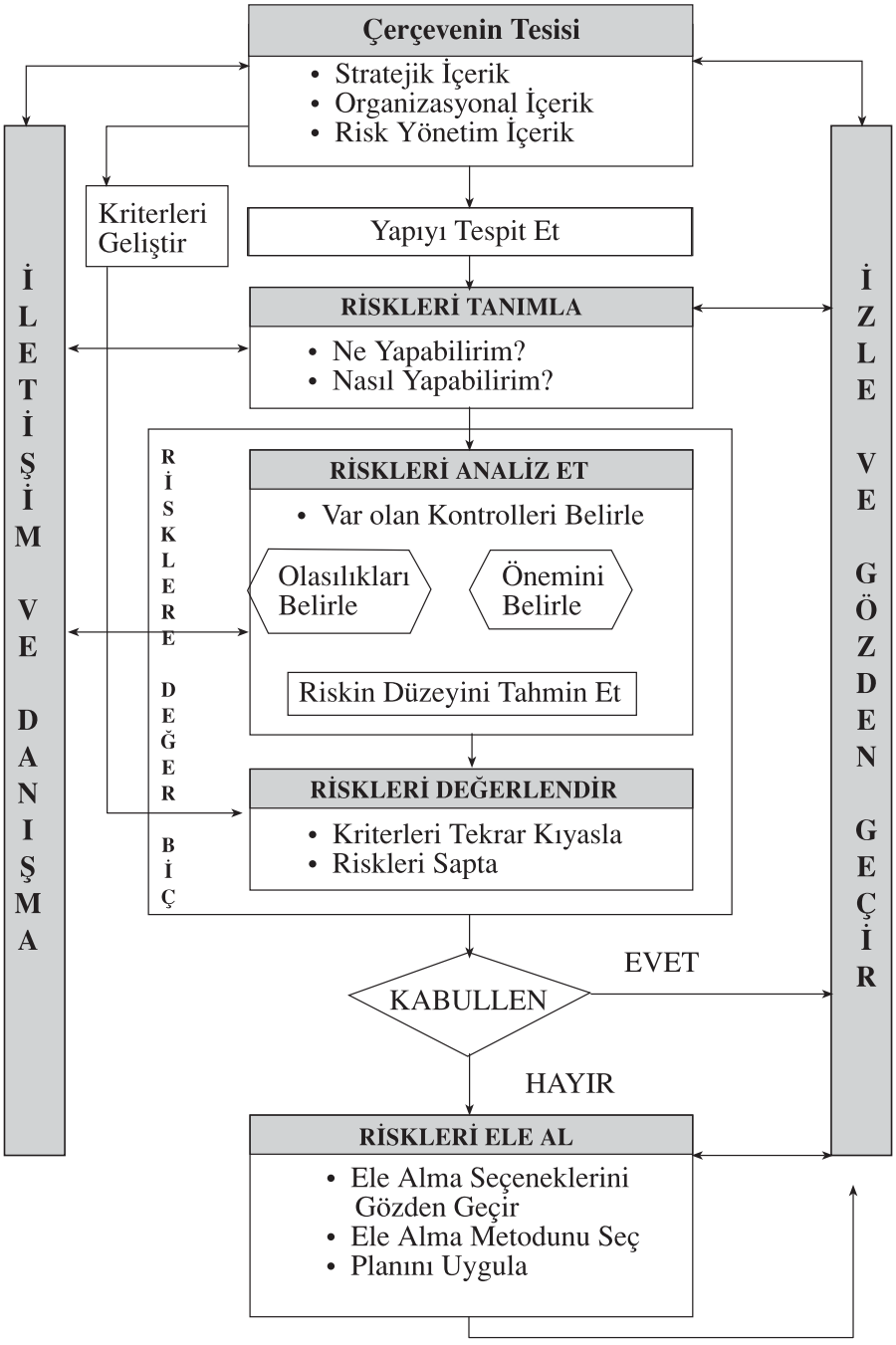
Riskin seviyesini etkileyecek muhtemel faktörlerde veya çerçevelerde, örneğin; malzeme, iş yeri, yöntemler veya metotlarda değişiklik olduğu durumlarda, düzenli gözden geçirme gereklidir. Denetimler ve İş emniyeti kontrollerinde olduğu gibi aktivitelerin gözden geçirilmesi ve izlenmesi sıklığı ve çeşidi ile ilgili belli kanuni gereksinimler varsa buna göre uygulama yapılır.

ISO 31010: 2009'a göre riskler ve kontroller, risk yönetim sürecinin bir parçası olarak aşağıdaki hususların doğrulanabilmesi için düzenli aralıklarla gözlemlenmeli ve incelenmelidir:

- Risklere yönelik varsayımlar geçerliliğini korumakta mıdır?
- İç ve dış bağlam da dahil olmak üzere risk değerlendirmesinin dayalı olduğu varsayımlar geçerliliğini korumakta mıdır?
- Beklenen sonuçlar elde edilmiş midir?
- Risk değerlendirmesine ilişkin sonuçlar, gerçek tecrübeler ile aynı doğrultuda mıdır?
- Risk değerlendirme teknikleri, gerektiği şekilde uygulanmış mıdır?
- Risk müdahaleleri etkili bir nitelik taşımakta mıdır?

Ayrıca gözlemleme ve incelemeye yönelik sorumluluklar oluşturulmalı ve tanımlanmalıdır.

Şekil 8: Risk Yönetim Prosesi



Riskin belirlenmesi, risk değerlendirme ve kontrol önlemlerinin ardından; riski ortadan kaldırmaya/azaltmaya yönelik gerekli faaliyetin zamanında tanımlanmasının izlenmesi ve gözden geçirilmesinin de mutlaka yapılması gerekir. Alınan önlemler sonucunda risk kontrol proseslerinde de değişiklikler olabileceğinden geriye kalan risklerin yeni durumlarını belirlemek amacıyla risk değerlendirmesinin yapılması gekebilir, bu nedenlede tutulan tüm kayıtların analizlerinin yapılması gereklidir.

Sonuçlar, düzeltici/önleyici faaliyetlerin tanımlanması, konu ile ilgili gelişmeler, değişiklik yapılan veya yeni İş Sağlığı ve Güvenliği amaçlarının oluşturulması için girdi sağlanması amacıyla yönetime bilgi verilmeli, ayrıca bilgi toplama aşamasında alt işverenlerde dahil olmak üzere tüm grublarla iletişim ve danışma kurulmalıdır.

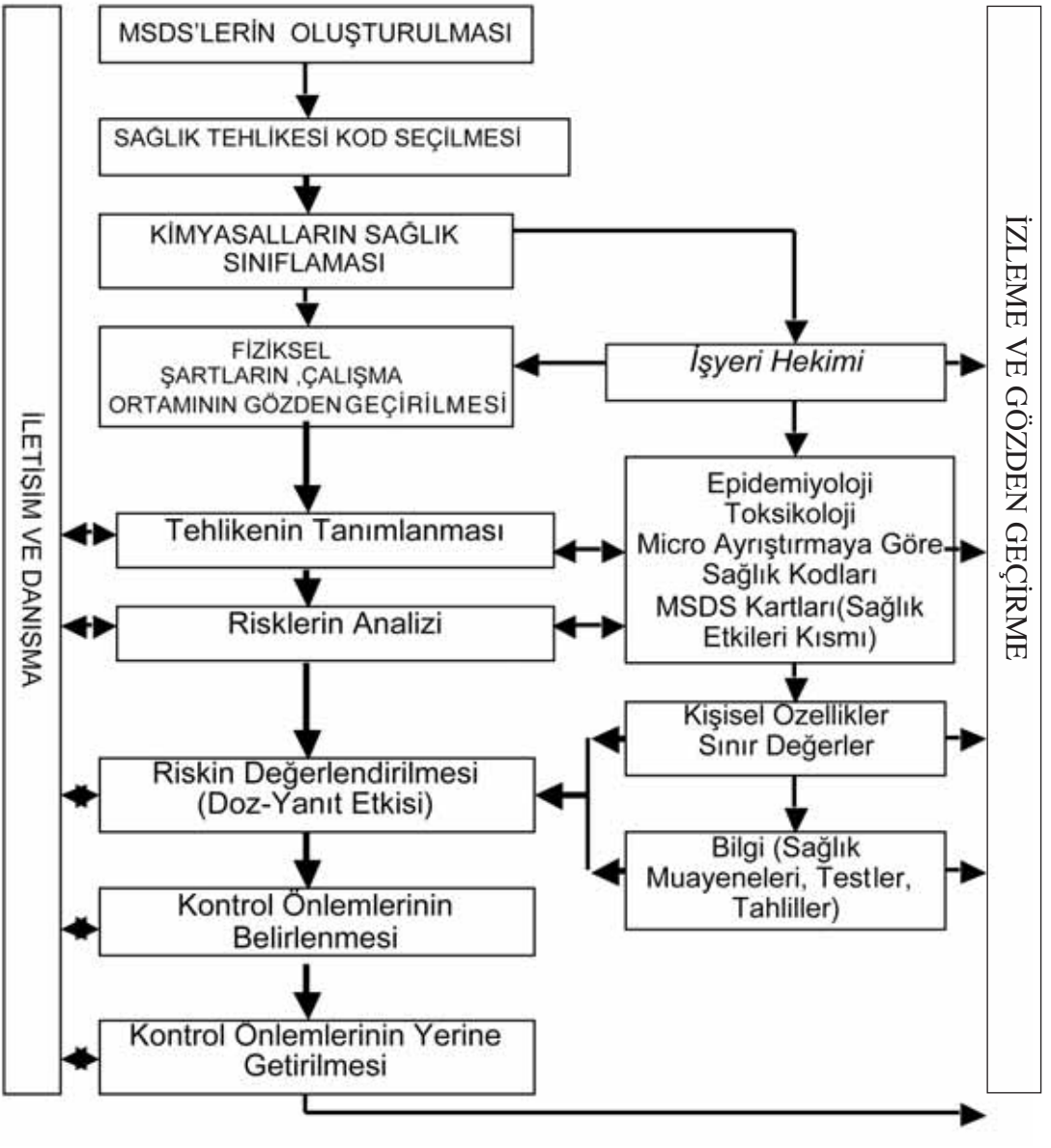
7.1.3. Kimyasallarla Çalışmada Meslek Hastalığı Risk Yönetim Prosesi

Meslek hastalıklarının kontrolü için Risk Yönetim Prosesinin uygulanması özellik arzetmektedir. Meslek hastalıklarının kontrolünün sağlanabilmesi için İşyeri Hekiminin risk değerlendirme takımında aktif olarak görev alması gerekmektedir.

İşyerlerinde kimyasallarla gerçekleştirilen faaliyetlerde, "Meslek hastalığı Risk Yönetim Prosesi" nin kurulması aşamasında, ilk adım olarak öncelikle işletmede/işyerindeki tüm kimyasalların Malzeme Güvenlik Bilgi Formlarının oluşturulması gerekmektedir. Ancak bu formların oluşturulması da yeterli değildir, ikinci adım olarak bu kimyasalların sınıflandırılması ve işletmede görev yapan teknik ekip tarafından bu Malzeme Güvenlik Bilgi Formlarının parçalanarak sağlık etkisi ve ilk yardım ile ilgili kısımlarının İşyeri Hekimine verilmesi gerekmektedir. Ayrıca İşyeri Hekimi özellikle işletmenin risk haritası oluşturulurken bu çalışmalara bir fiil katılarak micro ayrıştırmanın yapılmasında, meslek hastalıkları konusunda teknik ekibe bilgi vermelidir. Kimyasallarla yapılan faaliyetlerde uygulanması uygun olan "Meslek Hastalığı Risk Yönetim Prosesi"nin aşamaları **Şekil 9**'da verilmiştir.

Risk yönetimi aşamasında işyeri çalışma koşulları, kullanılan kimyasallar ve çevresel etkiler nedeniyle oluşabilecek meslek hastalıkları belirlenmeli ve risk değerlendirmesi yaparken ortaya çıkan risk değerinin kabul edilir olup olmadığına karar verilmeli ve ortaya çıkan risk değerinin azaltılması için gerekli kontrol önlemleri seçilerek sürekli olarak sağlık muayeneleri, testler ve tahlillerle izlemesinin yapılması gereklidir.

Şekil 9: Meslek Hastalığı Risk Yönetim Prosesi



8. BÖLÜM: RİSK DEĞERLENDİRMESİ MEDOLOJİLERİNİN SEÇİM KRİTERLERİ

Bir işletmede risk değerlendirme yöntemlerinin seçim aşaması en önemli aşamadır, bu seçimin yanlış yapılması işletmede maddi ve manevi kayıplara neden olucaktır. Verilen her kararda, kişisel yargı, sezgi ve deneyimin etkisi her zaman vardır, risk değerlendirme tekniklerini de kullanırken kişisel bilgi, yargı, sezgi ve deneyimin birleşirilmesi gerekir.

Risk değerlendirme tekniklerini ne tümüyle teknik bilgi kullanarak ne de yalnızca kişisel yargı, sezgi ve deneyime dayalı olarak yürütmek uygun değildir. Önemli olan husus, risk değerlendirme metodolojilerini kullanırken etkinliği artırmak, sübjektifliği azaltmak için yaygın ve etkin bir şekilde olasılık ve güvenilirlik teorilerinden yararlanmaktır. Düşük düzeydeki teknolojiye sahip olan ve karmaşık olmayan sistemler için kişisel deneyim, sezgi ve yargılar ile risk değerlendirme çalışmaları yapılabilir.

Ancak orta düzeyde karmaşıklığa sahip bir sistemde oluşabilecek tehlikelerin etkileri ile bu tehlikelerin ortaya çıkma olasılıkları konunun uzmanı kişilerin görüşlerinden ve deneyiminden faydalanılarak belirlenmelidir. Yüksek riskli ve karmaşık sistemlerde ise ortaya çıkabilecek tehlikelerin yönetilmesi için disiplinli bir şekilde teknik bilgi ve deneyime ihtiyaç duyan risk değerlendirme tekniklerinin ve olasılık ve güvenilirlik teorilerinin kullanılması gerekir.

Modern endüstride karşılaşılan sistemler; çoğunlukla çok sayıda ve birbirleri ile ilişkilerinin saptanması genelde zor olan alt sistemlerden oluşmaktadır. Risk değerlendirmesine ilişkin tekniklerin kullanılması halinde, analizi yapan analisti sistem yaklaşımı içerisinde altsistemleri de incelemeye iter ve özel durumlardaki keyfi kesilmeleri ve sapmaları da tahmin etmeye zorlanır. Sonuçların ciddilik derecesi düşünüldüğüne tahmin edileceği gibi, bir sistem hiçbir kaza veya ekonomik kayıp tehlikesi arzetmiyorsa bu tür araştırmalar yapmak akla gelmeyecektir. Buna karşın yüksek riskli endüstrilerde (nükleer, uzay ve ulaşıma ilişkin, kimya endüstrisi, petrokimya vb.) bu tür araştırmalar çok gerekli olmak ile birlikte aslında kabul edilebilir risk düzeyine sahip sistemlerin elde edilmesi için tamamlayıcı yöntemler halindedirler.

İşte özellikle çeşitli "Risk Değerlendirmesi Metodolojileri" büyük ölçüde bu tamamlayıcılık işlemini gerçekleştirmek maksadı ile geliştirilmişlerdir.

Bir kaza olmadıkça pahalı olarak nitelendirilen sigorta olayında olduğu gibi, risk değerlendirmesi çalışmaları da işverenlere ilk başlarda çoğunlukla yüksek

maliyetli gibi görünmüştür. Bu nedenle risk değerlendirmesi gerçekleştirme kararı çoğunlukla hafife alınmaktadır. Böyle bir karara sebep olabilecek nedenler şunlardır:

- **Yenilik:** Bir sistemi anlamak için uzmanlar genelde benzer sistemler üzerinde edinilmiş tecrübelere çok fazla dayanırlar. Geçmiş hiçbir deneyimin olmadığı yeni bir sistem anlaşılmak istendiğinde ise onun gerçek çalışmasını görmeden önce nelerin meydana gelebileceğini öngörmek gerekir. Güvenilirlik ile ilgili tekniklerin ortaya konulması sonucu kağıt üzerinde deneyimler kazanmak mümkündür. Bu şekilde sistemin gelecekteki davranışı hayal edilebilir. Zayıf ve kuvvetli yönleri ortaya konulabilir ve son olarak kazaların olmasına fırsat vermeden engelleme yolları bulunabilir.
- **Karmaşıklık:** Endüstriyel sistemler giderek daha fazla karmaşıklaşmakta ve anlaşılmaları giderek daha spesifik konularda uzmanlaşmış kişiler tarafından yürütülen çok sayıda disipline gereksinim duymaktadır. Her uzman, kendi konusuna giren kısmı olabilecek en iyi şekilde algılamaktadır ancak sorunlar çoğunlukla farklı tarafların birbirleri ile bütünleşmesi gereken zamanlarda ortaya çıkmaktadır. Parçaları biraraya getiren bir uzman yoktur ve sistemin tek tek patçalarını optimize etmek yolu ile tüm sistem için optimizasyon sağlanamadığından sonuç bazen çok kötü olabilmektedir.

Bugün için dünyada kullanılan pekçok risk değerlendirme yönteminde riskin gerçekleşme olasılığı hakkında basit ve doğrusal dış değer biçme (linear extrapolation) mekanizmasıyla risk limitleri hakkında "Tahmin Yürütme" eğilimi mevcuttur. Ancak risk değerlendirme yöntemleri uygulanırken, bilinen olasılık dağılımları veya simülasyonları ile hareket etmediğimiz takdirde, riskin gerçekleşme olasılığına ilişkin tahminimiz, bu tahmine duyduğumuz güven ve risk öncelik katsayısına dair tahminimiz subjektif nitelikte olucaktır. Bu nedenle de işyerlerinde risk değerlendirme çalışmaları yapılırken mümkün olduğu kadar kalitatif yöntemler yerine kantitatif ya da yarı kantitatif yöntemlerin olasılık ve güvenilirlik teoremleri ile birlikte kullanılması yerinde olucaktır. Bu şekilde yapılan çalışmalar sağlam temeller üzerine oturacak ve her nekadar tüm riskleri sıfırlamamız mümkün değilse de mümkün olduğu kadar sıfıra yakınsayacaktır.

Bir sistemde veya makinede ortaya çıkan arızalar, zamanında müdahale edilmezse, ikincil arızalara neden olur ve daha sonra sistemin katastrofik bir

şekilde devre dışı kalmasıyla gelişir. Kritik sistemlerde hataların ne kadar ciddi boyutta insani ve ekonomik sonuçlar doğurabileceğini ancak güvenilirlik analizi yaparak anlayabiliriz. Güvenilirlik teorisi, olası sistem aksaklıkları hakkında genel bir teoridir. Araştırmacılara ve mühendislere, sistemlerinde ve sistemin elemanlarında meydana gelebilecek aksaklıkların, bu sistemin ömrünü ve belirlenmiş standartlara göre işletim kabiliyetini etkileyen faktörlerin tahmin edilmesini sağlar. Bir sitemin güvenilirliği ise, sistemin oluşturulması sırasındaki hatalardan kaçınmak, sistem kullanımda iken hataları belirleyip düzeltmek ve işlevsel hataların vereceği zararı kısıtlamak ile başarılabilir.

Bir elemanın arızalanması, sistemi tamamen devre dışı bırakabileceği gibi sistemin davranışına hiçbir etkisi de olmayabilir veya sistemin kapasitesinde (performansında) bir düşüşe yol açabilir. Kritik sistemlerin en temel özelliği yüksek bir güvenilirliğe sahip olmaları gerekliliğidir. Bu nedenlede kritik sistemler, sistemin kullanış amacına göre kullanılabilirlik, doğruluk, hatasızlık, güvenlik, güvenilirlik konularına daha fazla önem vermek zorundadır. Bir sistemde güvenilebilirlik ve kullanılabilirlik gerekli görülürken çalışabilirlik ve güvenlik için kesin şartlar yoktur.

Günümüzde özellikle kritik risklere sahip işletmeler için sadece acil eylem planları oluşturulmasının yeterli olmadığı görüşü hakim olmaktadır. Özellikle ülkemizde de Çalışma ve Sosyal Güvenlik Bakanlığı ile Çevre ve Şehircilik Bakanlığı tarafından yayınlanmış olan "Büyük Endüstriyel Kazaların Önlenmesi ve Etkilerinin Azaltılması Hakkında Yönetmeliki" çerçevesinde acil eylem planlarının, felaket senaryoları içermesi ve bu felaket senaryolarına göre acil durumdan geri dönüş planları içermesi gerekecektir.

Bu değerlendirme çerçevesinde, işyeri veya organizasyon için müdahale gerektiren en önemli riskler ortaya çıkarılabilir ve öncelikle bu riskler üzerine odaklanılması sağlanarak, etkileri ve olasılıkları değerlendirilir. Bu çalışmalar sonucunda ortaya çıkacak risk haritası ilgili tüm taraflarla da paylaşılarak bilinçlendirme sağlanır.

Kayıpların hangi noktalarda oluşabileceğinin belirlenmesi en önemli aşamadır. Bunun için işyeri birimleriyle görüşülmesi, mevcut olanakların, süreçlerin, proses ekipmanlarının, makina parkının, sistem tasarımlarının incelenmesi, açık noktaların ve tehditlerin araştırılması, simülasyon tekniklerinin kullanılması gerekebilecektir. Ancak değerlendirme yapılırken, kritik olmayan sistem ve süreçlerle vakit kaybedilmemesi gerekir. Örneğin, bir kimya fabrikasında kritik önem

taşıyan proses koşulları veya kontrol odası ya da yangın tesisatı dururken, atelye kısmına yada ofis kısmına veya yemekhaneye öncelik tanımak doğru bir yaklaşım olmayacaktır. Felaket senaryoları ile çalışmak zaman alıcı bir çalışma olabilir, ancak bu analizlerde, riskin gerçekleşme sıklığı, yaşanabilecek kaybın önem ve şiddeti, toplam kayıpların hesaplanması ve riskin gerçekleşme zamanı konuları üzerinde durulmalıdır. Bunlarla ilgili veri mevcutta tutulmuyor olabilir ama zaman içinde sağlıklı analiz için bu bilgilerin tutulmaya başlanması önemlidir.

Tüm bu çalışmalar yapıldıktan sonra olası tehditler dikkate alınarak, "Tehdit gerçekleşirse işyerindeki kritik sistemlerin kaybı ne olur? Bu kayıpları ve/veya olayın etkilerini en aza indirgeyebilmek için önceden ne tür tedbirlerin alınması gerekir?" şeklindeki soruların netleştirilmesi gerekir. Son aşamada ise alınan önlemler sonucunda kabul edilebilirlik derecelendirmesinin yapılması şarttır.

Risk değerlendirmesi yapılacak bir işletmede önceliklede "Risk Yönetim Prosesi" nin oluşturulabilmesi için, prosesin aşamalarının iyi anlaşılmış olması gerekir. "Risk Yönetim Prosesi"nin ilk aşaması olan "Tehlike Tanımlama" aşaması en önemli aşamadır. Bu aşamada işletmede makro ayrıştırma algoritması ve mikro ayrıştırma algoritması uygulanması, malzeme güvenlik formlarının oluşturulması, bu formların parçalanarak taşıma, depolama, kullanma ve acil eylem ve ilk yardım talimatlarının oluşturulması ve tehlike derecelendirme ve sınıflandırma yapılması gerekmektedir.

Risk değerlendirmesine başlamadan önce işletmede bilgilendirme toplantıları yapılmalı ve konu ile ilgili eğitimler verilmeli ve işletmedeki tüm çalışanlar ile birlikte yönetim kadrosu bu çalışmaya dahil edilmelidir. Tehlikelerin doğru tanımlanabilmesi, risklerin değerlendirilebilmesi için mutlaka veri gereklidir, bu verilerin çoğuda çalışanlardan (Kazaya ramak kalma, tehlikeli durum, çalışmaktan kaçınma formları, kaza/olay araştırma raporları) elde edilebilir. Özellikle doldurulan formlarda bulunan durumlarla ilgili olarak, formu dolduran çalışana olumlu yaklaşılmalı ve olayın tekrarını engellemek için beraber çalışılmalıdır, sorgulayıcı bir yaklaşım bu verilerin gelmesini engelleyecek ve analist en önemli veri kaynağını kaybedecektir.

Risk haritasının oluşturulması ve başlangıç tehlike analizi yapılırken hangi kalitatif ve kantitatif yöntemlerin seçileceğine, işletmenin kendi ihtiyaçlarına, yapısına, tehlikelerinin büyüklüğüne göre bu konuda uzman kişi tarafından karar verilmelidir. Tehlike ve tehlike kaynakları rahatlıkla tanımlanabilecek olan küçük ölçekli kuruluşları, karmaşık ve zor tehlike tanımlaması, risk değerlendirmesi ve

risk kontrol uygulamalarına zorlamak başarı oranını düşürecektir. İşyerlerinde risk değerlendirmesi, değişik derinlik ve ayrıntı düzeyleri ile basitten zora sıralanan bir veya daha fazla yöntem kullanılarak gerçekleştirilebilir. ISO IEC 31010'a göre uygun teknikler, genel hatlarıyla aşağıdaki özellikleri taşımaktadır:

- İşletmenin tehlike kaynaklarını ve risk seviyelerini tespit etmek üzere savunulabilir olmalıdır,
- İncelenmekte olan durum veya organizasyonun yapısına uygun olmalıdır,
- Riskin niteliği ve riske nasıl müdahale edilmesi gerektiği konusundaki algıları geliştirecek şekilde sonuçlar sunmalıdır,
- İzlenebilir, yinelenebilir ve doğrulanabilir şekilde kullanılmaya uygun olmalıdır.

Risk değerlendirmesi çalışmaları, yanlızca işletmedeki bir kişinin/analistin tek başına yapabileceği bir işlem değildir. İşletmede bu işle ilgilenen bir tek İş Güvenliği Uzmanı olsa dahi, işletmedeki üst yönetim kadrosundan, tüm işçilere kadar herkesin bir fiil çalışmasını gerektiren bir çalışmadır. Unutulmamalıdır ki; işletmedeki bu konuya bakış açısı sadece yasal bir zorunluluğu yerine getirmek ise o işletmedeki iş kazası ve meslek hastalıkları ağırlık hızında ya da mal hasar şiddet frekansında bir azalma sağlanamayacak, iş günü ve maddi kayıplar önlenemeyecektir.

Geçerlilik ve uygunluk bakımından tekniklerin seçilme nedeni de açıklanmalıdır. Farklı çalışmalardan elde edilen sonuçların bütünleştirilmesi söz konusu olduğunda, kullanılan teknikler ve elde edilen sonuçlar birbiri ile kıyaslanabilir nitelikte olmalıdır.

ISO IEC 31010'a göre uygun teknik seçiminde, bir işletmede risk değerlendirmesi kararı alındığında ve kapsam ile hedefler tanımlandığında, sıra aşağıdaki faktörler doğrultusunda teknikleri seçmeye gelir:

- **Çalışmanın hedefleri**: Risk değerlendirmesine ilişkin hedefler, kullanılan teknik üzerinde doğrudan etkiye sahip olacaktır. Örneğin; farklı seçenekler arasında karşılaştırmalı bir çalışma yürütülürse, farklılıktan etkilenmeyen sistem parçaları için daha az ayrıntılı sonuç modellerinin kullanılması daha makuldur,
- **Karar mercilerinin gereksinimleri:** Bazı durumlarda iyi bir karar alabilmek için yüksek bir ayrıntı düzeyi gerekirken, diğer durumlar için konuya genel hatlarıyla hakim olmak yeterlidir,

- **Analize tabi tutulan riskin türü ve kapsamı:** Analiz yapılan işyerine ait risklerin türü ve kapsamı o sektöre özel risk değerlendirme tekniklerinin seçilmesini gerektirebilir,
- **Sonuçların olası önemi:** Risk değerlendirmesinin gerçekleştirileceği derinliğe ilişkin olarak alınacak karar, başlangıçta sonuçlara ilişkin olarak geliştirilen algıyı yansıtmalıdır (ön değerlendirme tamamlandığında bunun değiştirilmesi gerekebilir);
- **İhtiyaç duyulan uzmanlık, kişi ve diğer kaynak düzeyleri:** Başarı ile gerçekleştirilmiş basit bir yöntem, değerlendirmenin kapsam ve hedeflerini karşıladığı sürece yetersiz şekilde gerçekleştirilmiş daha karmaşık bir yönteme kıyasla daha iyi sonuçlar verebilir;
- **Bilgi ve verilerin kullanılabilirliği:** Bazı teknikler, diğerlerine oranla daha ayrıntılı bilgi ve veriler gerektirir.
- **Risk değerlendirmesini değiştirme/güncelleme ihtiyacı:** Söz konusu değerlendirmenin gelecekte değiştirilmesi/güncellenmesi gerekebilir. Bu konuda bazı tekniklerin üzerinde, diğerlerine göre daha fazla değişiklik yapılabilmektedir;
- **Diğer düzenleyici ve sözleşmesel gereklilikler:** Bazı durumlarda yasal düzenlemeler veya çeşitli yönetim standratları da bazı tekniklerin kullanılmasını gerekli kılabilir.

Risk değerlendirme tekniklerinin seçimini etkileyen faktörler şu şekilde özetlenebilir;

- Problemin güçlük düzeyi ve analiz edilmesi için gereken yöntemler;
- Mevcut bilgi düzeyine dayalı olan risk değerlendirmesi belirsizliğinin niteliği ve düzeyi ile hedeflerin gerçekleştirilmesi için gerekenler;
- Uzmanlık süresi ve düzeyi, veri gereksinimleri veya maliyet bakımından gereken kaynakların miktarı;
- Yöntemin kantitatif bir sonuç sağlayıp sağlamayacağı.

Kaynakların kullanılabilirliği, mevcut bilgi ve verilerin niteliği ve belirsizlik düzeyi, uygulamanın güçlüğü gibi birçok faktör, risk değerlendirme yaklaşımlarının seçimini etkilemektedir.

8.1. Kaynakların Kullanılabilirliği

Risk değerlendirme tekniklerinin seçimini etkileyen kaynak ve imkanlar arasında şunlar bulunmaktadır:

- Risk değerlendirme ekibinin beceri, deneyim, kapasite ve yeterlilikleri,
- Organizasyon içerisindeki zaman ve kaynak kısıtlamaları,
- Dış kaynak gereksinimi söz konusu olduğunda yararlanılabilir bütçe.

8.2. Belirsizliğin Niteliği ve Düzeyi

Belirsizliğin niteliği ve düzeyi, incelenmekte ola riske ilişkin bilgilerin kalitesi, miktarı ve bütünlüğünün anlaşılmasını gerektirir. Aynı zamanda risk değerlendirme tekniklerinin seçimini, risk kaynakları, nedenleri ve sonuçlarına ilişkin olarak belirlenen risk kontrol hedeflerinin gerçekleştirilebilmesi için gereken bilgilerin ne derece mevcut olduğu da etkiler. Belirsizlik, yetersiz veri kalitesinden veya gerekli ve güvenli bilgilerin eksikliğinden kaynaklanabilir. İşyerlerinin veri toplama yöntemleri değişiklik gösterebilir ya da işyerinin tanımlanan risk hakkında hali hazırda etkili bir veri toplama yöntemi olmayabilir. Örneğin; bir makinedeki bir parçanın arızalanma sıklığı bakım programından çıkartılamıyor veya veri bankasında saklanmıyor olabilir.

İşyerindeki mevcut veriler her zaman geleceğin yani riskin olasılığının tahmin edilmesi için güvenilir bir dayanak oluşturmayabilir. Kendine özgü nitelikler taşıyan riskler söz konusu olduğunda, geçmiş veriler faydalı olmayabilir veya mevcut veriler farklı kişiler tarafından farklı şekilde yorumlanabilir. Risk değerlendirmesini yürütecek kimselerin belirsizliğin niteliğini ve düzeyini anlamaları ve risk değerlendirme sonuçlarının güvenilirliğine yönelik önermeleri ve değerlendirmeleri gereklidir. Söz konusu önermeler, değerlendirmeler ya da kabul yapılan hususlar bu risk değerlendirmelerini incelemekle görevli yetkililere açıklanabilir nitelikte olmalıdır.

8.3. Güçlük Düzeyi

Risklerin tespit edilmesi, belirli güçlük düzeylerine sahip olabilir. Örneğin karmaşık sistemlerde risklerin her bir bileşene ayrı ayrı müdahale edilmesindense, sistem çapında değerlendirilmesi ve etkileşimlerin dikkate alınması gerekebilir. Diğer durumlarda ise tek bir riske müdahale edilmesi, başka bölüm ve faaliyetler üzerinde çeşitli etkiler yaratabilir. Tek bir riske müdahale edildiğinde diğer bölümlerde tahammül edilemez nitelikte bir durumun baş göstermeyeceğinden emin olmak için nihai etkiler ve risk bağımlılığının anlaşılması gerek-

mektedir. İşyerine yönelik tek bir riskin veya risk portföylerinin güçlük düzeyinin anlaşılması, risk değerlendirmesine uygun yöntem ve tekniklerin seçilebilmesi için önem arz etmektedir.

8.4. Kullanım Süresi Evreleri Boyunca Risk Değerlendirmesinin Uygulanması

Birçok faaliyet, proje veya prosesin, başlangıç evresi, sonlandırma aşaması ile ekipman, sistem veya donanımı devre dışı bırakma ve durdurma işlemlerini de içerecek şekilde tüm aşamalarını kapsayan risk değerlendirme tekniklerinin seçilmesi ve bu tekniklerin bu evrelerde uygulanabiliyor olması gerekmektedir.

Kullanım süresi evreleri farklı gereksinimlere sahiptir ve farklı teknikler gerektirir. Risk değerlendirmesi teknikleri seçilirken; seçilen tekniğin, faaliyet, proje veya prosesin kullanım süresinin tüm evreleri boyunca gerçekleştirilebilir ve her evrede verilmesi gereken kararlara yardımcı olması için genellikle farklı ayrıntı düzeylerinde birçok defa uygulanabilir düzeyde olması önemlidir. Örneğin; risk değerlendirmesi, bir faaliyet, proje veya prosesin başlangıç evresi ve tanımlama evresi süresinin herhangi bir aşamasında, tehlike doğup doğmayacağının belirlenmesi ve söz konusu eylemin yapılıp yapılmamasına yönelik karar verme işleminde kullanılabilir olmalıdır. Risk değerlendirmesinin, tasarım ve geliştirme evresi süresince katkıda bulunduğu unsurlar arasında:

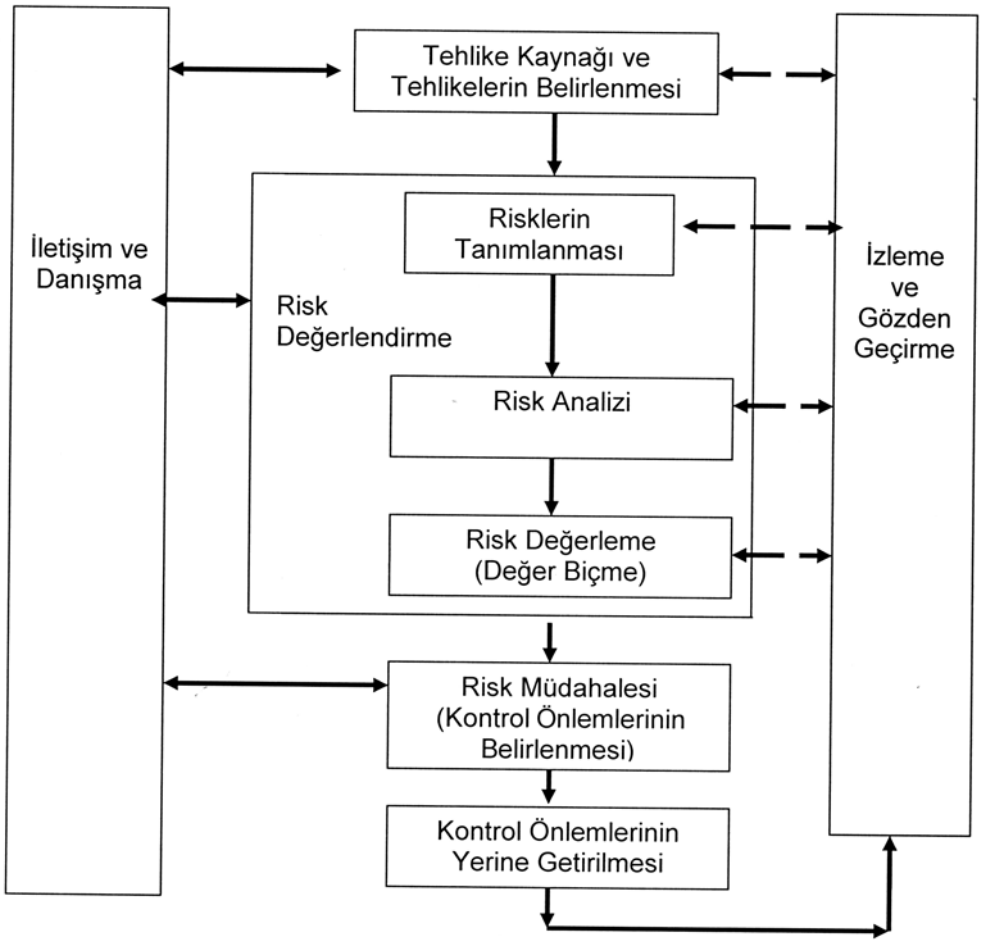
- Tasarım ve geliştirme sürecindeki tehlikeleri başlangıç aşamasında iken tespit edebilmek,
- Sonraki kullanım süresi evreleri üzerinde etkili olabilecek risklerin tanımlanması ve bulunmasını sağlamak
- Sistem risklerinin tahammül edilebilir nitelikte olduğunu ispatlamaktır.

Risk değerlendirmesi, faaliyet ilerledikçe normal ve acil koşullara yönelik prosedür geliştirme sürecine yardımcı olacak bilgilerin sağlanması için de kullanılabilir olmalıdır.

9. BÖLÜM: RİSK DEĞERLENDİRMESİ UYGULAMA ADIMLARI

Risk değerlendirmesinin amacı, belirli risklerin nasıl ele alınacağı ve seçenekler arasından nasıl tercih yapılacağı konusunda bilinçli kararların alınabilme-

Şekil 10: Risk Değerlendirme Yönetim Süreci Genel Bakış



si için kanıtlara dayalı bilgi ve çözümler sunmaktır. Risk değerlendirmesi gerçekleştirmenin bazı temel faydaları şunlardır:

- Riskin ve hedefler üzerindeki olası etkilerinin anlaşılması,
- Karar mercilerine bilgi sağlanması,

- Müdahale seçenekleri arasından bir seçim yapılmasına yardımcı olunması için riskin anlaşılmasına katkıda bulunulması,
- Riske katkıda bulunan önemli faktörleri ile sistemler ve organizasyonlarda bulunan zayıf halkaların saptanması,
- Alternatif sistem, teknoloji ve yaklaşımlarda risklerin kıyaslanması,
- Risk ve belirsizlikler hakkında iletişim kurulması,
- Önceliklerin oluşturulmasına yardımcı olunması,
- Vaka sonrası soruşturmaya dayalı olarak vakanın önlenmesine katkıda bulunulması,
- Farklı risk müdahale türlerinin seçilmesi,
- Yasal gereksinimlerin karşılanması,
- Önceden belirlenmiş kriterler çerçevesinde riskin kabul edilip edilmemesi gerekliliğinin değerlendirilmesine yardımcı olacak bilgilerin sağlanması,
- Vadesi tamamlanmış kullanıma yönelik risklerin değerlendirilmesi.

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği madde 7'ye göre risk değerlendirmesi; tüm işyerleri için tasarım veya kuruluş aşamasından başlamak üzere tehlikeleri tanımlama, riskleri belirleme ve analiz etme, risk kontrol tedbirlerinin kararlaştırılması, dokümantasyon, yapılan çalışmaların güncellenmesi ve gerektiğinde yenileme aşamaları izlenerek gerçekleştirilir. Risk değerlendirmesi, ISO 31000'da tanımlanan risk yönetim sürecine ilişkin temel unsurları içerir ve aşağıdaki hususları kapsar:

- Kapsamı oluşturma (tehlike kaynağı ve tehlikelerin belirlenmesi);
- Risk değerlendirmesi (risk tanımlama, risk analizi ve risk değerlemedeğer biçme),
- Risk müdahalesi (kontrol önlemlerinin belirlenmesi),
- İletişim ve danışma;
- Gözlemleme ve inceleme.

Standarta göre risk değerlendirmesi, "hedeflerin gerçekleştirilmesini etkileyebilecek risklerin ve mevcut kontrollerin yeterliliği ile verimliliğinin, karar mercileri ve ilgili taraflarca gelişmiş bir düzeyde kavranmasına olanak tanıyan bir süreç" olarak tarif edilmiştir. Bu yönüyle, riske müdahale edilmesi için kul-

lanılabilecek en uygun yaklaşıma karar verme konusunda bir temel oluşturulur. Risk değerlendirmesinin çıktısı, aynı zamanda organizasyonun karar verme süreçlerine yönelik bir girdidir.

Bazı koşullarda sonuçlar, birçok farklı vaka ya da durum sonucunda veya özel vaka tanımlanmadığında meydana gelebilmektedir. Bu durumda risk değerlendirmesinin odak noktası; koruma düzeyleri veya iyileştirme stratejilerine bağlı müdahalelerin saptanması amacıyla sistem bileşenlerinin önem ve hassasiyetini analiz etmektir.

9.1. Kapsamı Oluşturma (Tehlike Kaynakları ve Tehlikelerin Tanımlanması)

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği madde 8'e göre tehlikeler tanımlanırken çalışma ortamı, çalışanlar ve işyerine ilişkin ilgisine göre asgari olarak aşağıda belirtilen bilgiler toplanması gerekmektedir.

- İşyeri bina ve eklentileri.
- İşyerinde yürütülen faaliyetler ile iş ve işlemler.
- Üretim süreç ve teknikleri.
- İş ekipmanları.
- Kullanılan maddeler.
- Artık ve atıklarla ilgili işlemler.
- Organizasyon ve hiyerarşik yapı, görev, yetki ve sorumluluklar.
- Çalışanların tecrübe ve düşünceleri.
- İşe başlamadan önce ilgili mevzuat gereği alınacak çalışma izin belgeleri.
- Çalışanların eğitim, yaş, cinsiyet ve benzeri özellikleri ile sağlık gözetimi kayıtları.
- Genç, yaşlı, engelli, gebe veya emziren çalışanlar gibi özel politika gerektiren gruplar ile kadın çalışanların durumu.
- İşyerinin teftiş sonuçları.
- Meslek hastalığı kayıtları.
- İş kazası kayıtları.
- İşyerinde meydana gelen ancak yaralanma veya ölüme neden olmadığı halde işyeri ya da iş ekipmanının zarara uğramasına yol açan olaylara ilişkin kayıtlar.

- Ramak kala olay kayıtları.
- Malzeme güvenlik bilgi formları.
- Ortam ve kişisel maruziyet düzeyi ölçüm sonuçları.
- Varsa daha önce yapılmış risk değerlendirmesi çalışmaları.
- Acil durum planları.
- Sağlık ve güvenlik planı ve patlamadan korunma dokümanı gibi belirli işyerlerinde hazırlanması gereken dokümanlar.

Yönetmeliğe göre tehlikelere ilişkin bilgiler toplanırken aynı üretim, yöntem ve teknikleri ile üretim yapan benzer işyerlerinde meydana gelen iş kazaları ve ortaya çıkan meslek hastalıkları da değerlendirilmelidir. Toplanan bilgiler ışığında; iş sağlığı ve güvenliği ile ilgili mevzuatta yer alan hükümler de dikkate alınarak, çalışma ortamında bulunan fiziksel, kimyasal, biyolojik, psikososyal, ergonomik ve benzeri tehlike kaynaklarından oluşan veya bunların etkileşimi sonucu ortaya çıkabilecek tehlikeler belirlenir ve kayda alınır. Bu belirleme yapılırken aşağıdaki hususlar, bu hususlardan etkilenecekler ve ne şekilde etkilenebilecekleri göz önünde bulundurulur.

- İşletmenin yeri nedeniyle ortaya çıkabilecek tehlikeler.
- Seçilen alanda, işyeri bina ve eklentilerinin plana uygun yerleştirilmemesi veya planda olmayan ilavelerin yapılmasından kaynaklanabilecek tehlikeler.
- İşyeri bina ve eklentilerinin yapı ve yapım tarzı ile seçilen yapı malzemelerinden kaynaklanabilecek tehlikeler.
- Bakım ve onarım işleri de dahil işyerinde yürütülecek her türlü faaliyet esnasında çalışma usulleri, vardiya düzeni, ekip çalışması, organizasyon, nezaret sistemi, hiyerarşik düzen, ziyaretçi veya işyeri çalışanı olmayan diğer kişiler gibi faktörlerden kaynaklanabilecek tehlikeler.
- İşin yürütümü, üretim teknikleri, kullanılan maddeler, makine ve ekipman, araç ve gereçler ile bunların çalışanların fiziksel özelliklerine uygun tasarlanmaması veya kullanılmamasından kaynaklanabilecek tehlikeler.
- Kuvvetli akım, aydınlatma, paratoner, topraklama gibi elektrik tesisatının bileşenleri ile ısıtma, havalandırma, atmosferik ve çevresel şartlardan korunma, drenaj, arıtma, yangın önleme ve mücadele ekipmanı ile benzeri yardımcı tesisat ve donanımlardan kaynaklanabilecek tehlikeler.

- İşyerinde yanma, parlama veya patlama ihtimali olan maddelerin işlenmesi, kullanılması, taşınması, depolanması ya da imha edilmesinden kaynaklanabilecek tehlikeler.
- Çalışma ortamına ilişkin hijyen koşulları ile çalışanların kişisel hijyen alışkanlıklarından kaynaklanabilecek tehlikeler.
- Çalışanın, işyeri içerisindeki ulaşım yollarının kullanımından kaynaklanabilecek tehlikeler.
- Çalışanların iş sağlığı ve güvenliği ile ilgili yeterli eğitim almaması, bilgilendirilmemesi, çalışanlara uygun talimat verilmemesi veya çalışma izni prosedürü gereken durumlarda bu izin olmaksızın çalışılmasından kaynaklanabilecek tehlikeler.

Risk Değerlendirmesi yönetmeliği gereğince çalışma ortamında bulunan fiziksel, kimyasal, biyolojik, psikososyal, ergonomik ve benzeri tehlike kaynaklarının neden olduğu tehlikeler ile ilgili işyerinde daha önce kontrol, ölçüm, inceleme ve araştırma çalışması yapılmamış ise risk değerlendirmesi çalışmalarında kullanılmak üzere; bu tehlikelerin, nitelik ve niceliklerini ve çalışanların bunlara maruziyet seviyelerini belirlemek amacıyla gerekli bütün kontrol, ölçüm, inceleme ve araştırmalar yapılır.

9.2. Risk Değerlendirmesi

Risk değerlendirmesi bağımsız bir faaliyet değildir; risk yönetim sürecinde yer alan diğer tüm unsurlara tamamıyla entegre edilmelidir. Risk değerlendirmesi; kapsamlı bir risk tanımlama süreci, risk analizi ve risk tespitinden oluşur. Bu sürecin uygulanma biçimi yalnızca risk yönetim sürecine değil; risk değerlendirmesi yapılırken kullanılan yöntem ve tekniklere de dayalıdır.

9.3. Risk Analizi

Risk analizinin geniş anlamda üzerinde uzlaşılmış bir tanımı olmamakla birlikte önerilen tanımlardan biri aşağıda verilmiştir. Bu tanım nitel ve nicel yöntemleri de içine alacak şekilde geniştir. Bu aynı zamanda aşağıda daha detaylı verilen risk analizi tanımını da kapsar.

Risk analizi sistemlerin, içerdiği tehlikelerin ve güvenlik karakteristiklerinin tanımlanması ve değerlendirilmesi amacıyla analiz edilmesidir.

Bu kitapta verilen risk analiz uygulamalarının çoğunda, güvenliği geliştirmek için öneriler üretilmesi, analizin temel parçasıdır. Ortak amaç, sistemdeki tehlikelerin genel bir resmini elde etmektir.

Güvenilirlik alanında uluslararası bir standart olan IEC 60300-3-9 "risk analizi" ve ilgili bazı terimleri tanımlamıştır. Bu standarta göre:

Risk analizi, mevcut bilginin tehlikelerin tanımlanması ve bireylere, topluma, mallara veya çevreye karşı risklerin tahmin edilmesi amacıyla sistematik biçimde kullanılmasıdır.

Standartta risk, sıklığın veya meydana gelme olasılığının ve sözkonusu tehlikeli olayın sonucunun kombinasyonunu ifade eder. Risk analizi bazen Olasılıksal Güvenlik Analizi (Probabilistic Safety Analysis -PSA), Olasılıksal Risk Analizi (Probabilistic Risk Analysis -PRA), Kalitatif Güvenlik Analizi ve Kantitatif Risk Analizi (Quantitative Risk Analysis -QRA) olarak ifade edilir.

Risk analizi, riske yönelik bir anlayış geliştirmeye yöneliktir. Risk değerlendirme süreci, risklere müdahale edilip edilmemesi ve en uygun müdahale strateji ve yöntemlerine bağlı kararlar hakkında çeşitli veriler sunmaktadır. Risk analizi, mevcut kontrollerin varlığı ve etkililiğini göz önüne alarak, tanımlanmış risk olaylarına ilişkin olasılığın ve sonuçlarının belirlenmesini içermektedir. Ardından, sonuçlar ve sonuçlara yönelik olasılıklar, risk düzeyinin saptanması için bir araya getirilir.

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği madde 9'a göre tespit edilmiş olan tehlikelerin her biri ayrı ayrı dikkate alınarak bu tehlikelerden kaynaklanabilecek risklerin hangi sıklıkta oluşabileceği ile bu risklerden kimlerin, nelerin, ne şekilde ve hangi şiddette zarar görebileceği belirlenir. Bu belirleme yapılırken mevcut kontrol tedbirlerinin etkisi de göz önünde bulundurulur. Toplanan bilgi ve veriler ışığında belirlenen riskler; işletmenin faaliyetine ilişkin özellikleri, işyerindeki tehlike veya risklerin nitelikleri ve işyerinin kısıtları gibi faktörler ya da ulusal veya uluslararası standartlar esas alınarak seçilen yöntemlerden biri veya birkaçı bir arada kullanılarak analiz edilir. İşyerinde birbirinden farklı işlerin yürütüldüğü bölümlerin bulunması halinde birinci ve ikinci fıkralardaki hususlar her bir bölüm için tekrarlanır.

Yine yönetmeliğe göre analizin ayrı ayrı bölümler için yapılması halinde bölümlerin etkileşimleri de dikkate alınarak bir bütün olarak ele alınıp sonuçlandırılır. Analiz edilen riskler, kontrol tedbirlerine karar verilmek üzere etkilerinin büyüklüğüne ve önemlerine göre en yüksek risk seviyesine sahip olandan başlanarak sıralanır ve yazılı hale getirilir.

Risk analizi, risklerin nedeni ve kaynağı, sonuçları ve aynı sonuçların tekrarlanma olasılığı üzerinde durur. Sonuç ve olasılıkları etkileyen faktörlerin saptanması gerekmektedir. Herhangi bir vaka birden fazla sonuç doğurabilmekte ve birden çok hedefi etkileyebilmektedir. Mevcut risk kontrolleri ve bunların verimliliği göz önünde bulundurulmalıdır. Söz konusu analizlere yönelik birçok yöntem bulunmaktadır. Karmaşık uygulamalarda birden fazla tekniğe yer vermek gerekebilir. Normal şartlarda risk analizi; risk düzeyinin ölçülebilmesi için herhangi bir vaka, durum ya da koşuldan doğabilecek olası sonuçların ve bunlarla ilişkili olasılıkların tahmin edilmesini içermektedir.

Risk analizinde kullanılan teknikler üç sınıfta ele alınabilir :

- Kantitatif **(quantitative)** Teknikler
- Kalitatif **(qualitative)** Teknikler
- Yarı Kantitatif **(quantitative)** Teknikler

Kantitatif risk analizi, riski hesaplarken sayısal yöntemlere başvurur. Kalitatif risk analizinde tehditin olma ihtimali, tehditin etkisi gibi değerlere sayısal değerler verilir ve bu değerler matematiksel ve mantıksal metotlar ile proses edilip risk değeri bulunur. Diğer temel risk analizi yöntemi ise kalitatif risk analizidir. Kalitatif risk analizi riski hesaplarken ve ifade ederken numerik değerler yerine yüksek, çok yüksek gibi tanımlayıcı değerler kullanır.

Riskler analiz edilirken kullanılan yöntemler kalitatif, yarı kantitatif veya kantitatif olabilmektedir. Gereken ayrıntı düzeyi ise özel uygulamaya, güvenilir verilerin mevcudiyetine ve organizasyonun karar verme gereksinimlerine bağlı olacaktır. Bazı yöntemler ve risk analize ilişkin ayrıntı düzeyi, yasalarca tayin edilebilmektedir. (Örneğin; Seveso direktifi)

Kalitatif değerlendirme; "yüksek", "orta" ve "düşük" gibi önem dereceleri yoluyla risklerin sonuçlarını, olasılıklarını ve düzeylerini belirler, sonuçlar ile olasılıkları bir araya getirir ve kalitatif kriterler doğrultusunda nihai risk düzeyini değerlendirir.

Yarı kantitatif yöntemler; sonuç ve olasılıklar için sayısal derecelendirme ölçeklerinden faydalanır ve risk düzeyini belirlemek için formül kullanmak suretiyle bunları bir araya getirir. Ölçekler doğrusal veya logaritmik olabilir ya da başkaca türden bir ilişki içerebilir. Kullanılan formüller de değişiklik gösterebilir.

Kantitatif analiz ise sonuçlar ve olasılıklara yönelik uygulamalı değerleri hesaplar ve kapsam geliştirilirken belirlenen özel birimlerdeki risk düzeyi

değerlerini ortaya koyar. Tam kantitatif analiz; analiz edilen sistem veya faaliyete dair yeterli bilgi sahibi olunmaması, veri eksikliği, insan faktörünün etkileri vb. ya da kantitatif analiz verisinin garanti edilmemesi veya gerekmemesi nedeniyle her zaman mümkün veya cazip olamayabilmektedir. Bu tür koşullar altında uzmanlar ya da alanında bilgi sahibi olan kimselerce gerçekleştirilen ve risklerin karşılaştırmalı olarak yarı kantitatif veya kalitatif derecelendirilmesini içeren bir yöntem tercih edilebilir.

Analizin kalitatif oluğu durumlarda kullanılan tüm terimlerin açık bir şekilde ifade edilmesi ve tüm kriter dayanaklarının kaydedilmesi gerekmektedir. Tam kantitatif analizin uygulandığı durumlarda bile hesaplanan risk düzeylerinin tahminlerden ibaret olduğu bilinmelidir. Kantitatif analiz yapılırken, kullanılan veri ve yöntemlerin doğruluğu ile tutarlılığı ve kesinlik düzeyinden emin olmak için gerekli özen gösterilmelidir.

Kalitatif sonuçların güvenilirliği, uygulamayı yapan uzman personelin tecrübesine ve deneyimlerine bağlıdır. Bu sebepten dolayı kalitatif teknikler sübjektif olarak değerlendirilir. Tekniklerin büyük bir kısmı kantitatif sonuçlardan yoksundur. Ayrıca kalitatif tekniklerin bir kısmı, sadece bir gözlem niteliğinde olup, ciddi kaza potansiyeli taşıyan durumlar üzerinde etkisiz kalabilirler.

Bir işletme içerisinde risk değerlendirmesi tekniklerinin tümü duruma bağlı olarak kullanılır. Kantitatik ve kalitatif yöntemlerin kullanımı eldeki veriye, risk değerlendirmesini yapıcak olan kişilerin bilgi birikimine ve konu hakkındaki deneyimine, yöntemleri kullanma becerisine bağlıdır. Risklerin etkin bir şekilde yönetilebilmesi için kantitatif ve kalitatif yöntemlerin uygun bir şekilde harmanlanması gerekir. Sübjektif/deneyime bağlı risk değerlendirme metodolojileri, uzman görüşleri, benzerleriyle karşılaştırma ya da geçmiş deneyimlerden öğrenme gibi bilgi birikimi gerektiren tekniklerdir. Uzman görüşleri ile kalitatif tekniklerde, konunun uzmanı kişilerden risklerin olasılıkları ve şiddetin büyüklüğünün ne olduğu bilgisi edinilir.

Risk yönetim prosesinin her adımında uygulanacak metodolojiler, risk yönetiminin planlanması açamasında seçilmeli ve seçilen metodolojilerinin uygunluğu yönetim tarafından onaylanır. Kullanılacak yöntem bilim, teknik ve gereçler program fazına göre değerlendirilmelidir. İş programı ilerledikçe artan bilgi düzeyine bağlı olarak kullanılabilecek metodoloji ve gereçler değişebilmelidir.

Çoğunlukla risk ve tehlike kavramları aynı anlamda kullanılmaktadır. Oysa bu iki kavram tamamen birbirinden farklıdır, Birinci bölümde bu iki kavramın terminolojisini ayrıntılı olarak incelemiştik. Tehlike; belirli koşullar altında zarara yol açabilecek bir özellik veya durum, Risk ise; tanımlanan bir tehlikenin olma ihtimali veya olasılığı ile bu oluşumun etkilerinin büyüklüklerinin bir bileşkesidir.

Bir başka ifadeyle risk, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayıba ya da zarara uğrama olasılığıdır ve gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eder. Riskin iki temel bileşeni vardır;

1. Belirli bir sonuca ulaşamama olasılığı ya da istenmeyen bir olayın oluşma olasılığı (olasılık)
2. Riskin oluşması durumunda sonuca etkisi (şiddet)

$$\text{Risk} = f(\text{olasılık, şiddet})$$

Risk = Tehditin Olma İhtimali (likelihood) * Tehditin Etkisi (impact) formülü kalitatif risk analizinin temel formülüdür.

9.4. Olasılık Tayini veya Hesaplaması

Olasılığı hesaplamak için genellikle üç genel yaklaşım benimsenmekte ve söz konusu yaklaşımlar ayrı ayrı ya da birlikte uygulanabilmektedir.

- Geçmişte yaşanmış ilgili geçmiş veri ya da vakaların kullanımı yoluyla bunların gelecekte tekrarlanma olasılıklarını tahmin etmeyi içerir. Kullanılan verilerin, bakım programları veya kayıtlarında, kaza analiz raporlarında vb. bulundurulan sistem, imkan, organizasyon veya faaliyet ve sürece dahil olan organizasyonun işletimsel standartları ile ilişkili veri olması gerekmektedir. Geçmişe bakıldığında bir olayın tekrarlanma olasılığı bir hayli düşük ise, herhangi bir olasılık hesaplaması belirsiz bir nitelik taşıyacaktır. Bu durumda, örneğin ön tehlike analizinde olasılık tayini yaparken bu durum ya da koşulun gelecekte tekrarlanmasının "ihtimal dışı" anlamı taşıyabileceği söylenebilir.
- Hata ağacı analizi, olay ağacı analizi, neden sonuç analizi vb. tekniklerden faydalanılarak yapılan olasılık tahminlerini içerir. Geçmiş verileri mevcut olmadığında veya yetersiz geldiğinde; sistem, faaliyet, donanım veya organizasyon ile organizasyonun ilgili başarı ve başarısızlık durumlarının analiz edilmesi yoluyla olasılığın kestirilmesi gerekmektedir.

İşletimsel tecrübeler veya yayınlanmış veri kaynaklarından elde edilen ve donanım, insanlar, organizasyonlar ve sistemlere yönelik olan sayısal veriler, en yaygın vakanın olasılığını hesaplamak için bir araya getirilir. Bu teknikler kullanıldığında, aynı sebepten kaynaklanan ve sistem içerisindeki farklı bölüm ya da bileşenlerin sayısına ilişkin tesadüfi arızaları içeren yaygın arıza türleri olasılığının analizinde yeterli ödeneğin sağlandığından emin olunması önemlidir. Eskime ve diğer bozulma süreçlerine bağlı donanımsal ve yapısal arızaların olasılıklarını saptamak için belirsizliklerin etkilerini hesaplayan simülasyon teknikleri gerekebilir.

- Olasılığın hesaplanması için sistematik ve yapısal bir süreçte gözlem yapılmasına ve olasılık teoremlerine başvurulabilir. Değerlendirmeyi yapan uzman; tarihsel, sisteme özel, organizasyona özel, deneysel, tasarım vb. tüm ilgili bilgilerden yararlanmalıdır. Uygun soruların açık ve kesin bir şekilde ifade edilmesine yardımcı olan uzman değerlendirmesinin sağlanması için çok sayıda olasılık teoremi mevcuttur. Mevcut yöntemler arasında Delphi yaklaşımı, ikili karşılaştırmalar, kategori derecelendirmesi ve mutlak olasılık değerlendirmesi bulunmaktadır.

9.5. Risk Değerleme (Kabul Edilebilirlik Kriterini Belirleme)

IEC ISO 31010: 2009'a göre risk değerleme, risk düzeyi ve türünün önemini belirlemek amacıyla, hesaplanmış risk düzeylerinin, risk analizi bağlamında oluşturulan risk kriterleri ile karşılaştırılmasını içerir.

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği'nin 4. maddesinde ise ***"Kabul Edilebilir Risk Seviyesi"*** yasal yükümlülüklere ve işyerinin önleme politikasına uygun, kayıp veya yaralanma oluşturmayacak risk seviyesi olarak tanımlanmıştır.

Risk değerleme, geleceğe yönelik faaliyetler hakkında kararlar almak için risk analizi süresince karşılaşılan risklerin anlaşılmasından faydalanır. Risk algısı da dahil olmak üzere etik, yasal, finansal ve diğer hususlar da karar sürecinde etkili olan girdiler arasındadır.

Söz konusu kararlar, aşağıdaki unsurları içerebilir:

- Riskin müdahale gerektirip gerektirmediği,
- Müdahale öncelikleri,
- Bir faaliyetin yürütülüp yürütülmeyeceği,
- Faaliyet yürütülürken hangi yöntemin benimseneceği.

Alınması gereken kararların niteliği ve söz konusu kararlar alınırken kullanılacak kriterler risk değerlendirmesi oluşturulurken belirlenmiştir. Ancak, belirlenen risk hakkında daha fazla bilgi sahibi olunduğu aşamada daha ayrıntılı bir biçimde yeniden değerlendirilme yapılması gerekmektedir.

Risk kriterlerinin belirlenmesi için en basit yapı tek düzeylidir; müdahale gerektiren ve gerektirmeyen riskleri birbirinden ayırır. Bu sayede oldukça basit sonuçlar elde edilir.

Riske müdahale edilip edilmeyeceği veya nasıl müdahale edileceğine yönelik kararlar, risk alma maliyeti ve faydaları ile gelişmiş kontrollerin uygulanmasına ilişkin maliyet ve faydalara dayalıdır.

Bu konudaki genel bir yaklaşım, riskleri üç gruba ayırma yönündedir:

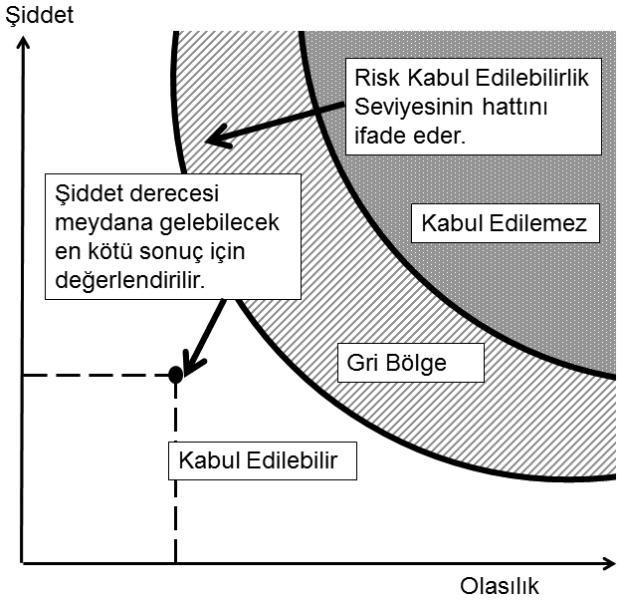
- Faaliyetin getireceği faydalara bakılmaksızın, risk düzeyinin tahammül edilemez olduğunu gösteren ve maliyeti ne olursa olsun riske müdahale gerektiren bir üst bant;
- Maliyet ve faydaların göz önüne alındığı ve olası sonuçlara karşı olanakların dengelendiği bir orta bant (veya "gri" alan);
- Risk düzeyinin önemsiz veya risk müdahale önlemlerinin alınmayacağı kadar küçük görüldüğü bir alt bant.

Güvenlik uygulamalarında kullanılan "makul şekilde uygulanabilecek kadar düşük" veya orijinal adıyla ALARP kriter sistemi de bu yaklaşımdan faydalanır. Söz konusu yaklaşımın orta bandında, düşük riskler için maliyet ve faydaların doğrudan kıyaslanabileceği değişken bir ölçek bulunur ve yüksek riskler için, zarar olasılığını düşürme maliyeti elde edilen güvenlik kazancına tamamen orantısız hale gelene dek, bu olasılığın düşürülmesi gerekir.

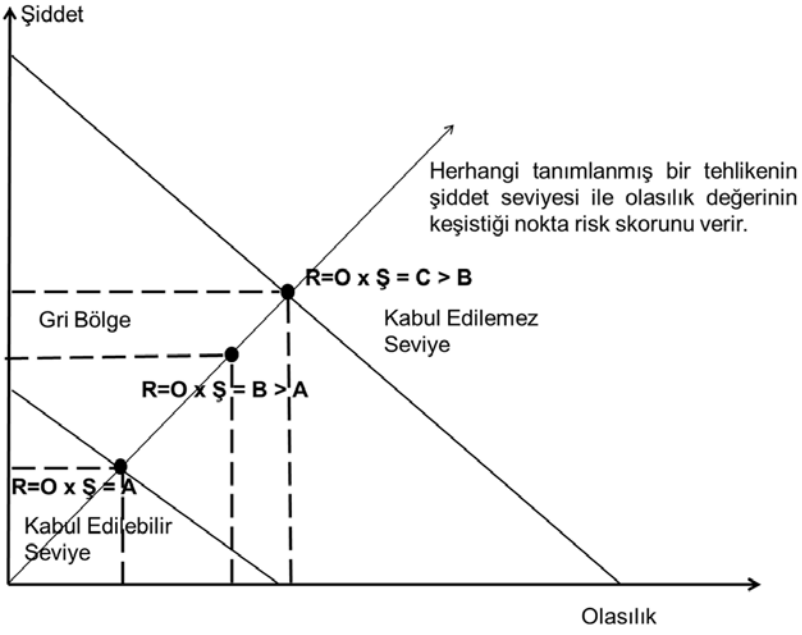
Risk değerlendirmesi çalışması yapılırken belli bir risk için birtakım kriterler ve kabul edilme seviyesi gerekmektedir. Şekil 11'de meydana gelme olasılığı ile sonuçlarının şiddeti ve kabul edilme seviyesi arasındaki ilişki gösterilmiştir. Şimdi bu seviyeleri inceleyecek olursak;

- **A tehlikesi;** hem düşük olasılığa hem de kaza meydana gelmesi durumunda önemsiz sonuçlara yani şiddete sahiptir. Bu risk kabul edilme seviyesinin altında olduğundan kabul edilebilir olarak sınıflandırılır.
- **C tehlikesi;** ise yüksek olasılığa ve önemli sonuçlara sahiptir ve kabul edilemez seviyenin üzerindedir. Analiz edilen sistemin onaylanması için, meydana gelme olasılığını veya meydana gelmesi durumunda sonuçlarını azaltmak derhal ve acil olarak birşeyler yapılmalıdır. Buradaki önemli husus ise şudur; bu önlemler alınırken işin devam etmesine izin verilemez.

Şekil 11: Risk Kabul Edilebilirlik Sınırları



Şekil 12: Risk Skoru



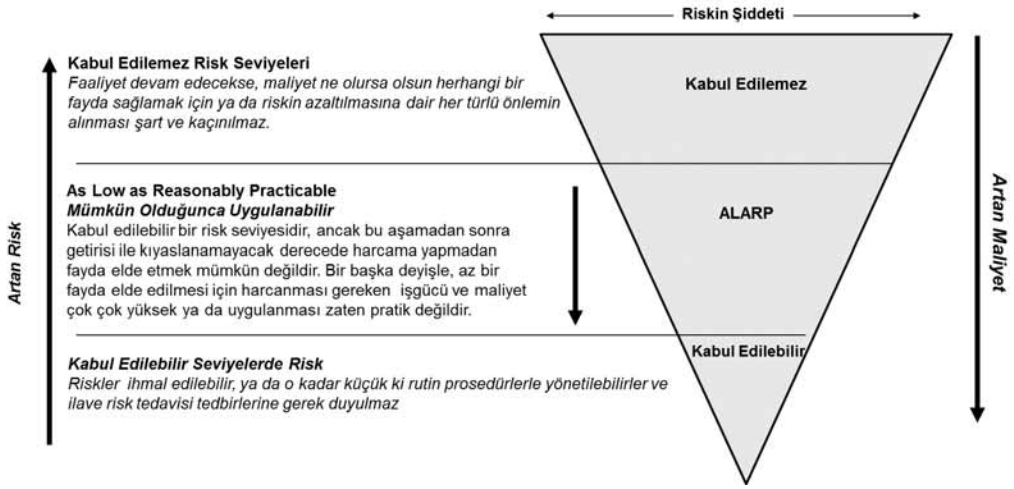
• **B tehlikesi;** limitler arasındaki gri bölgede yer almaktadır. B tehlikesinin orta derecede meydana gelme olasılığı vardır aynı zamanda da kaza meydana gelmesi durumunda şiddet derecesi çok yüksek değildir.

Asıl önemli olan soru şudur? Bu seviye organizasyon tarafından kabul edilmeli midir? Yoksa edilmemeli midir? Eğer kabul edilmez ise bu tehlike kabul kriterleri içinde yer almamaktadır ve meydana gelme olasılığını veya meydana gelmesi durumunda sonuçlarını azaltmak için ilave tedbirlere ihtiyaç duyulmaktadır. Bu çoğu zaman, özellikle de geniş ve kompleks sistemlerde karmaşık bir sorudur. İşte burada çözüm için genellikle iki genel prensip geçerli olur.

- Mümkün Olduğunca Mantıklı ve Ulaşılabilir En Düşük Seviye - ALARA (As Low As Reasonably Achievable)
- Mümkün Olduğunca Uygulanabilir En Düşük Seviye - ALARP (As Low As Reasonably Practicable)

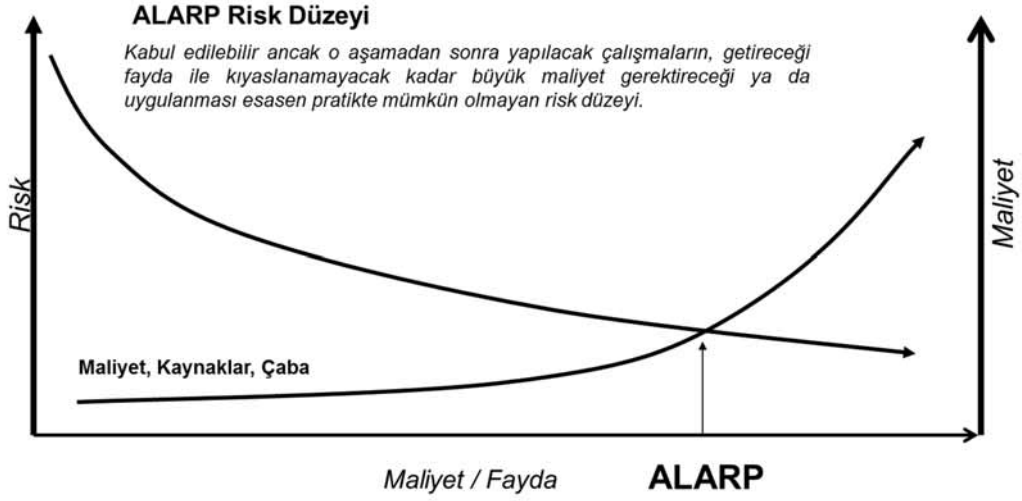
ALARP prensibi, mevcut şartlar altında mümkün olanın en iyisinin yapılmasını öngürür. "Mümkün Olduğu Kadar Düşük" risk prensiplerine göre alınması gereken önlem düzeyi belirlenir. ALARP prensibinde pratik olarak elde edilebilecek kadar düşük seviyeye kadar risk koru düşürülür. ALARP tekiğinin bir uygulaması, güvenlik ekipmanının "Güvenilirlik" seviyesini artırarak güvenliği artırmaktır.

Şekil 13: ALARP Seviyesi



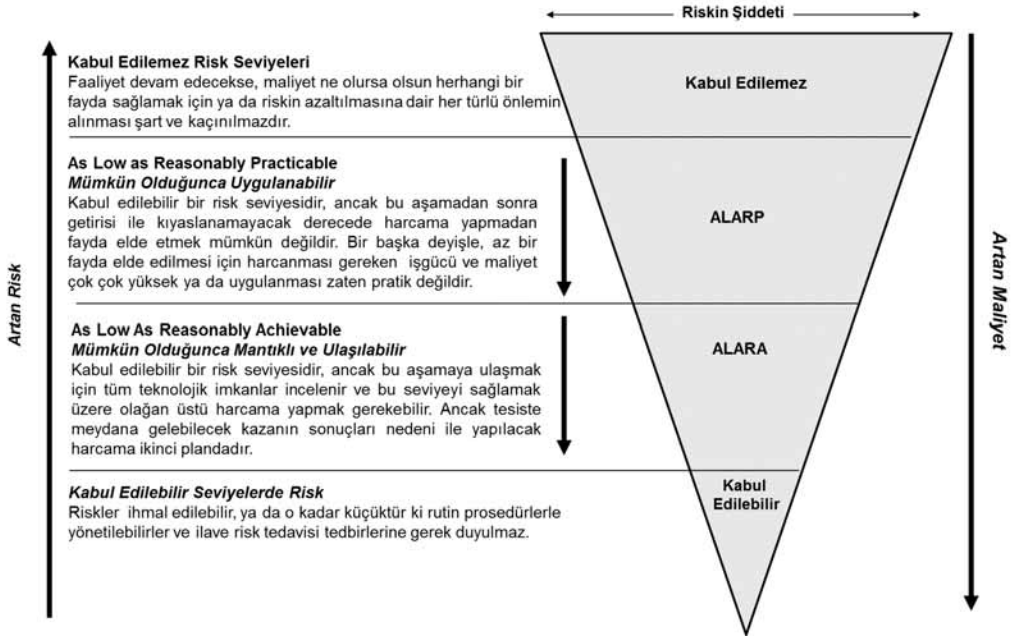
Orta derecede kabul edilebilirlik olarak tanımlanan "Gri Bölge"ye dahil olan riskler, maliyetin elverdiği ölçüde değerlendirmeye alınır. ALARP, kantitatif (sayısal) yaklaşımlı bir risk değerlendirmesi için çok yararlı ve sayısal olarak ifade edilebilen bir kavramdır. Tanımlanmış ve uygulanabilir risk azaltma yöntemi için sorumlular, uygulamanın makul olmadığı durumlar dışında önlemleri uygulamak zorundadır. Bu prensip özellikle Seveso II Direktifi çerçevesinde birçok ülkede üst seviyeli tesislerinem alma sorumluluğu için bir zorunluluk olarak uygulanmaktadır.

Şekil 14: ALARP Risk Düzeyi



ALARA ise buna çok benzer fakat daha sıkı ve dikkatli bir uygulamadır. Risk **"mümkün olduğunca"** yerine **"mantıklı seviyeye"** kadar indirilir. Bir tesisdeki tanımlanmış bir risk için, tüm teknolojik imkanlar incelenerek "Mantıklı ve Ulaşılabilir En Düşük Seviye"ye kadar risk skoru azaltılmalıdır. Alınan önlemler, tesis içinde bir arızanın veya normal olmayan bir durumun gerçekleşmesini önlemeli ve büyük kazaların insan ve çevre üzerindeki etkilerini en aza indirmelidir. Bu prensip İngilterenin nükleer ve açık deniz tesislerinde ayrıca da radyasyonla yapılan iş ve işlemlerde sıklıkla uygulanmaktadır.

Şekil 15: ALARP ve ALARA Seviyesi



ALARP; riskin mümkün olan en düşük seviyeye çekilmesi anlamı taşımaktadır. Burada "mümkün olan en düşük" derken "olağanüstü harcama yapmadan" mümkün olan kastedilmektedir. ALARA'da ise risk azaltma çözümünün ekonomik maliyetine odaklanmadan (yani gerekiyorsa olağanüstü harcama da yaparak) riskin azaltılması yaklaşımını anlatır. ALARA, ALARP'dan daha hassas ve daha sınırlayıcıdır, alınacak olan tedbirlerin maaliyetinin ekonomik olup olmaması ise ikinci plandadır.

Riski sıfırlamak mümkün değildir. Ancak kontrol altında tutarak kabul edilebilir seviyeye getirmek mümkündür. A.B.D Federal Havacılık Otoritesinin, Sistem Güvenliği El Kitabında (Federal Aviation Authorities- System Safety Handbook,2000), çeşitli risk türlerinden bahsedilmektedir, **Şekil 16**'da bunlar arasındaki ilişki gösterilmektedir.

• **Tanımlanmış Risk**

Bir sistemin, prosesin veya ekipmanın emniyetli bir şekilde çalışabilmesi için ilk yapılması gereken şey mümkün olabildiğince ortaya çıkabilecek tüm tehlikeleri tanımlamak ve bu tehlikelerin ortaya çıkma olasılıkları ile ortaya çık-

tıklarında meydana getirecekleri etkinin büyüklüğünün tanımlanmasıdır. Çeşitli risk değerlendirme yöntemleri kullanılarak belirlenen risklerdir.

- **Tanımlanamayan Risk**

Sistem, proses veya ekiman için henüz belirlenememiş riskleri ifade eder. Bu riskleri tanımlamak için yeterli bilgi birikimi veya teknoloji ya da geçmiş verisi olmayabilir. Çoğunluğu ancak ortaya çıkan bir kazadan sonra tanımlanabilirler.

- **Kabul Edilebilir Risk**

İlave mühendislik ve kontrol çalışmalarına gerek kalmaksızın, sistemde, proseste veya ekipmanda kalmasına müsaade edilmiş olan tanımlanmış riskin bir parçasıdır. Bu riskin ya ortaya çıkma olasılığı çok çok küçüktür ya da etkisi oldukça azdır. Yönetim faaliyetlerindeki sorumluluktan dolayı bu kararı almak zordur. Riske maruz kalan kullanıcı, yeterli bilgiye sahip olduğunda ancak bu karar verilebilir.

- **Kabul Edilemeyen Risk**

Yönetim tarafından asla göz yumulmaması gereken risklerdir. Ortadan kaldırılması veya kontrol altında tutulması gereken tanımlanmış riskin bir alt unsurudur.

- **Toplam Risk**

Tanımlanmış ve tanımlanamayan risklerin toplamıdır.

- **Artık Risk**

Sistemin, prosesin veya ekipmanın emniyeti için yapılan çalışmalar tamamlandıktan sonra geriye kalan risktir. Kabul edilebilir riskle aynı anlama gelmez. Kabul edilebilir risk ile tanımlanamayan risklerin toplamı ve kullanıcıya iletilen toplam risktir.

Risk değerlendirmesinin genel amacı, bir sistemde var olan risklerin yukarıda anlatıldığı üzere kabul edilebilir risk olup olmadığının, değişiklik gerekip gerekmediğinin tespiti için temel oluşturabilmektir. Ayrıca risk değerlendirme çalışmalarının başka hedefleri de bulunmaktadır;

- Riskin boyutu ile ilgili tahmin yapmak,
- Önemli ve daha önemsiz riskler arasında ayrım yapmak,
- Risk seviyelerini kriterlere göre karşılaştırarak sistemi onaylamak,

- Güvenliği arttırmak için sistemde iyileştirme yapılmasına gerek olup olmadığına karar vermek,
- Uyarılar için temel oluşturmak, örneğin, proses tehlikesini azaltmak üzere güvenlik için kurulmuş sisteminin proseste başka bir güvenlik zafiyetine sebep olup olmadığına karar vermek.

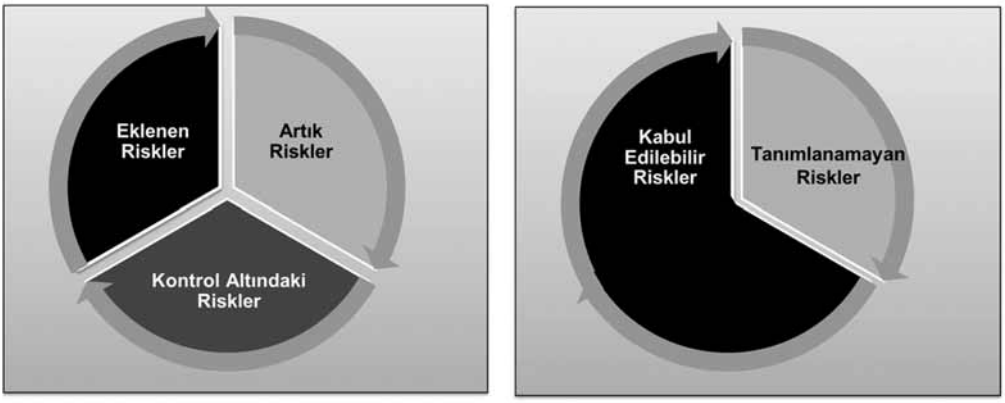
9.6. Sonuç Analizi

Risk değerlendirmesi yapılırken, analiz edilecek sonuçların türü ve durumdan etkilenebilecek taraflar göz önünde tutulması gerekmektedir. Sonuç analizi, belirli bir olay ya da durum baş gösterdiğinde karşı karşıya kalınabilecek etkinin niteliği ve türünü belirler. Herhangi bir olay, farklı büyüklüklere sahip çok sayıda etki doğurabilir ve çok sayıda farklı hedefler ile tarafları etkileyebilir.

Büyük endüstriyel kazayı tanımlayacak olursak; Seveso Direktifi kapsamındaki tesislerde meydana gelen, hemen veya sonra, tesis içinde ve dışında, bir yada birkaç tehlikeli maddenin sözkonusu olduğu, insan sağlığı ve/veya çevrede önemli tehlikeye neden olan, kontrolsüz büyük emisyon, yangın veya patlama olaylarıdır. Bazı kaza tipleri aşağıda verilmiştir;

A. Direk sonuçları olan kaza: Şans eseri istenmeden tetiklenmiş ani istenmeyen olaydır. Kısa bir zaman periyodu içinde istenmeyen sonuçlar gözlemlenir. Buna örnek olarak preste sıkışma, patlama veya ekipmanın parçalanması verilebilir.

Şekil 16: Risk Türleri



Toplam Risk Artık Risk

B. Yüksek olasılıkla yaralanma ve zarara neden olan kazalar: Bu A ile aynıdır fakat sonuçları dolaylı olur. Buna örnek olarak radyasyona veya kimyasal maddeye maruziyet sonucu kanser olma olasılığı verilebilir.

C. Yavaş yavaş kötüleşme ve dejenerasyon: Buna örnek ise küçük dozda kimyasal maddelere sürekli ve tekrarlı maruziyet sonucu ortaya çıkan meslek hastalıkları ve çevreye verilen zararlardır.

D. Sabotaj: Kişilerin kasten yaptıkları hareketler sonucu ortaya çıkan negatif hadiselerdir. Bazen bu tip olaylar kaza olarak sınıflandırılmaz.

Bu kategoriler arasındaki çizgilerin sınırları muğlaklaşabilir. Örneğin, A ve C arasındaki fark bazen tartışılabilir. A durumunda, olayın sonucunun ortaya çıkması saatler alırken C için yıllar sürebilir.

Baş gösterebilecek etkiler, düşük sonuçlara sahip olmasına rağmen yüksek olasılığa veya yüksek sonuçlara rağmen düşük olasılığa sahip olabilir. Bu iki ihtimalin arasında bir sonuç da söz konusu olabilir. Genellikle potansiyel olarak bir hayli büyük sonuçlar içeren risklere odaklanmak daha uygundur. Diğer durumlarda ise yüksek ve düşük sonuçlar içeren riskleri ayrı ayrı analiz etmek önem arz eder. Örneğin; sık karşılaşılan ancak düşük etkiye sahip (veya kronik) bir problem, geniş, yığılmalı veya uzun süreli etkiler doğurabilir. Dolayısıyla tüm sonuçları ayrı ayrı analiz etmek faydalı bir çözüm yolu olacaktır. Sonuç analizi şu unsurları içermektedir;

- Sonuçların üstesinden gelebilmek için, sonuçlar üzerinde etkisi olan tüm ilgili faktörlerle birlikte mevcut kontrolleri de gözden geçirme,
- Riske ilişkin sonuçları başlangıçta belirlenen hedefler ile ilişkilendirme;
- Hem dolaysız sonuçları hem de değerlendirme kapsamı ile tutarsız olması nedeniyle belirli bir zaman geçtikten sonra baş gösterebilecek sonuçları hesaba katma;
- Bağlı sistem, faaliyet, donanım veya prosesler, sistemler üzerinde etkili olan ikincil sonuçları dikkate alma.

Sonuç analizi, basit sonuç tanımlamasından ayrıntılı kantitatif örnekleme veya hasar görebilirlik analizine kadar farklı derecelerde yapılabilir. Örneğin Seveso direktifi çerçevesinde kantitatif sonuç analizi yapılması gerekmektedir. Direktif özellikle yerleşim planlamasını düzenlerken yangın, patlama veya toksikolij yayılma vb. durumlar için sonuç analizi ve modelleme istemektedir.

Bu konuda ortak bir yaklaşım tanımlanan tehlikelerin ilgili olayın meydana gelme sıklığı ve sonuçlarına göre sınıflandırılmasıdır. Risk hesaplamaları riskin

uygun terimlerle ifade edilmesine yardımcı olacaktır. Ortak olarak kullanılan bazı ölçümler aşağıda verilmiştir:

• **Bireysel Risk:** Bireylerin ölüm oranlarının tahmin edilen sıklıklarıdır.

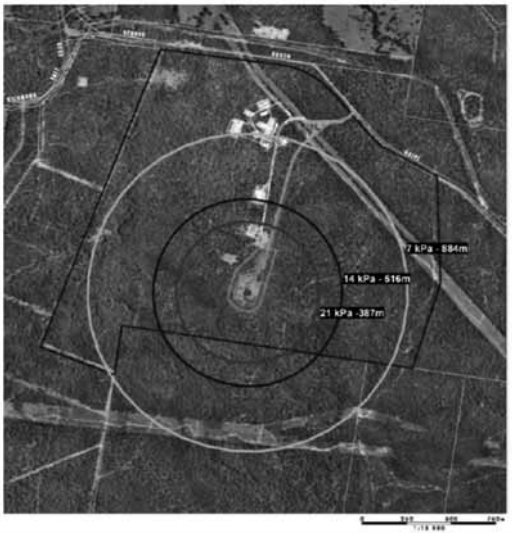
• **Toplumsal Risk:** Toplumsal risk için sıklığın sonuçlara göre çizilmiş diagramıdır. Bu, F-N eğrisi olarak da bilinir. Burada F sıklığı, N ise istenmeyen çıktıların (örneğin; ölen insan sayısı) kümülatif değerini ifade eder.

• **Coğrafi Risk:** Belirli bir alan için yaralanmalar, ekonomik maliyetler ve çevresel hasarlar olarak istatistiksel olarak beklenen kayıp oranıdır.

Hassasiyet Analizi; bununla yakında ilgili olup herbir model parametresindeki değişime karşılık modeldeki değişimi inceler.

Büyük Endüstriyel Kazaların Önlenmesi ve Etkilerinin Azaltılması Hakkında Yönetmelik'in Ek II'de verilen güvenlik raporu'nda bulunması gereken asgarî bilgiler madde 4.2'de; yönetmeliğin 17 ve 21 inci maddeleri göz önünde bulundurularak, kuruluştan kaynaklanabilecek büyük kazalardan etkilenmesi muhtemel alanları gösteren haritalar, görüntüler veya uygun olduğu durumda benzer tanımlamaları içeren, tanımlanmış büyük kazaların ***sonuçlarının, boyutunun ve şiddetinin değerlendirilmesi*** istenmektedir.

Şekil 17: Örnek Patlama Sonuç Analizi Modellemesi



9.7. Risk Müdahalesi (Kontrol Önlemlerinin Belirlenmesi)

Risk değerlendirmesi tamamlandığında; risk müdahalesi, riskin tekrarlanma olasılığını, risklerin etkilerini ya da her ikisini değiştirmeye yönelik bir veya daha fazla seçenek arasından tercih yapmayı, kararlar almayı ve söz konusu seçenekleri uygulamaya koymayı içerir.

Bu süreci, yeni risk düzeyinin yeniden değerlendirilmesini gerektiren döngüsel süreç takip eder. Burada amaç, daha fazla müdahalenin gerekip gerekmediğine karar verilmesi için önceden belirlenmiş olan kriterler doğrultusunda riskin tahammül edilebilirliğini saptamaktır. Söz konusu risklerin önlenmesinde kullanılan temel yöntemlerin hiyerarşi sıralamasını yapıcak olursak aşağıdaki gibi bir sıra karşımıza çıkacaktır;

1. Riskin Ortadan Kaldırılması (Elimine Etmek): Tesis içerisinde yüksek risk taşıyan materyalin, makinanın veya prosesin elimine edilmesidir. Örneğin; Teknolojisi eski olan ve çift el kumanda yada fotosel tertibatı yapılamayan presin kullanımdan kaldırılması.

2. Yerine Koyma (Substitusyon): Eğer tehlike elimine edilemiyorsa, yüksek risk taşıyan materyal, makina veya proses daha az risk taşıyan ile değiştirilmelidir. Örneğin; proses içerisinde kullanılan toksik veya çabuk yanıcı bir çözücünün, toksik olmayan ve parlama noktası yüksek bir çözücü ile değiştirilmesi.

3. Kontrol ve İzolasyon: Eğer tehlike elimine edilemiyor yada ikame edilemiyorsa tehlike kaynağı materyal, makina, ekipman veya proses izole edilmelidir. Tehlike kaynağını izole etmek mümkün değil ise kontrolünün sağlanması için tehlikeli durumdan etkilenen insan sayısının azaltması, etkilenme süresinin azaltılması, miktarının azaltılması sağlanmalıdır. Örneğin; boyahanede kullanılan boyaların daha az tehlikeli (su bazlı gibi) boyalarla değiştirilmesi mümkün olmuyor ise kapalı sistem boya kabini kullanılarak tehlike izole edilebilir, bir hastanede çalışan ve röntgen çeken bir sağlık elemanının çalışma saati azaltılabilir (günde beş saat), mevzuata uygun yıllık izin (senede dört hafta) kullandırılır.

4. Mühendislik Kontrolü: Dizayn mühendisleri, elimine, ikame ve izole edilemeyen ve kontrolü sağlanamayan tehlikeyi gidermek için makinanın, tesisatın veya prosesin tasarımı üzerinde çalışır. Mühendislik kontrolü ayrıca korunma yolları, bariyerler, operasyon noktası koruyucuları, sıkışma - ezme noktaları, hareket eden parçaların korunması vb. koruyucu donanımların hangisinin nerede nasıl kullanılabileceğine karar verir.

5. Yönetimle İlgili Kontroller: Yönetimle İlgili Kontroller ise güvenli iş akışı ve düzeni, güvenlik sistemleri, çalışma prosedürleri gibi yazıların yayımlanması yoluna başvurur. Bu amaçla;

- Riski ortadan kaldırma süreci belirlenir
- Sorumlulukların ataması yapılır
- İşçinin karakteristiği ve prosesteki işin gerekliliği hesaba katılır
- Eğitim prosedürleri oluşturulur
- Çalışma izin formları oluşturulur
- İşçinin olaya ilgisini sağlama ve sürdürme prosedürü hazırlanır
- İş akışı şeması üzerinde çalışılır
- İşçileri bilgilendirme ve katılımlarını sağlamak üzere formlar oluşturulur
- İşyeri düzeni ile ilgili çalışma yapılır

İdari olarak riski ortadan kaldırma yöntemleri olarak prosedürlerin hazırlanarak yayınlanması (resmen ilan etmek), yürütüm (uygulama) sağlanması ve güvenlik operasyonlarının yapılması gereklidir. Tehlike tanımlama aşamasında sağlık ve güvenlik açısından oluşturulan risk haritaları göz önüne alınarak, işletmede/fabrikada işaretlemeler yapılmalıdır.

Belirlenen kontrol önlemleri uygulamaya konur, ancak tanımlanan her gerekli risk azaltma ve kontrol önlemleri ile ilgili değişiklikler uygulamaya konulmadan önce denenmelidir. Kontrol önlemleri; öncelikle tehlikelerin bertaraf edilmesi ve riskin ortadan kaldırılması prensibini yansıtmalıdır, risk ortadan kaldırılamıyorsa azaltılma yoluna gidilir, riskin azaltılması için personel koruyucu teçhizatın kullanılması ise son çare olarak düşünülmelidir. Riskin ortaya çıkma ihtimalinin önlenmesi, azaltılması veya hasarın potansiyel şiddet derecesinin azaltılması sırası ile amaçlanır. Uygun kontrol ölçümleri bu aşamada devreye girer. Ölçümler uygulanırken uzun zaman alabilir çünkü değişim için gelen direnç nedeniyle sık sık eğitim, techizat satın alınması veya tesisat da değişikliğe ihtiyaç duyulabilir.

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği madde 10'a göre risklerin kontrolünde şu adımlar uygulanır.

- **Planlama:** Analiz edilerek etkilerinin büyüklüğüne ve önemine göre sıralı hale getirilen risklerin kontrolü amacıyla bir planlama yapılır.

- **Risk kontrol tedbirlerinin kararlaştırılması:** Riskin tamamen bertaraf edilmesi, bu mümkün değil ise riskin kabul edilebilir seviyeye indirilmesi için aşağıdaki adımlar uygulanır.
  - o Tehlike veya tehlike kaynaklarının ortadan kaldırılması.
  - o Tehlikelinin, tehlikeli olmayanla veya daha az tehlikeli olanla değiştirilmesi.
  - o Riskler ile kaynağında mücadele edilmesi.
- **Risk kontrol tedbirlerinin uygulanması:** Kararlaştırılan tedbirlerin iş ve işlem basamakları, işlemi yapacak kişi ya da işyeri bölümü, sorumlu kişi ya da işyeri bölümü, başlama ve bitiş tarihi ile benzeri bilgileri içeren planlar hazırlanır. Bu planlar işverence uygulamaya konulur.
- **Uygulamaların izlenmesi:** Hazırlanan planların uygulama adımları düzenli olarak izlenir, denetlenir ve aksayan yönler tespit edilerek gerekli düzeltici ve önleyici işlemler tamamlanır. Risk kontrol adımları uygulanırken toplu korunma önlemlerine, kişisel korunma önlemlerine göre öncelik verilmesi ve uygulanacak önlemlerin yeni risklere neden olmaması sağlanır.

Belirlenen risk için kontrol tedbirlerinin hayata geçirilmesinden sonra yeniden risk seviyesi tespiti yapılır. Yeni seviye, kabul edilebilir risk seviyesinin üzerinde ise bu maddedeki adımlar tekrarlanır.

9.8. Belgelendirme

Risk değerlendirme sürecinin, değerlendirmeden elde edilen sonuçlar ile birlikte belgelendirilmesi gerekmektedir. Riskler, anlaşılabilir terimlerle açıklanmalı ve risk düzeyinin açıklandığı bölümler net olmalıdır.

Raporun uzunluğu, değerlendirmenin hedef ve kapsamına dayalı olacaktır. IEC ISO 31010: 2009'a göre oldukça basit nitelik taşıyan raporlar dışında, risk değerlendirme raporlarında belgelendirilecek unsurlar arasında şunların bulunması gerektiği belirtilmiştir:

- Hedefler ve kapsam;
- Sistemin ilgili parçaları ve bunların fonksiyonlarına ilişkin tanımlamalar,
- Kurumun değerlendirilmekte olan durum, sistem veya koşullar ile nasıl ilişkilendirildiğine ve iç ve dış bağlamına dair bir özet,
- Benimsenen risk kriterleri ve bunların değerlendirilmesi,

- Hipotezlerin sınırlılıkları, varsayımları ve değerlendirilmeleri,
- Değerlendirme yöntemi,
- Risk tanımlama sonuçları,
- Veriler, varsayımlar ve bunların kaynakları ile geçerlilikleri,
- Risk analiz sonuçları ve bunların değerlendirilmesi,
- Duyarlılık ve belirsizlik analizi,
- Kritik varsayımlar ve kontrol edilmesi gereken diğer faktörler,
- Sonuçların irdelenmesi,
- Sonuç ve öneriler,
- Referanslar.

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği madde 10'a göre risk değerlendirmesi asgarî aşağıdaki hususları kapsayacak şekilde dokümante edilir.

- İşyerinin unvanı, adresi ve işverenin adı.
- Gerçekleştiren kişilerin isim ve unvanları ile bunlardan iş güvenliği uzmanı ve işyeri hekimi olanların Bakanlıkça verilmiş belge bilgileri.
- Gerçekleştirildiği tarih ve geçerlilik tarihi.
- Risk değerlendirmesi işyerindeki farklı bölümler için ayrı ayrı yapılmışsa her birinin adı.
- Belirlenen tehlike kaynakları ile tehlikeler.
- Tespit edilen riskler.
- Risk analizinde kullanılan yöntem veya yöntemler.
- Tespit edilen risklerin önem ve öncelik sırasını da içeren analiz sonuçları.
- Düzeltici ve önleyici kontrol tedbirleri, gerçekleştirilme tarihleri ve sonrasında tespit edilen risk seviyesi.

Yönetmeliğe gore risk değerlendirmesi dokümanının sayfaları numaralandırılarak; gerçekleştiren kişiler tarafından her sayfası paraflanıp, son sayfası imzalanır ve işyerinde saklanır. Risk değerlendirmesi dokümanı elektronik ve benzeri ortamlarda hazırlanıp arşivlenebilir.

9.9. İzleme ve Gözden Geçirme (Güncelleme)

Risk değerlendirmesi süregelen bir risk yönetim sürecini destekliyorsa; sistem, organizasyon, donanım veya faaliyetin kullanım süresi boyunca sürdürülebilecek bir şekilde gerçekleştirilmeli ve belgelendirilmelidir. Söz konusu değerlendirme, hatırı sayılır yeni bilgiler edinildikçe ve bağlam, yönetim sürecinin gereksinimleri doğrultusunda değiştikçe güncellenmelidir.

Risk değerlendirme süreci, bağlama ve zaman içerisinde değişmesi beklenen ve risk değerlendirmesini değiştirebilecek ya da geçersiz kılabilecek diğer faktörlere dikkat çekecektir. Söz konusu faktörler, risk değerlendirmesini gerektiğinde güncellenebilmesi amacıyla devam etmekte olan izleme ve inceleme çalışmaları için özellikle belirlenmelidir. Risk değerlendirmesinin geliştirilmesi için gözlemlenmesi gereken veriler de tanımlanmalı ve toplanmalıdır. Risk analizinde kullanılmak üzere çeşitli verilerin sağlanması için kontrollere ilişkin verimliliğinin kontrol edilmesi ve belgelendirilmesi; delil ve belgelerin oluşturulması ve incelenmesine yönelik sorumlulukların tanımlanması gerekmektedir.

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği madde 10'a göre yapılmış olan risk değerlendirmesi; tehlike sınıfına göre çok tehlikeli, tehlikeli ve az tehlikeli işyerlerinde sırasıyla en geç iki, dört ve altı yılda bir yenilenir. Aşağıda belirtilen durumlarda ortaya çıkabilecek yeni risklerin, işyerinin tamamını veya bir bölümünü etkiliyor olması göz önünde bulundurularak risk değerlendirmesi tamamen veya kısmen yenilenir.

- İşyerinin taşınması veya binalarda değişiklik yapılması.
- İşyerinde uygulanan teknoloji, kullanılan madde ve ekipmanlarda değişiklikler meydana gelmesi.
- Üretim yönteminde değişiklikler olması.
- İş kazası, meslek hastalığı veya ramak kala olay meydana gelmesi.
- Çalışma ortamına ait sınır değerlere ilişkin bir mevzuat değişikliği olması.
- Çalışma ortamı ölçümü ve sağlık gözetim sonuçlarına göre gerekli görülmesi.
- İşyeri dışından kaynaklanan ve işyerini etkileyebilecek yeni bir tehlikenin ortaya çıkması.

10. BÖLÜM: RİSK DEĞERLENDİRME METODOLOJİLERİNİN SINIFLANDIRILMASI

Endüstrideki yıllar boyunca gelişme sonucunda ileri teknoloji içeren proses ve sistemler yüksek karmaşıklığa sahip omuşlardır. Bu durum ise, insan, makine ve teçhizat gibi sebeplerden kaynaklanan kazaları sayıca artırmıştır. Kazalara neden olan potansiyel tehlikelerin incelenmesi, günümüzde yaygın bir şekilde kullanılan "Risk Değerlendirme Metodolojileri"nin ortaya çıkmasını sağlamıştır. Genel anlamda risk değerlendirme metodolojileri, kaza meydana getirme potansiyeline sahip olan her teknolojinin sistemlerinin analiz edilesi yoluyla kazaya açık olan yönlerinin tespit edilmesi, kazaya sebebiyet verebilecek faktörlerinin ve bileşenlerinin belirlenmesi ve ortadan kaldırılması ile kazaların önüne geçilmesini amaçlar.

Sistemlerin karmaşıklığı arttıkça değişik amaca hizmet eden farklı risk değerlendirme metodolojilerinin kullanım gereksinimi artmıştır. Tüm dünyadaki risk değerlendirme metodolojilerine yani yöntem bilimlerine ve standartlara baktığımızda ise 150'den fazla yöntem bulunduğunu görürüz. Bu yöntemlerden en çok kullanılanları aşağıda verilmiştir;

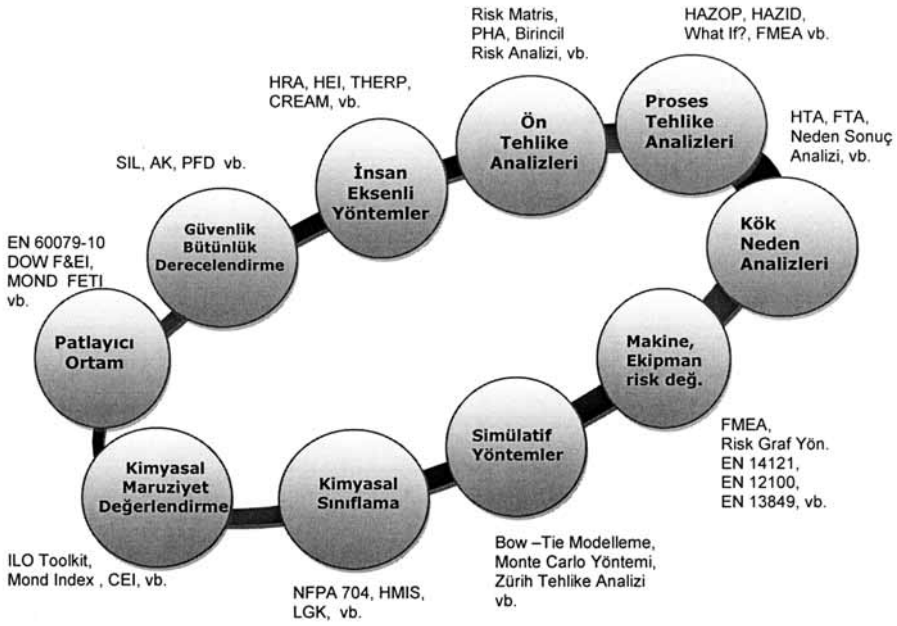
- Ön Tehlike Analizi (Preliminary Hazard Analysis – PHA),
- İş Güvenlik Analizi (Job Safety Analysis - JSA),
- Olursa Ne Olur? (What İf..?),
- Çeklist Kullanılarak Birincil Risk Analizi -(Preliminary Risk Analysis-PRA Using Checklists),
- Birincil Risk Analizi -(Preliminary Risk Analysis (PRA),
- Risk Değerlendirme Karar Matrisi (Risk Assessment Decision Matrix)
  a) L Tipi Matris
  b) Çok Değiskenli X Tipi Matris Diyagramı
- Tehlike ve İşletilebilme Çalışması (Hazard and Operability Studies - HAZOP),
- Tehlike Derecelendirme İndeksi (DOW index, MOND index, NFPA index),
- Hızlı Derecelendirme Metodu (Rapid Ranking, Material Factor),

- Hata Ağacı Analizi (Fault Tree Analysis -FTA),
- Hata Modu ve Etki Analizi (Failure Mode and Effects Analysis-FMEA)
- Hata Modu ve Etkisinin Kritiklik Analizi (Failure Mode and Critically Effects Analysis- FMECA),
- Güvenlik Denetimi (Safety Audit),
- Olay Ağacı Analizi (Event Tree Analysis - ETA),
- Neden - Sonuç Analizi (Cause and Consequence Analysis),
- Neden - Etki Analizi (Cause and Effect Analysis),
- Kinney Metodu (Mathematical Risk Evaluation Method),
- Karar Şeması (Decision Tree),
- Çok Kriterli Karar Analizi (Multi Criteria Decision Analysis -MCDA),
- Zürih Tehlike Analizi (Zurih Hazard Analysis),
- Makine Risk Değerlendirme (Mashine Risk Asessment),
- Toksikolojik Risk Değerlendirme veya Kimyasal Maruziyet Değerlendirme (Toxicological Risk Assessment - Chemical Exposure Assessment),
- Çevresel Risk Değerlendirmesi (Environmental Risk Assessment)
- Tehlike Analizi ve Kritik Kontrol Noktaları (Hazard Analysis and Critical Control Points - HACCP)
- Güvenlik Fonksiyon Analizi (Safety Function Analysis),
- Güvenilirlik Merkezli Bakım(Reliability Centred Maintenance – RCM)
- Sneak Analizi -Sneak Devre Analizi (Sneak Analysis - Sneak Circuit Analysis)
- İş Etki Analizi (Business Impact Analysis)
- İnsan Hata Tanımlaması (Human Error Identification - HEI),
- İnsan Güvenilirlik Değerlendirmesi (Human Reliability Assessment - HRA),

- İnsan Hata Oranı Tahmini Tekniği (Technıque For Human Reliability Analysis -THERP),
- Kavramsal Güvenilirlik ve Hata Analiz Yöntemi (Cognitive Reliability and Error Analysis Method - Cream),
- Hiyerarşik Görev Analizi (Hierarchical Task Analysis),
- Sapma Analizi (Deviation Analysis),
- Yönetim Bakışı ve Risk Ağacı (Management Oversight and Risk Tree - MORT),
- Enerji Analizi (Energy Analysis),
- Güvenlik Bariyer Diyagramları (Barrier Diagram),
- Koruma Katmanları Analizi (Layers of Protection Analysis - LOPA)
- Bow-Tie Metodolojisi,
- Kök Neden Analizi (Root Cause Analysis),
- Senaryo Analizi (Scenario Analysis),
- Markov Analizi (Markov Analysis),
- Monte Carlo Analizi (Monte-Carlo Analysis),
- Bayesian Analizi (Bayesian Analysis),
- F-N Eğrileri (F-N Curves).

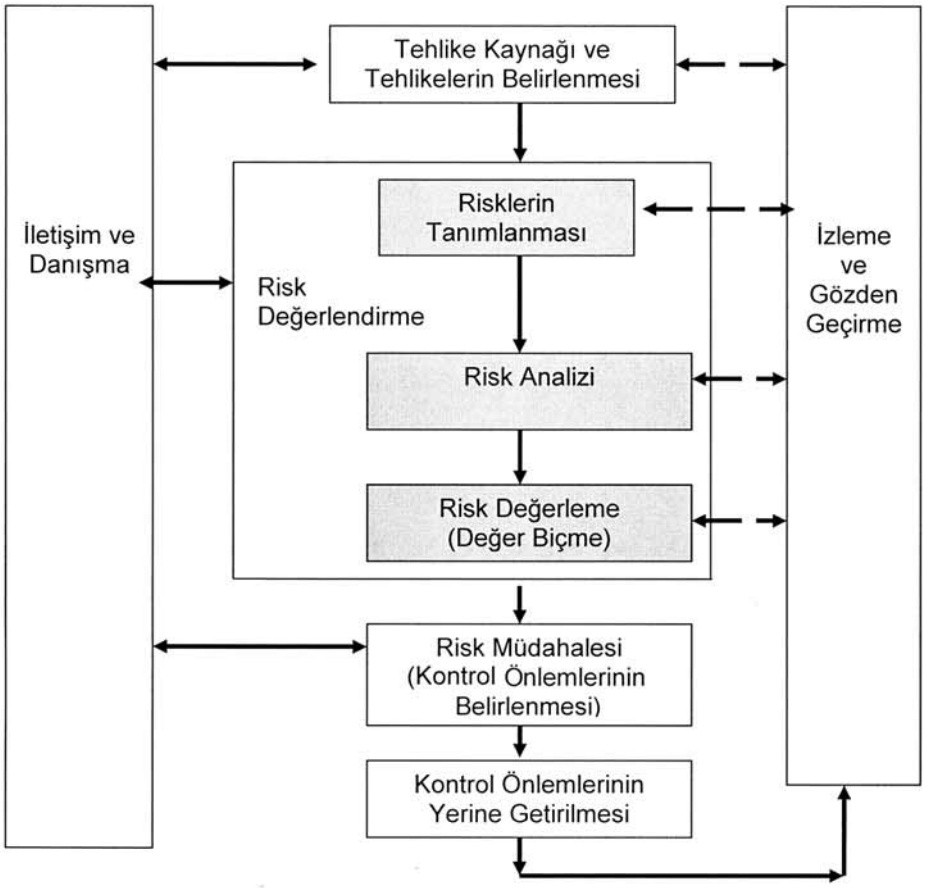
Bu yöntemlerin birçoğu ihtiyaçtan doğmuştur, özellikle de sigorta şirketleri, üniversiteler, enstitüler ile NASA'nın bu yöntem bilimlerin çeşitlenmesinde büyük rolleri olmuştur. Endüstriyel fabrikaları sigortalayan şirketler bu fabrikalardaki iş sağlığı ve güvenliğini ilgilendiren tehlikeler, yangın, patlama, deprem, sel, çevre felaketi vb. konulardaki risklerinin net olarak tayin edilmesini istemiş ve bir çok yöntemin geliştirilmesinde öncülük yapmışlardır. Örneğin; Zürih Sigortanın geliştirdiği Zürih Tehlike Analizi, DOW Chemical Co.'nun geliştirdiği DOW F&EI indeksi gibi. Risk değerlendirme metodolojilerini sınıflandırmaya çalışırken öncelikle hangi amaca hizmet ettikleri ve kullanıldıkları alanların dikkate alınması gereklidir, bu kriterlere göre risk değerlendirme metodolojilerini Şekil 18'deki şekilde sınıflandırmaya çalışabiliriz.

Şekil 18: Risk Değerlendirme Metodolojilerinin Sınıflandırılması



IEC ISO 31010: 2011 Uluslararası Standartı, risk değerlendirmesine ilişkin sistematik tekniklerin seçimi ve uygulanması konusunda işverenlere, iş güvenliği uzmanlarına ve işyeri hekimlerine rehberlik etmek amacı ile hazırlanmıştır. Bu standart doğrultusunda gerçekleştirilen risk değerlendirmesi, diğer risk yönetim faaliyetlerine de katkıda bulunmaktadır. Standart tekniklerin uygulanması ve kapsam hakkında daha ayrıntılı bilgilerin sunulduğu diğer uluslararası standartlara belirli atıflarda bulunarak, birçok tekniğin uygulanmasına ilişkin tanımlamalar yapmıştır. Aynı zamanda bu standart, tüm teknikleri ifade etmemektedir. Dolayısıyla, herhangi bir tekniğin dahil edilmemesi, söz konusu tekniğin geçersiz olduğu anlamına gelmemektedir. Herhangi bir yöntemin belirli bir durum için uygulanabilir olması, yine o yöntemin mutlak suretle kullanılması gerektiğini de vurgulamamaktadır. Risk değerlendirme teknikleri, risklere ilişkin güçlü ve zayıf yönlerinin anlaşılması amacıyla çeşitli yollarla sınıflandırılabilmektedir. IEC ISO 31010: 2011' da sunulan tablolar, açıklayıcı amaçlarla bazı olası teknikler ve ait oldukları kategoriler arasında bağlantı kurmaktadır. Söz konusu tekniklerin her biri, sağladıkları değerlendirmenin niteliği ve belirli durumlarda uygulanabilirliklerine yönelik rehberlikleri bakımından da standartta daha ayrıntılı bir biçimde açıklanmıştır.

Şekil 19: Risk Değerlendirme Yönetim Süreci Genel Bakış



IEC ISO 31010: 2011 uluslararası standartında **Tablo 2** ve **Tablo 3**'de risk değerlendirme yönetim süreci içerisindeki adımlardan aşağıda gösterildiği gibi risk değerlendirme sürecinin her aşamasında tekniklerin nasıl uygulanabileceğini gösteren karşılaştırmalar yapılmıştır. Bu adımlar;

- Risk tanımlaması;
- Risk analizi – niteliksel, yarı niceliksel veya niceliksel olasılık hesaplaması;
- Risk analizi – mevcut kontrollerin verimliliğinin değerlendirilmesi;
- Risk analizi – risk düzeyinin hesaplanması;

- Risk değerlemesi.

Eğer gerekli ise;

- Risk analizi – sonuç analizi;

Risk değerlendirme yöntemlerine ilişkin türlerin örnekleri, her yöntemin söz konusu nitelikler bakımından yüksek, orta ve düşük şeklinde derecelendirildiği **Tablo 2**'de listelenmiştir. Risk değerlendirme sürecindeki her bir aşama için yöntemin uygulanması, oldukça uygulanabilir, uygulanabilir veya uygulanamaz şeklinde tanımlanma yapılarak karşılaştırmalar verilmiştir.

Tablo 2: Risk Değerlendirme Araçlarına İlişkin Seçimin Öz Nitelikleri

Risk Değerlendirme Tekniğinin Türü	Tanım	Etkileyici Faktörlerin Uygunluğu			Kantitatif Bir Sonuç Doğurabilir mi?
		Kaynak ve Olanaklar	Belirsizliğin Niteliği ve Düzeyi	Güçlük Düzeyi	
ARAŞTIRMA YÖNTEMLERİ					
Kontrol Listeleri (Çeklistler)	Risk tanımlanmasının oldukça basit bir biçimidir. Aynı zamanda göz önünde bulundurulması gereken belirsizliklerin listelenmesini öngören bir tekniktir. Kullanıcılar, önceden geliştirilmiş liste, kod veya standartlardan faydalanabilirler.	Düşük	Düşük	Düşük	Hayır
Ön Tehlike Analizi	Belirlenmiş bir faaliyet, olanak veya sistem için hasar teşkil edebilecek tehlike, tehlikeli durum ya da	Düşük	Yüksek	Orta	Hayır

Tablo 2'nin devamı 1

	olayları saptama amacı güden, tümevarımsal ve basit bir analiz yöntemidir.				
DESTEKLEYİCİ YÖNTEMLER					
Yapılandırılmış Görüşmeler ve Beyin Fırtınası	Geniş kapsamlı bir dizi fikir ve değerlendirmelerin toplanarak, ekip tarafından derecelendirme aracıdır.	Düşük	Düşük	Düşük	Hayır
Delphi Tekniği	Kaynağı destekleyen ve tanımlama, olasılık, sonuç hesaplaması ve risk değerlemesini etkileyen uzman görüşlerinin bir araya getirildiği araçtır. Uzmanlar arasında uzlaşma sağlanmasına yönelik işbirlikçi bir tekniktir; bağımsız analiz ve uzman oylamasını içerir.	Orta	Orta	Orta	Hayır
...Olursa Ne Olur? Tekniği (What If? veya SWIFT)	Herhangi bir ekibin riskleri tanımlamaya teşvik edilmesidir. Normal şartlarda elverişli hale getirilmiş işyerlerinde kullanılmakla birlikte, risk analizi ve değerleme teknikleri ile	Orta	Orta	Hiç	Hayır

Tablo 2'nin devamı 2

	ilişkilidir.				
İnsan Güvenilirlik Değerlendirmesi (HRA)	İnsan Güvenilirlik Değerlendirmesi (HRA), insanların sistem performansı üzerindeki etkisini ele alır ve sistem üzerindeki hata etkilerini değerlendirmek için kullanılır.	Orta	Orta	Orta	Evet
SENARYO ANALİZLERİ					
Kök Neden Analizi (Tekli Kayıp Analizi)	Yardımcı etkenlerin ve gelecekte bu tür zararların yaşanmasını önlemek adına sistem veya sürecin nasıl geliştirilebileceğinin anlaşılması için meydana gelen tekli bir zarar analiz edilir. Söz konusu analiz, zarar meydana geldiğinde hangi kontrollerin mevcut olduğunu ve kontrollerin nasıl geliştirilebileceğini dikkate alır.	Orta	Düşük	Orta	Hayır
Senaryo Analizi	Hayal gücü ya da içinde bulunulan duruma ilişkin kestirim yoluyla geleceğe yönelik olası senaryolar tanımlanır.	Orta	Yüksek	Orta	Hayır

Tablo 2'nin devamı 3

	Tanımlanan senaryoların her birini göz önünde bulundurduğu düşünülen farklı riskler meydana gelebileceği öngörülür. Söz konusu analiz resmi, gayri resmi, kalitatif veya kantitatif şekilde gerçekleştirilebilir.				
Toksikolojik Risk Değerlendirmesi	Tehlikeler tanımlanıp analiz edildikten sonra, belirli bir hedefin maruz kalmış olabileceği kaynaklar saptanır. Maruziyet düzeyi ve belirli bir maruziyet düzeyinin yol açtığı zararın niteliğine ilişkin bilgiler, zararın yaşanma olasılığını önlemek için bir araya getirilir.	Yüksek	Yüksek	Orta	Evet
İş Etki Analizi	Temel aksaklık risklerinin, organizasyonun faaliyetlerini nasıl etkileyebileceğine ilişkin bir analiz sağlar ve bunun için gereken olanakların niceliğini belirtir.	Orta	Orta	Orta	Hayır
Hata Ağacı	İstenmeyen olaydan	Yüksek	Yüksek	Orta	Evet

Tablo 2'nin devamı 4

Analizi (FTA)	(en önemli olay) başlayarak, bunun meydana gelebileceği tüm yolları belirleyen bir yöntemdir. Söz konusu olaylar, mantıksal ağaç diyagramında grafik olarak gösterilir. Hata ağacı tamamlandığında, olası nedenlerin/kaynakların azaltılması veya ortadan kaldırılması üzerinde durulur.				
Olay Ağacı Analizi (ETA)	Başlangıç niteliğindeki olayların olası sonuçlara dönüştürüldüğü tümevarımsal akıl yürütme tekniklerinin kullanımına dayalıdır.	Orta	Orta	Orta	Evet
Neden-Sonuç Analizi	Süre gecikmesi de dahil olmak üzere hata ve olay ağacı analizlerinin bir araya getirilmesidir. Başlangıç niteliğindeki olayın neden ve sonuçları birlikte değerlendirilir.	Yüksek	Orta	Yüksek	Evet
Neden-Etki Analizi	Meydana gelen bir etki, farklı kategorilere	Düşük	Düşük	Orta	Hayır

Tablo 2'nin devamı 5

	ayrılabilecek çok sayıda yardımcı etkene sahip olabilir. Katkıda bulunan faktörler beyin fırtınası yoluyla sıklıkla tanımlanır ve bir ağaç yapısı veya balık kılçığı diyagramı ile gösterilir.				
FONKSİYON ANALİZLERİ					
Hata Modu ve Etki Analizi Metodolojisi (FMEA) **Hata Modu ve Etkisine İlişkin Kritiklik Analizi (FMECA)**	FMEA (Arıza Modu ve Etki Analizi), arıza modlarını, mekanizmalarını ve etkilerini tanımlayan bir tekniktir. Çok sayıda FMEA türü mevcuttur: bileşen ve ürünler için kullanılan Tasarım (veya ürün) FMEA; sistemler için kullanılan Sistem FMEA; üretim ve montaj süreçlerinde kullanılan Süreç FMEA; Hizmet FMEA ve Yazılım FMEA. FMEA, her bir arıza modunun önemini niteliksel, yarı niceliksel veya niceliksel şekilde tanımlayan bir kritiklik	Orta	Orta	Orta	Evet

Tablo 2'nin devamı 6

	analizi (FMECA) tarafından takip edilebilir. Kritiklik analizi, arıza modunun sistem arızasına yol açacağı olasılığına, arıza modu ile ilişkili risk düzeyine veya risk öncelik sayısına dayalı olabilir.				
Güvenilirlik Merkezli Bakım	Her bir ekipman için güvenlik, güvenilirlik, kullanılabilirlik ve operasyon tasarrufunun verimli ve etkili bir biçimde sağlanması adına arızaların giderilmesi için çeşitli politikaların belirlenmesi yöntemidir.	Orta	Orta	Orta	Evet
Sneak Devre Analizi (Gizlilik Devre Analizi)	Tasarım hatalarının saptanmasına yönelik bir yöntemdir. Sneak durumu; gizli bir donanım, yazılım veya istenmeyen bir duruma yol açan, istenen faaliyeti engelleyen ya da bileşen arızasından kaynaklanmayan entegre bir koşuldur. Söz konusu durumlar, rastlantısal özellikleri ve en titiz şekilde	Orta	Orta	Orta	Hayır

Tablo 2'nin devamı 7

	standartlaştırılmış sistem testlerinde bile algılanmama yeterlilikleri ile nitelendirilirler. Sneak durumları, hatalı işletim, sistem kullanılabilirlik kaybı, program gecikmeleri ve hatta personel ölümü ya da yaralanmasına yol açabilir.				
Tehlike ve İşletilebilirlik Çalışması (HAZOP)	Olası veya amaçlanan performansta meydana gelen sapmaların belirlenmesi için genel bir risk tanımlama sürecidir. Anahtar ve klavuz kelimelere dayalı bir sistemden faydalanır. Sapmaların kritiklik düzeyi değerlendirilir.	Orta	Yüksek	Yüksek	Hayır
Tehlike Analizi ve Kritik Kontrol Noktaları (HACCP)	Belirlenmiş limitler çerçevesinde olması gereken özel niteliklerin ölçümü ve izlenmesi yoluyla ürün kalitesi ve güvenilirliği ile süreç güvenliğinin sağlanması için sistematik, proaktif ve önleyici bir sistem	Orta	Orta	Orta	Hayır

Tablo 2'nin devamı 8

	analizidir.				
KONTROL DEĞERLENDİRMELERİ					
Koruma Katmanları Analizi (LOPA)	Aynı zamanda bariyer analizi şeklinde de adlandırılabilir. Kontrollerin ve kontrollere ilişkin etkililiğin değerlendirilmesine olanak tanır.	Orta	Orta	Orta	Evet
Papyon Analizi (Bow-Tie)	Tehlikelerden sonuçlara risk yollarını tanımlama, analiz etme ve kontrolleri gözden geçirme amaçlı basit, diyagramlı bir yöntemdir. Olayların nedenlerini analiz eden hata ağacı (papyon diyagramı ile temsil edilir) ile sonuçları analiz eden olay ağacının mantıksal bir kombinasyonu şeklinde düşünülebilir.	Orta	Yüksek	Orta	Evet
İSTATİSTİKSEL YÖNTEMLER					
Markov Analizi	Kimi zaman durum uzayı analizi şeklinde de adlandırılan Markov analizi, kısıtlanmış çeşitli durumlar da dahil olmak üzere birçok	Yüksek	Düşük	Yüksek	Evet

Tablo 2'nin devamı 9

	durumda mevcut olan onarılabilir karmaşık sistemlerin analizinde yaygın bir şekilde kullanılır.				
Monte - Carlo Simülasyonu	Monte Carlo simülasyonu, her bir girdinin belirli bir dağılıma sahip olduğu ve girdilerin belirlenmiş ilişkiler yoluyla çıktılara bağlı olduğu her girdi için, sistemde meydana gelen sapmalar sonucu sistemdeki sapma kümesinin oluşturulmasında kullanılır. Analiz, çeşitli girdilere ilişkin etkileşimlerin matematiksel olarak saptanabileceği özel bir model için kullanılabilir. Girdiler, temsil etmeleri planlanan belirsizliğin niteliği doğrultusunda çok sayıda dağılım türüne dayalı olabilir. Risk değerlendirmesi için genellikle üçgen dağılımı veya beta dağılımı yaygın şekilde kullanılır.	Yüksek	Düşük	Yüksek	Evet
Bayes Analizi	Sonuca ilişkin olasılığın değerlendirilmesi için ön	Yüksek	Düşük	Yüksek	Evet

Tablo 2'nin devamı 10

	dağılım verilerinden faydalanan istatistiksel bir prosedürdür. Bayes analizi, kesin bir sonucun elde edilmesi için ön dağılım verilerinin doğruluğuna dayanır. Bayes yöntemi, sonuç elde etmek için çeşitli girdilerin olasılıksal ilişkilerini elde tutarak, birçok bölgede modelin sebep ve etki ağını oluşturur.				

Tablo 3: Risk Değerlendirmesi İçin Kullanılan Araçların Uygulanabilirliği

Araç ve teknikler	Risk değerlendirme süreci				
	Risk tanımlama	Risk analizi			Risk değerleme
		Sonuç	Olasılık	Risk düzeyi	
Beyin Fırtınası	Oldukça uygulanabilir	Uygulanamaz	Uygulanamaz	Uygulanamaz	Uygulanamaz
Delphi Tekniği	Oldukça uygulanabilir	Uygulanamaz	Uygulanamaz	Uygulanamaz	Uygulanamaz
Kontrol Listeleri	Oldukça uygulanabilir	Uygulanamaz	Uygulanamaz	Uygulanamaz	Uygulanamaz
Ön Tehlike Analizi	Oldukça uygulanabilir	Uygulanamaz	Uygulanamaz	Uygulanamaz	Uygulanamaz
Tehlike ve İşletilebilirlik Çalışması (HAZOP)	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir	Uygulanabilir
Tehlike Analizi	Oldukça	Oldukça	Uygulanamaz	Uygulanamaz	Oldukça

Tablo 3'ün devamı 1

ve Kritik Kontrol Noktaları (HACCP)	uygulanabilir	uygulanabilir			uygulanabilir
Çevresel Risk Değerlendirmesi	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir
..Olursa Ne Olur? (What If? - SWIFT)	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir
Senaryo Analizi	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir	Uygulanabilir
İş Etki Analizi	Uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir	Uygulanabilir
Kök Neden Analizi	Uygulanamaz	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir
Hata Modu ve Etki Analizi (FMEA)	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir
Hata Ağacı Analizi	Uygulanabilir	Uygulanamaz	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir
Olay Ağacı Analizi	Uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir	Uygulanamaz
Neden -Sonuç Analizi	Uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir
Neden - Etki Analizi	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanamaz	Uygulanamaz	Uygulanamaz
Koruma Katmanları Analizi (LOPA)	Uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir	Uygulanamaz
Karar Şeması	Uygulanamaz	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Uygulanabilir
İnsan Güvenilirlik	Oldukça	Oldukça	Oldukça	Oldukça	Uygulanabilir

Tablo 3'ün devamı 2

Değerlendirmesi (HRA)	uygulanabilir	uygulanabilir	uygulanabilir	uygulanabilir	
Papyon Analizi (Bow-Tie)	Uygulanamaz	Uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir
Güvenilirlik Merkezli Bakım	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir
Sneak Devre Analizi	Uygulanabilir	Uygulanamaz	Uygulanamaz	Uygulanamaz	Uygulanamaz
Markov Analizi	Uygulanabilir	Oldukça uygulanabilir	Uygulanamaz	Uygulanamaz	Uygulanamaz
Monte Carlo Simülasyonu	Uygulanamaz	Uygulanamaz	Uygulanamaz	Uygulanamaz	Oldukça uygulanabilir
Bayes İstatistikleri ve Bayes Ağları	Uygulanamaz	Oldukça uygulanabilir	Uygulanamaz	Uygulanamaz	Oldukça uygulanabilir
F-N Eğrileri	Uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Oldukça uygulanabilir
Risk İndeksleri (Dow& FEI, Mond FETI vb.)	Uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Oldukça uygulanabilir
Risk Matrisleri	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Oldukça uygulanabilir	Uygulanabilir
Çok Kriterli Karar Analizi (MCDA)	Uygulanabilir	Oldukça uygulanabilir	Uygulanabilir	Oldukça uygulanabilir	Uygulanabilir

11. BÖLÜM: RİSK DEĞERLENDİRME METODOLOJİLERİNİN İNCELENMESİ

Risk değerlendirme metodolojilerini birbirinden ayıran en önemli farklar, risk değerini bulmak için kullandıkları kendilerine has metodlardır. Bu kitapta özellikle metedolojilerin karşılaştırılması ile kalitatif ve kantitatif yöntemlerinin farkları ve uygulanabilecekleri sektörler ve uygulayacak analistlerin tecrübe gereksinimleri incelenecektir. Endüstrilerde en fazla kullanılan ve en çok bilinen belli başlı risk değerlendirme yöntemlerini inceleyeceğiz ve örneklerle de bu yöntemleri daha iyi anlamaya çalışacağız.

11.1. Beyin Fırtınası Tekniği (Brainstorming)

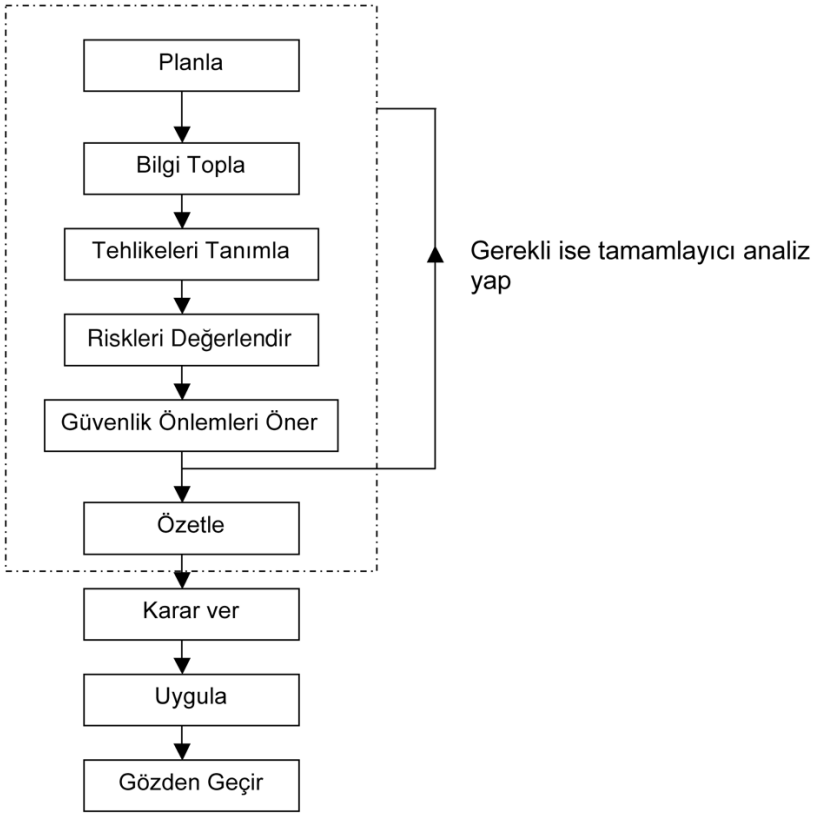
Beyin fırtınası, potansiyel arıza modlarını ve bunlarla ilişkili tehlike ve riskleri belirlemek için, karar verme kriterleri ve/veya değerlendirme seçeneklerine yönelik bilgili kişilerden oluşan bir grup arasındaki teşvik edici ve ilham verici niteliklerde yapılan konuşma şeklindeki bir tekniktir. İşyerindeki tehlikeler ve bulardan korunma yolları konusunda bilgilenmek isteyen birçok ilgili taraf bulunmaktadır. Ancak bu tarafların farklı ilgi alanları olabilir ve herhangi bir analizde birbirinden farklı talepleri ortaya çıkabilir. İşte bu aşamada beyin fırtınası tekniği kişilere veri sağlar. İlgili taraflara örnek verecek olursak;

- İşyerinde riske en yakın, yaralanma ihtimali en fazla olan çalışanlar,
- Çalışmayan fakat risk altında olanlar. Örneğin, tehlikeli tesise yakın oturanlar,
- İşverenler veya tesislerin sahipleri,
- İşveren kuruluşların yönetimi,
- Dizayn yapan kişiler (fakat operasyondan sorumlu olmayanlar),
- Kamu otoritesi ve denetleyiciler,
- İşyerlerinden mal alan müşteriler,
- Sigorta şirketleridir.

‘’Beyin Fırtınası’’ terimi genellikle her türlü grup tartışmasını ifade etmek için kullanılmaktadır. Ancak, gerçek bir beyin fırtınası insanların hayal gücünün grup içersindeki diğer kişilerin düşünceleri ve ifadeleri ile tetiklenmesini sağlamaya yönelik girişimler için özel teknikler içermektedir. Beyin fırtınası tekniği sonuçlarına örnekler aşağıdakileri kapsar:

- İşyerindeki risklerin genel gözden geçirmesi,
- İşyerindeki tehlikelerin listesi ve bunların değerlendirmeleri,
- İşyeri için alınacak güvenlik önlemleri,
- Belli kazaların nasıl meydana gelebileceğinin detaylı açıklaması, bunların meydana gelme ihtimali ve muhtemel sonuçları.
- Bir kazanın incelenmesi, teknik, insani ve organizasyonel faktörlerin olaya etkisinin irdelenmesi,
- İşyerinde alınmış güvenlik önlemlerinin özeti ve bunların etkinliğinin değerlendirmesi,
- Katılımcıların üretim ve güvenlik sisteminin işleyişine dair daha kapsamlı bilgilendirilmesidir.

Şekil 20: Beyin Fırtınası Uygulama Aşamaları



Bu teknikte etkili bilgi akışı ve ön araştırma çok önemlidir. İlham verici başlangıç konuşması sonrasında, grubun analiz yapılan alanlardaki tehlike kaynaklarını ve olası etkilerini tartışması ve sorunları saptamaya çalışması, beyin fırtınasının genel özellikleridir.

Beyin fırtınası tekniğinin merkezi bileşeni tehlikelerin ve sistemde kazaya neden olabilecek diğer faktörlerin tanımlanmasıdır. Amaçlardan biri ana tehlike kaynaklarını tespit etmek ve hangi faktörlerin kazayı tetiklediğini ortaya çıkarmaktır. Seçilecek diğer risk değerlendirme yöntemleri ile tehlike tanımlaması sürecinin nasıl ilerleyeciği de belirlenebilir. O tehlike kaynağına özel bir risk değerlendirme yöntemi kullanılmaz ise bazı tehlikeler keşfedilir iken bazıları gözden kaçabilir.

Ancak yanlızca beyin fırtınası tekniği ile risk değerlendirmesi yapmak çok yetersiz kalır, bu nedenle beyin fırtınası aşağıda açıklanan diğer risk değerlendirme yöntemleri ile birlikte kullanılır. Risk yönetim sürecinin ve bir sistemin yaşam döngüsünün her aşamasında bu yönteme ihtiyaç duyulabilir. Ayrıca sorunların belirlendiği yüksek düzeyli tartışmalar ve daha detaylı bir inceleme için ya da özel problemlere yönelik detaylı seviyedeki tartışmalar için kullanılabilir.

Beyin fırtınası hayal gücünün üzerinde önemle durmaktadır. Bu nedenle özellikle herhangi bir verinin olmadığı veya problem çözümlerinin gerekli olduğu yeni bir teknolojinin kullanımı durumunda riskleri tahmin etmek üzere kullanışlıdır. Organizasyon, sistem, işlem veya uygulama hakkında bilgi sahibi olan bir grup kişi ile değerlendirme yapılabilir. Beyin fırtınası önceden hazırlanan bilgiler ışığında katılımcılar ile birlikte şu süreçleri içerecek şekilde kullanılır;

- Oturum yöneticisi öncelikle, oturum amaçlarını belirler ve kurallarını açıklar,
- Oturum yöneticisi, düşünme sistemini hazırlar ve oturum öncesi içeriğe uygun olarak konuşmaları sorular ile tetikler,
- Düşünce zincirinden hareketle, herkes mümkün olduğu kadar sorunlara kendi fikirleri ile cevap vermeye çalışır,
- Tüm girdiler kabul edilir ve hiçbiri eleştirilmez,
- Grup etraflıca düşünmeyi tetiklemek amacıyla fikirlerin oluşmasına izin vermek için hızlıca hareket eder,
- Oturum yöneticisi, düşüncenin bir yönü tükendiğinde veya tartışma çok fazla saptığında, yeni bir yol izlemeleri için seçenekler sunabilir, ancak

amaç, daha sonraki analiz için mümkün olduğu kadar çok farklı fikirler toplamaktır.

Sonuçlar uygulanan risk yönetim sürecinin aşamasına bağlıdır, örneğin tanımlama aşamasındaki sonuçlar, bir risk ve mevcut kontrol listesi olabilir.

Güçlü Yönler:

- Yeni riskleri ve özgün çözümleri belirlemeye yardımcı olan hayal gücünü teşvik eder,
- Tüm çalışanlar tarafından rahatlıkla uygulanabilir ve dolayısıyla iletişime kapsamlı olarak yardım eder,
- Düzenlenmesi nispeten hızlı ve kolaydır.

Sınırlılıklar:

- Katılımcıların etkili katkılar sağlamak adına bilgi ve beceri eksikliği olabilir,
- Nispeten yapılandırılmamış olduğu için, sürecin anlaşılmasını, örneğin tüm potansiyel risklerin tespit edildiğinden emin olunmasını sağlaması zordur,
- Katılımcılardan bir kısmı tartışmaya hakim iken, değerli fikirleri olan insanların sessiz kaldığı belirli bir grup dinamiği olabilir. Konuşur vaziyette tartışarak veya normal grup tekniği kullanarak bilgisayar üzerinden beyin fırtınası yoluyla bunun üstesinden gelinebilir. Bilgisayar beyin fırtınası anonim olarak kurulabilir, böylelikle fikirlerin serbest akışını engelleyen kişisel ve siyasi sorunlardan kaçınılır.

11.2. Yapılandırılmış veya Yarı Yapılandırılmış Görüşmeler (Structured or semi-structured interviews)

Yapılandırılmış bir görüşmede, görüşme yapılan kişilerden bir durumu farklı bir bakış açısından görmeye teşvik eden ve daha önceden hazırlanmış bir dizi sorulara cevap verilmesi istenir ve böylelikle riskler belirlenmeye çalışılır. Yarı-yapılandırılmış bir görüşme de buna benzerdir, ancak ortaya çıkan sorunları keşfetmeye yönelik bir görüşme için daha fazla özgürlük sağlar. Bu yöntem özellikle çalışanların söz konusu faaliyet ile ilgili ortaya çıkan veya çıkabilecek tehlikeler hakkında bilgilerine başvurmak ve görüşlerini almak için uygundur, ancak yine tek başına risk değerlendirmesi faaliyetleri için yetersiz bir değerlendirme olarak kalabilir.

Uygulama Adımları:

Planlanmış sıra ile farklı adımlar takip edilebilir. Bu analizdeki ortak adımlar aşağıda verilmiştir:

- Sistem farklı bileşenlere ayrılarak sistemin basitleştirilmiş bir modeli elde edilir. Bu adıma "yapılandırma" denir,
- Sistemin her bileşeni için riskler (tehlikeler) ve kaza riskleri ile ilgli diğer faktörler tanımlanır,
- Risk değerlendirmesinin diğer teknikleri de kullanılabilir,
- Çoğu durumda güvenlik önlemlerinin önerildiği adım dahil edilir.

Yapılandırılmış ve yarı-yapılandırılmış görüşmeler bir beyin fırtınası oturumu için insanları bir araya getirmenin zor olduğu veya bir grupta serbest şekilde seyreden tartışmanın durum veya katılan insanlar için uygun olmadığı zamanlarda kullanışlıdır. Bu görüşmeler, riskleri belirlemek veya risk analizlerinin bir parçası olarak mevcut kontrollerin etkinliğini değerlendirmek için de sıklıkla kullanılır. Bir projenin veya sürecin herhangi bir aşamasında uygulanabilir. Ayrıca risk değerlendirmesine yönelik olarak taraflara girdi sağlayan bir yöntemdir.

Girdi:

- Faaliyet adımları,
- Faaliyet hedeflerinin net tanımları,
- Faaliyet adımları için tehlikeleri tanımlamak maksadı ile hazırlanmış bir dizi soruları içermektedir.

İlgili bir dizi soru, analizi yöneten uzmana rehberlik etmek için oluşturulur. Sorular analize katılan ve cevap veren kişiler için mümkün olduğu kadar uygun bir dilde ve basit olmalıdır ve sadece tek bir konuyu kapsamalıdır. Konuya açıklık getirmek için olası takip soruları ayrıca hazırlanmalıdır. Detaylandırma yapılırken, sorular açık uçlu olmamalıdır.

Güçlü Yönler:

- Uzmanlara bir faaliyet hakkında daha önceden fark edemedikleri durumları veya olayları keşfetmelerine imkan verir,
- Birebir çalışanlarla iletişim kurulması vasıtası ile tehlike kaynakları ve olası tehlikeler üzerinde daha derin düşünülmesini sağlar,
- Nispeten daha küçük bir gruba yönelik olan beyin fırtınasından daha fazla sayıda tarafın ve kişinin katılımına olanak sağlar.

Sınırlılıklar:

- Birden fazla görüşü bu yolla almak, analizi yapacak olan uzman için zaman alıcı bir yöntemdir,
- Önyargılar grup tartışması olmaması sebebi ile kapsam dışı bırakılamayabilir,
- Beyin fırtınasının bir özelliği olan hayal gücünü tetikleme durumu oluşamayabilir.

11.3. Delphi Tekniği (Delphi Technique)

Delphi tekniği, bir uzman grubundan güvenilir bir uzlaşma görüşü elde etmeye yönelik bir yöntemdir. Terim genellikle beyin fırtınasının herhangi bir şeklini ifade etmek için geniş çapta kullanılmasına rağmen, Delphi tekniğinin önemli bir özelliği, uzmanların süreç ilerledikçe diğer uzman görüşlerine sahip olurken, fikirlerini bireysel ve anonim olarak ve özgün bir biçimde formülleştirerek ifade etmeleridir.

Delphi tekniği risk yönetim sürecinin her aşamasında veya uzman görüşlerinin fikir birliğine ihtiyaç duyulduğu bir sistem kullanım döngüsünün her aşamasında uygulanabilir.

Uzlaşmanın gerekli olduğu bir dizi seçeneklerdir.

Bir grup uzmana yarı-yapılandırılmış bir anket kullanılarak sorular sorulur. Uzmanlar yüz yüze gelmez, böylece görüşleri bağımsızdır.

Süreç:

- Delphi sürecini üstlenmek ve izlemek için bir ekibin oluşturulması;
- Bir grup uzmanın seçilmesi (bir veya daha fazla uzman panelleri olabilir);
- Anketin test edilmesi;
- Panelistlere bireysel olarak anket gönderilmesi;
- İlk turda alınan cevapların analiz edilmesi, birleştirilmesi ve yeniden dolaştırılması;
- Panelistlerin cevap vermesi ve sürecin uzlaşma sağlanana kadar tekrarlanması.

Mevcut konu üzerinde uzlaşmaya yönelik bir noktada birleşme durumudur.

Güçlü Yönler:

- Görüşler anonim iken, popüler olmayan fikirlerin ifade olasılığı daha yüksektir;

- Tüm görüşler, kişilikleri yönetme problemini önleyen eşit bir ağırlığa sahiptir;
- Sonuçlara sahip olmayı sağlar;
- Kişilerin tek bir yerde, tek bir zamanda bir araya getirilmesine ihtiyaç yoktur;

Sınırlılıklar:

- Yoğun bir emek sarf edilir ve zaman kaybına neden olur;
- Katılımcıların yazılı olarak kendilerini açıkça ifade etmesi gerekir.

11.4. Ön Tehlike Analizi (Preliminary Hazard Analysis – PHA)

Mevzuatta "risk değerlendirmesi" gibi terimler sıklıkla genel anlamda kullanılmaktadır. Ön Tehlike Analizi, bir işletmede özellikle tasarım aşamasında ya da hiç risk değerlendirme çalışması yapılmamış bir tesiste ilk yapılacak risk değerlendirme metodolojisidir. Bu analizde riskler sistematik olarak incelenir ve belgelenerek değerlendirilir, ayrıca hangi tehlike kaynakları için diğer risk değerlendirme teknikleri ile analizin derinleştirilmesine karar verilir. Ülkeler arasında yasal mevzuat ve bunun uygulanması konusunda birçok farklılıklar vardır, ülkemizde ise 6331 sayılı İş Sağlığı ve Güvenliği Kanunu ve yönetmelikler çalışma ve güvenlik şartlarına ilişkin sorumlulukları tanımlamaktadır. Bu düzenlemeler incelendiğinde; tümünde sistematik güvenlik çalışması yapılması tezi savunulmakta ve bu çalışmaların da risk değerlendirmesi ile yapılması istenmektedir. Mevzuatlardaki ortak konular aşağıda verilmiştir:

- İşveren işyerinde sağlıklı ve güvenli bir çalışma ortamı sağlamakla yükümlüdür.
- İşyerindeki sağlık, güvenlik ve çevre yönetimi yeterli seviyede düzenlenmiş olmalıdır.
- Çalışanlar tehlikeler ve güvenli çalışma konusunda bilgilendirilmelidir.
- Tehlikeler tanımlanmalı ve değerlendirilmeli, gerekiyorsa azaltılmalı veya ortadan kaldırılmalıdır.

Ön tehlike analizi, tesisin son tasarım aşamasında ya da daha detaylı çalışmalara model olarak kullanılabilecek olan hızla hazırlanabilen kalitatif bir risk değerlendirme metodolojisidir. Genellikle, ön tehlike analizinde tehlike kaynakları, büyük kaza oluşma olasılıkları ve bunların sonuçları belirlenir. Ön tehlike analizi; tehlikeleri, tehlikeli durumları ve belirli bir etkinliğe, olanağa veya sisteme zarar verebilecek olayları tespit etme amacı güden basit ve tümevarımsal bir analiz yönetimidir.

Tasarım detayları veya işletim prosedürleri hakkında çok az bilgi varken, bir proje geliştirilmesi aşamasında en yaygın şekilde kullanılan yöntemdir. İleriki çalışmalara ya da bir sistem tasarımına yönelik bilgiyi sağlamak amacıyla da sıkça uygulanır. Tehlikelerin önceliklendirilmesi için mevcut sistemlerin analizinde, daha fazla incelemeye ihtiyaç duyulan risklerin analizinde veya daha kapsamlı bir yöntemin kullanılmasının mümkün olmadığı koşullarda (zaman ve maaliyeta nedeniyle) kullanımı önerilmektedir. Tehlike durumlar ve riskler aşağıdaki girdiler dikkate alınarak formülleştirilir:

- Değerlendirilecek sistem üzerindeki tasarım ayrıntıları,
- Proses akım diyagramları (P&ID, proses akım şemaları),
- Hammaddeler veya üretilen malzemeler,
- Kullanılacak kimyasallar ve reaksiyonlar;
- Kullanılacak ekipmanlar;
- İşletim şartları ve ortamı;
- Planlar (tapografya, yerleşim planları, yeraltı su haritaları vb.);
- Sistem bileşenleri ve arabirimler vb.

İstenmeyen bir olayın sonuç ve olasılıklarının kantitatif analizi daha ileriki risk değerlendirme çalışmalarında riskleri belirlemek üzere yapılabilir. Ön tehlike analizinin tasarım, yapım ve test aşamalarında yeni tehlikeleri tespit etmek ve gerekirse düzeltmeler yapmak amacıyla güncelleştirilmesi gerekir.

Elde edilen sonuçlar, tablolar halinde hazırlanır ve bu raporlar;

- Tehlike ve risk listesi;
- Kabul kriterleri,
- Tavsiye edilen kontroller,
- Tasarım özellikleri veya daha detaylı bir değerlendirme taleplerini kapsar.

Güçlü Yönleri:

- Sınırlı bir bilgi olduğunda kullanmak mümkündür,
- Sistem kullanım döngüsünde risklerin çok önceden dikkate alınmasına yardımcı olur.

Sınırlılıklar:

- Bir Ön Tehlike Analizi sadece ön bilgi sağlar; kapsamlı bir analiz değildir, ne ayrıntılı şekilde riskler hakkında bilgi verir, ne de en iyi şekilde nasıl önlenebileceği hakkında bilgi sağlar.

Eğer tesis Seveso (COMAH) Direktifi çerçevesinde bir kuruluş ise bir çok taraf bu sürece dahil olmalıdır. Bu taraflar, kapsam dahilindeki tesislerin isletmecileri, ilgili yetkili merciler, sivil toplum kuruluşları ve halktır ve bu tarafların risk değerlendirmesi hakkındaki bilgilere kolay erişimi önem arz etmektedir. Ön tehlike analizinin genel amacı, risklerle ilgili olarak alınacak kararlara akılcı bir temel sağlamaktır. Bu tür kararlar, risk analizinin sonuçları ile tolere edilebilir risk kriterleri karşılaştırılarak alınabilir. Dengeli bir karar oluşturabilmek için, çoğu durumda her bir olayın ayrı ayrı değerlendirilmesine ihtiyaç vardır. Tolere edilebilir risk konusu, sosyal, ekonomik ve politik hususları içeren son derece karmaşık bir konudur. Tehlikeler dört genel sınıf altında toplanabilir. Bu sınıflar:

- Tabiî afet tehlikeleri (seller, zelzeleler, kasırgalar, yıldırım, vb.),
- Teknolojik tehlikeler (sanayi tesisleri, binalar, ulaşım sistemleri, tüketim malları, böcek ilaçları, zirai mücadele ilaçları, ilaçlar, vb.),
- Sosyal tehlikeler (saldırı, savaş, sabotaj, bulaşıcı hastalıklar, vb.),
- Yaşam biçimi tehlikeleri (uyuşturucu madde kullanımı, alkol, sigara, vb.dir.

Belirtilen bu sınıfların karşılıklı olarak birbirinden bağımsız olmadığı bilinmekte ve teknolojik tehlikeler analiz edilirken genellikle diğer sınıflardaki faktörlerin (özellikle tabiî afet tehlikeleri) ve diğer sistemlerin etkilerinin, risk analizinin bir parçası olarak hesaba katılması gerekmektedir.

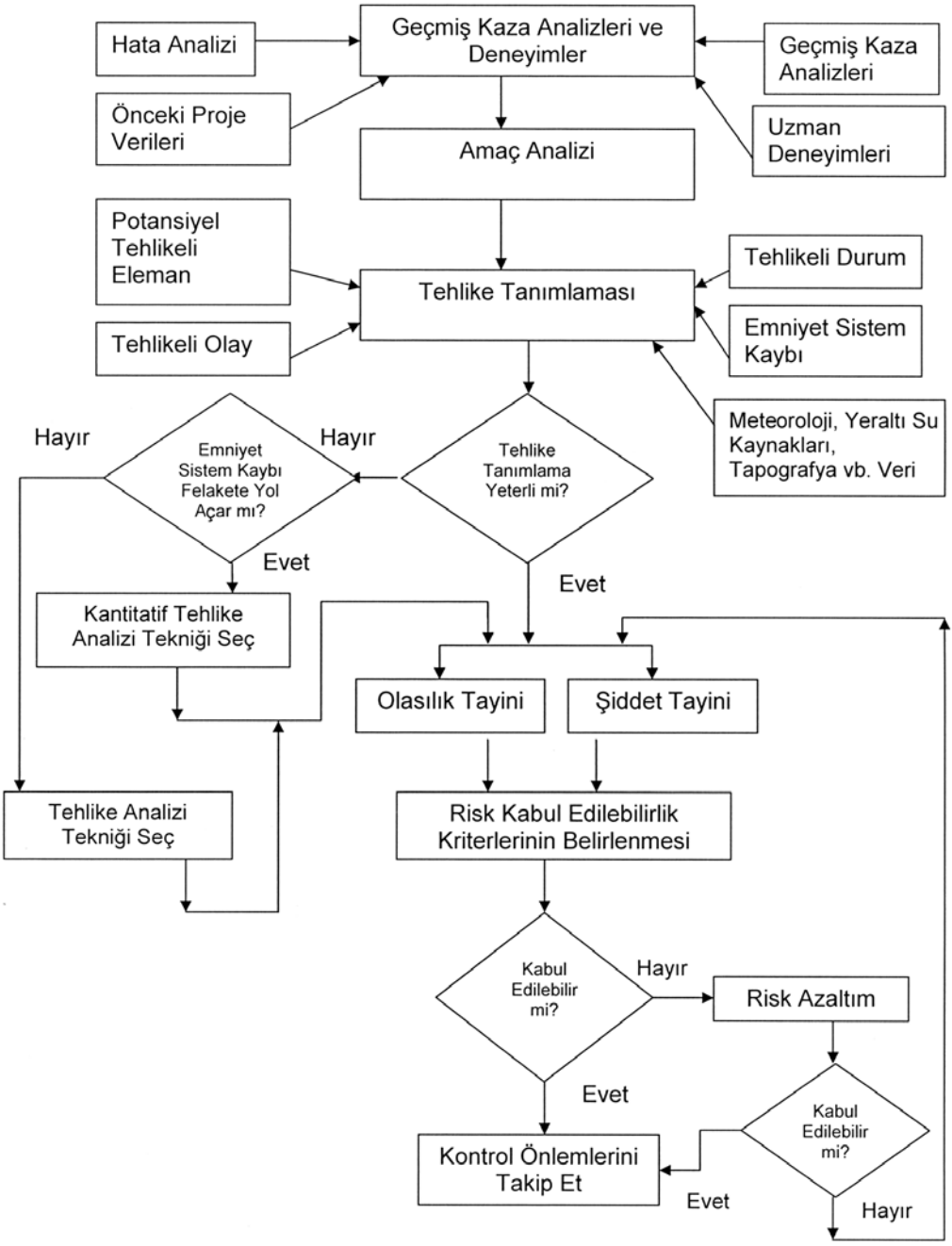
Riskler, incelenmeye konu olan, yol açtıkları sonuçların türüne göre de sınıflandırılabilir. Bu sınıflar, örneğin:

- Bireysel (vatandaşların bir kısmına kişisel olarak etki),
- Meslekî (Çalışanlara olan etki),
- Toplumsal (Genel olarak vatandaşlara olan etki),
- Mallara olan zarar ve ekonomik kayıplar (iş hayatının kesintiye uğraması, cezalar vb.),
- Çevreye olan etkilerdir. (toprağa, havaya, suya, bitki örtüsüne ve kültürel geleneklere olan etkiler)

Bir işletmenin kurulması aşamasında, oldukça fazla miktarda teknik bilginin toplanması, işlenmesi ve analiz edilmesi gerekmektedir. Ayrıca bu planlama aşamasında, risk kontrol faaliyetlerden acil durum yönetimine kadar tüm bilgilerin işletme içerisindeki bütün çalışanlara ve üçüncü kişilere dağıtılması gerekmektedir. Bir işletmenin kuruluş aşamasında yapılan ön tehlike analizi aşağıdaki safhalarda şu yararları sağlar;

- Kavram ve tarif/tasarım ve geliştirme safhaları:
  - Riske büyük katkısı olan unsurların ve konuyla ilgili önemli faktörlerin belirlenmesi,
  - Tasarım sürecine girdi sağlamak ve toplam tasarımın yeterliliğini değerlendirmek,
  - Tasarımda muhtemel güvenlik önlemlerini belirlemek ve değerlendirmek,
  - Önerilen potansiyel tehlikeli tesislerin, faaliyetlerin veya sistemlerin kabul edilebilirliklerinin değerlendirilmesine girdi sağlamak,
  - Normâl ve acil durum şartları için gerekli olan prosedürlerin geliştirilmesine yardımcı olacak bilgileri sağlamak,
  - Mevzuat ve diğer kurallarla ilgili riskleri değerlendirmek,
  - Seçenek tasarım kavramlarını değerlendirmek.
- İmalat, kurulum, işletme ve bakım safhalarında:
  - Öngörülen özelliklerle gerçek performansı karşılaştırma amacıyla kazanılan deneyimi izlemek ve değerlendirmek,
  - Normâl işletme, bakım/muayene ve acil durum prosedürlerinin en uygun hale getirilmesi için girdi sağlamak,
  - Riske büyük katkısı olan unsurlar ve riski etkileyen faktörler konusunda bilgi sağlamak,
  - İşletme kararlarının alınmasında riskin önem düzeyi konusunda bilgi sağlamak,
  - Organizasyon yapısında, işletme uygulamalarında ve prosedürlerinde ve sistem bileşenlerindeki değişikliklerin etkilerini değerlendirmek,
  - Eğitim gayretleri üzerine yoğunlaşmak.
- Devreden çıkarma safhası, hizmet dışı bırakma
  - Sistemin devreden çıkarma faaliyetleri ile ilgili riskleri değerlendirmek ve ilgili özelliklerin karşılanmış olduğunu güven altına almak,
  - Elden çıkarma prosedürlerine girdi sağlamak.

Şekil 21: Ön Tehlike Analizi Metodolojisi Aşamaları



Bu analiz kapsamında güvenlik zaafiyeti oluşabilecek tesisler, bölümler, prosesler, ekipman ya da makineler gibi tehlike kaynakları belirlenmeli, olası kaza sonuçları değerlendirilmeli ve yeterli önleme, kontrol ve azaltıcı önlemler belirlenmelidir. Bu bölümler, prosesler veya ekipmanlar bulundurdukları tehlikeli madde miktarı ve özellikleri ile bu bölümde gerçekleştirilen tehlikeli süreçlere göre belirlenmelidir.

Bu metodda olası sakıncalı olaylar önce tanımlanır daha sonra ayrı ayrı olarak çözümlenir. Herbir sakıncalı olay veya tehlike, mümkün olan düzelmeler ve önleyici ölçümler formüle edilir. Bu metodolojiden çıkan sonuç, hangi tür tehlikelerin sıklıkla ortaya çıktığını ve hangi analiz metodlarının uygulanmasının gerektiğini belirler. Tanımlanan tehlikeler, sıklık/sonuç diyagramının yardımı ile sıraya konur ve önlemler öncelik sırasına göre alınır. Ön tehlike analizi analistler tarafından erken tasarım aşamasında uygulanır, ancak tek başına yeterli bir analiz metodu değildir, diğer metodolojilere başlangıç verisi olması aşamasında yararlıdır.

Özellikle işyerinde/işletmede tehlikeli maddeler bulunması yada yüksek tehlike derecesi taşıyan proses veya sistem bulunduğu durumda ön tehlike analizi aşamasında "Proses Endüstrileri İçin Proses Tehlike Analizi Teknikleri ile Güvenlik Ölçümleme Sisteminin Uygulanması" gerektiğine karar verilebilir.

1. ADIM: Tehlike Tanımlama

Tehlikelerin tanımlanması adımı Ön Tehlike Analizi'nin en önemli aşamalarından biridir. İşletme içerisinde gerekli önlemlerin tanımlanabilmesi için işyerinde; ölüme, hastalığa, yaralanmaya, hasara veya diğer kayıplara sebebiyet verebilecek tüm istenmeyen durumların tanımlanması gereklidir. Ön tehlike analizinin başarısının en büyük sırrı ise bu potansiyel tehlike tanımlama aşamasının tesis kurulmadan ve işletilmeye başlanılmadan yapılmasıdır. İnsan sağlığına, çevreye veya mala herhangi bir zarar verme potansiyeline sahip olan durum, potansiyel bir zarar kaynağı, tehlikeli bir malzeme olabileceği gibi, yapılan bir aktiviteden de kaynaklanabilir. Tehlikelar tanımlanırken mutlaka aşağıdaki hususlara dikket edilmelidir, tehlikeler;

- Bir veya daha fazla sisteme, prosese, alana, ekipmana veya çalışana yönelik olabilir,
- Bir veya daha fazla aşamada karşımıza çıkabilir,
- Aynı tehlike değişik işletim aşamalarında veya farklı sistemlerde değişik riskler oluşturabilir,

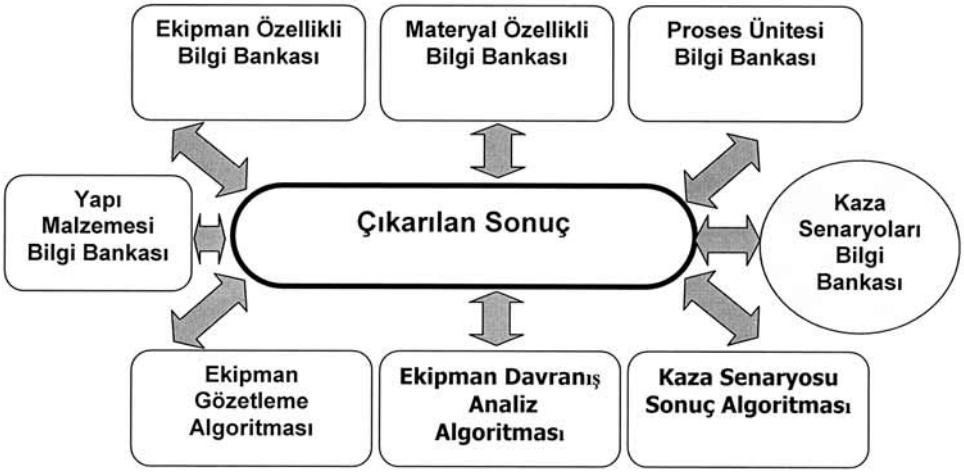
• Bir kaza oluşturana dek tanımlanamayabilir.

Ön tehlike analizini tek bir analist yerine beyin fırtınası gerçekleştirebilecek bir ekibin gerçekleştirmesi daha doğru olacaktır böylece hem tehlike kaynaklarını hem de potansiyel tehlikeleri tanımlamakta daha etkili olunacaktır. Kaynakların ve zamanın sınırlı olması durumunda ise tehlikelerin tanımlanmasında uzman kişilerin yardımının alınması uygun olacaktır.

Yeni kurulmaya ya da işletilmeye başlanılacak bir kuruluşda öncelikle "Risk Haritası" oluşturulması gereklidir. İşletmede/işyerinde yaralanma, kayma, düşme, ölüm, malzeme düşmesi, meslek hastalığı, makine - ekipman zararları, kimyasal maddelerle temaslar, yangın, patlama v.b. tehlikeler tanımlanarak ve bu tanımlamalara göre işyerinin "Risk Haritaları" ve "Bilgi Bankaları" oluşturulur.

Oluşturulan bilgi bankaları kullanılarak Ekipman Gözetleme Analiz, Ekipman Davranış Analiz ve Kaza Senaryosu Sonuç Algoritması oluşturulur, böylece Kaza Senaryoları Bilgi Bankası oluşturulabilir. Risk haritası oluşturulmuş bir işletmede Risk Yönetim Prosesini oturtmak çok daha kolaydır.

Şekil 22: Kaza Senaryosu Bilgi Bankası

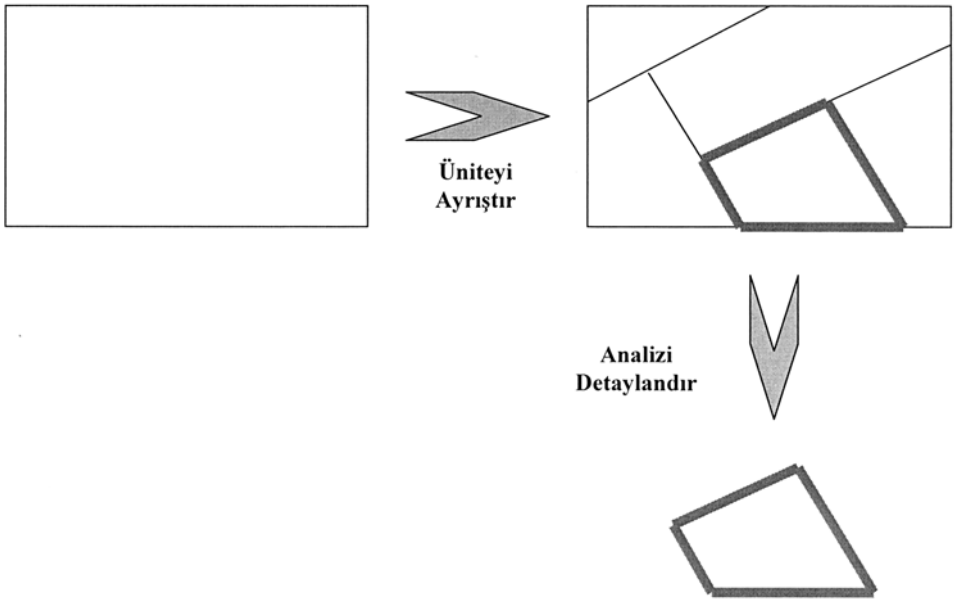


Risk haritalarının hazırlanması aşamasında öncelikle makro ve mikro ayrıştırma uygulanmalıdır, çünkü işletmelerin/işyerlerin her yeri aynı oranda tehlike taşımamaktadır. Bu işlemin yapılması risk değerlendirmesi yapıcak, İş Güvenliği Uzmanına veya takımına hem zaman kazandıracak hemde maddi

kaybı engelliyecektir. Bu aşamada; işyerinde tehlikeli bölümlerinin tehlike derecelerine göre birbirinden ayrıştırılması gereklidir.

Eğer tesiste büyük kaza oluşturma potansiyeli olan tehlikeli sistem, proses veya ekipman varsa, bu aşamada risk haritalarının oluşturulması ve tesise makro ve mikro açıdan bakılması daha da önem kazanmaktadır. Özellikle Seveso II Direktifi kapsamında üst seviyeli kuruluşlar için ise risk haritalarının oluşturulması olmazsa olmaz adımların başında gelmektedir. Olasılıklar ve bunların sonuçları belirlenir. Özellikle bu tür tesisler için; risk değerlendirmesinde büyük kazaların gerçekleşme olasılıkları değerlendirilmek ve insan ve çevrenin korunması için yeterli önlemlerin alındığının ispatlanması gerekmektedir. İzlenilen yöntem/yaklaşım ne olursa olsun, ön tehlike analizi kapsamında güvenlik ile ilgili tesisler veya bölümler belirlenmiş, potansiyel tehlike kaynakları tanımlanmış, olası kaza sonuçları değerlendirilmiş ve yeterli önleme, kontrol ve azaltıcı önlemler belirlenmiş olmalıdır. Yine bu tür tesisler için ön tehlike analizi bölüm, proses veya ekipmanlarda ne tür Tehlike Analizi teknikleri kullanmaları gerektiği konusunda da yönlendirici ve yardımcı olacaktır.

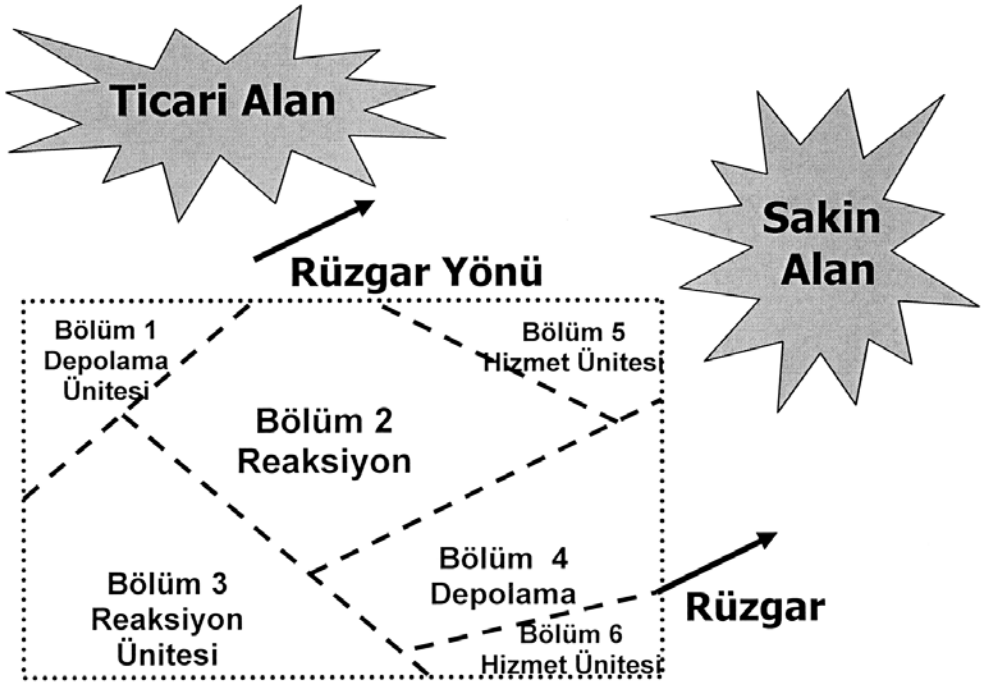
Şekil 23: Makro Ayrıştırma Algoritması



Makro ayrıştırma yapılırken işyerinin tapografyası, yeraltı suları, meteroloji vb. bilgiler de dikkate alınmalıdır, özellikle kimyasal madde depolama tankları, dış proses üniteleri, liman, dolum üniteleri içeren yerlerde mutlaka dış etkilerde(sabotaj, rüzgar, sel, çevre işyeri, vb.) hesaba katılmalıdır. Burada önemli olan, büyük bir kazaya yol açabilecek koşullara sahip olan tüm tesis veya tesis bölümlerinin belirlenmesidir.

Makro ayrıştırma uygulanırken özellikle kimyasal proses ünitesi içeren yada yanıcı, parlayıcı, patlayıcı maddelerle çalışmalar yapılan veya basınçlı kapların bulunduğu bölümler işaretlenmelidir. Mikro ayrıştırma uygulanırken bu bölümlerdeki etkiler de göz önüne alınarak, işyerlerinde mutlaka yangın, patlama, sabotaj, deprem, sel, savaş hali, iş kazaları ve çevreye zarar veren felaketlerin meydana gelme olasılığına göre **"Acil Eylem Planı"**nın hazırlanması gerekir. Bu planda acil çıkış kapıları ile yolları, yangın söndürme hortumları, yangın söndürücüler, motopomplar ile acil bir durumda bina dışında sakin bir alanda toplanmak için alanların belirlenmiş olması gereklidir.

Şekil 24: Makro Ayrıştırma



Yine bu acil eylem planının, büyük bir felaket halinde işletmenin makul bir sürede yeniden eski haline dönme oluşumunu sağlayacak yönetim ve uygulamalarını içermelidir, bu plamlara **"Acil Durum Geri Dönüş Planları"** denmektedir. Herhangi bir acil durum veya kriz durumu karşısında bu durumu karşılama ve yönetmeye hazır olunmasını sağlamak için organizasyon ve düzenlemelerin yapılması gereklidir.

Acil eylem gerektiren haller;

a) Yangın,

b) Patlama,

c) Deprem,

d) Sel,

e) İnsan sağlığını tehdit edici bir olay,

f) Çevre sağlığına etki edici bir olay,

g) Büyük hasar, zarar ve ziyan yaratacak durumlar,

h) Domino etkisi,

i) İnsan sağlığının hemen yada uzun vadede etkilenmesine neden olabilecek kimyasal madde/gaz ve zehirli maddelerin dökülmesine veya yayılmasına neden olan olay.

2.ADIM: Geçmiş Verilerin Analizi

Bu analiz aşamasında geçmis kazalardan alınan dersler ve edinilen deneyimler oldukça önemli bir katkıda bulunabilir. Ön tehlike analizi yapılırken, geçmiş kazalar ve eğer tutuluyorsa tehlikeli durum ve kazaya ramak kalma kayıtları da dikkate alınarak geçmiş deneyim verileri ile analiz yapılır. Bu aşama çok önemlidir, çünkü hangi metodolojilerin kullanılacağına karar verilmesi aşamasında büyük rol oynar. Söz konusu iş ve işlemler ile ilgili deneyimler ve geçmiş kaza analizleri işletmede daha çok hangi hataların meydana gelebileceği hususunda analiste veri sağlar.

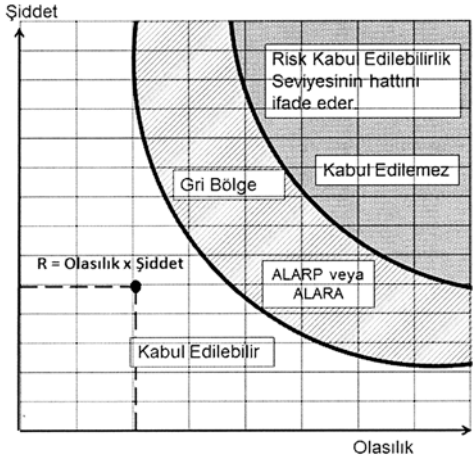
Bir sonraki adım ise amaç analizidir, bu aşamada istenilen hedefler belirlenir. Tehlike belirlenmesi aşamasında; potansiyel tehlikeli elemanlar, tehlikeli durumlar, tehlikeli olaylar, olası emniyet sistem kayıpları veri olarak kullanılır. İşletmenin tehlikeli durum ve geçmiş kaza kayıtları tutulmamış veya yeni faaliyete geçmiş bir

işletme olması durumunda aynı iş kolundaki işletmelerdeki kaza örnekleri veri olarak kullanılabilir, analistin tecrübesi bu aşamada büyük önem taşır.

3.ADIM: Risklerin Önceliklendirilmesi

Ön tehlike analizi sürecinde, risk seviyelerinin kabul edilebilirliğinin önceden tesis edilmiş kriterler ile kıyaslaması yapılması gereklidir. Ancak bu kabul edilebilir risk düzeyinin limitlerinin belirlenmesi gereklidir. Bu düzeyler bazı ülkelerde devlet otoriteleri tarafından tanılanmış veya onaylanmıştır, ancak bu şekilde bir durum yok ise o zaman işyeri üst düzey yöneticileri tarafından bu limitler belirlenmedir. Unutulmaması gereken husus ise kabul edilebilirlik kriterleri belirlenirken daha önce anlatıldığı üzere ALARP mı yoksa ALARA mı kabulünün yapıldığının bir prosedür aracılığı ile açıklanması gereklidir. Bu bir kabuldür ve tabiki de her kabulde olduğu gibi yöneticilere bir sorumluluk da yüklemektedir. O nedenle risk kabul kriterleri belirlenirken örnek tesislerde, standartlarda ya da farklı ülkelerde kullanılan kriterlerin esas alınması önerilmektedir. Bu limitler bir risk matris değerlendirmesinde tanımlanmış risk matrisi sınırları olabilir.

Şekil 25: Kabul Edilebilirlik Kriteri



Risk kabul kriterleri hücrelere ayrılarak bulunur.

	ŞİDDET				
OLASILIK	(1) Katostrofik (Felakete Yol Açan)	(2) Tehlikeli	(3) Marjinal (Pek az)	(4) Düşük	(5) Önemsiz
(A) Sık sık Tekrarlanan	1A	2A	3A	4A	5A
(B) Muhtemel	1B	2B	3B	4B	5B
(C)Ara Sıra Olan	1C	2C	3C	4C	5C
(D) Pek Az	1D	2D	3D	4D	5D
(E) İhtimal Dışı (Olanaksız)	1E	2E	3E	4E	5E

Belirlenen potansiyel tehlikelerin "Ön Tehlike Analizi Risk Derecelendirme ve Seçim Diyagramı" kullanılarak frekansı ve şiddetine göre risk skoru belirlenir. Burada dikkat edilmesi gereken bir husus şiddetin "felakete yol açan", "tehlikeli", "marjinal" ve "önemsiz" olarak değerlendirilmesidir. Yapılan risk değer-

lendirmesi sonucunda kabul edilemez bölgelerde çıkan bir risk skoru elde edilmesi durumunda prosesin/işletmenin mekanik bütünlüğünün korunması için alınan kontrol önemlerinin tehlike potansiyelini azaltmak için yeterli olmadığı anlamı çıkmaktadır.

Belirlenen her tehlikeden doğabilecek riskler tahminler yapılarak analiz edilir. Olayların ortaya çıkma olasılığı ve ortaya çıktığında maruz kalınabilecek sonuçlar belirlenir.

Risk skoru, olasılık ve şiddetin çarpımından elde edilir.

Risk Skoru= Olasılık x Şiddet

Zararın sonucu için derecelendirme **Tablo 4**'te verilmiştir. Tehlikenin, hedefi etkileme şekli tanımlanmış, hedef olarak; kişi, ekipman, işgücü, ürün, çevresel faktörlere yer verilmiştir. Her bir tehlikeye göre hedefte ortaya çıkabilecek zarar tanımlanmıştır.

Tablo 4: Şiddet Tablosu

	ŞİDDET				
KATEGORİ	**İNSAN**	**EKİPMAN/ PROSES ZARARI**	**DURUŞ**	**ÜRÜN KAYIP/ MALİYET**	**ÇEVRESEL ETKİSİ**
(1) Katostrofik (Felakete Yol Açan)	Ölüm	> 1Milyon	> 4 ay	> 1Milyon	Felaket, 5 yıl ve/ veya çevresel zarar
(2) Tehlikeli	Ciddi yaralanma, meslek hastalığı	250 Bin-1 Milyon	2 haftadan 4 aya kadar	250 Bin-1 Milyon	1-5 yıl arası zarar
(3) Marjinal (Pek az)	Yaralanma, yatarak tedavi	10 Bin-250 Bin	1 günden 2 haftaya	10 Bin-250 Bin	1 yıldan az zarar
(4) Düşük	Ölüm veya meslek hastalığı yok	< 10 Bin	< 1 gün	< 10 Bin	Önemsiz
(5) Önemsiz	Hiçbir kalıcı veya geçici etki yok	< 1 Bin	< 1 saat	< 1 Bin	Önemsiz

Zararın ortaya çıkma ihtimali için derecelendirme **Tablo 5**'te verilmiştir.

Tablo 5: Olasılık Tablosu

OLASILIK	
DERECE	**KATEGORİ**
A	Sık Sık Tekrarlanan
B	Muhtemel
C	Ara Sıra Olan
D	Pek Az
E	İhtimal Dışı (Olanaksız)

Olasılık ile şiddetin çarpımından elde edilen risk skoru **Tablo 6**'da verildiği üzere kesiştirilerek risk skoru belirlenir. Bu matris yardımıyla riskin kabul edilebilirlik değerleri bulunur.

Tehlikelerin belirmesi aşamasında verilmesi gereken önemli bir karar daha bulunmaktadır. Şayet tesiste makro açıdan ya da mikro açıdan yapı-

Tablo 6: Ön Tehlike Analizi Risk Değerlendirme Seçim Diyagramı

	ŞİDDET				
OLASILIK	(1) Katostrofik (Felakete Yol Açan)	(2) Tehlikeli	(3) Marjinal (Pek az)	(4) Düşük	(5) Önemsiz
(A) Sık sık Tekrarlanan	1A	2A	3A	4A	5A
(B) Muhtemel	1B	2B	3B	4B	5B
(C)Ara Sıra Olan	1C	2C	3C	4C	5C
(D) Pek Az	1D	2D	3D	4D	5D
(E) İhtimal Dışı (Olanaksız)	1E	2E	3E	4E	5E

lan incelemede işletme içerisindeki sistem, proses veya ekipmanlarda ortaya çıkabilecek tehlikelerin belirlenmesi aşamasında, katostrofik yani felakete yol açabilecek derecede yüksek şiddete sahip tehlikelerin olabileceğinden şüphelenilmesi durumunda veya bu tehlikelerden birine rastlanıldığında bu tesisle ilgili daha ayrıntılı tehlike değerlendirmesi yapılmasına gerekli olup olunmadığının kararının verilmesi gerekmektedir. Bir sonraki adım ise; incelemesi yapılan sistem, proses veya ekipmanı daha ayrıntılı incelemek ve meydana gelebilecek tehlikeleri belirlemek üzere hangi risk değerlendirme metodlarının seçileceğine karar verilmesidir.

Tablo 7: Örnek Ön Tehlike Analizi Risk Değerlendirme

Tarih :	12.01.2013	**ÖN TEHLİKE ANALİZİ**			Değerlendirme No:	1
Proses/Sistem :	Akü Şarj Odası Tasarım	**RİSK DEĞERLENDİRME TABLOSU**			Düzenleyen:	İş Güvenliği Uzmanı
Alt Sistem :	Havalandırma, Elektrik				Revizyon No:	1
Dizayn Rehberi:					Revizyon Tarihi:	12.01.2013
Takım:	İşveren Vekili, Fabrika Müdürü, İş Güvenliği Uzmanı, Bakım Amiri, İşletme Müh., Elektrik Müh.				Sayfa:	1
Potansiyel Tehlike Eleman	**Tehlikeli Olay Nedeni**	**Tehlikeli Durum**	**Korunma Kaybı**	**Kaza**	**Şiddet/Frekans**	**Düzeltici Önlem**
Akü Şarjı	Havalandırma yetersiz	H_2 gazı yayılımı	H_2 gaz dedektörü yok	Patlama	**1A**	Gerekli hava çekiş miktarının hesaplanarak havalandırma tesisatın kurulması ve test edilmesi H_2 gazı yayılmasına karşı gaz dedektörü takılması
Akü Şarjı	Havalandırma tesisatı exproof değil	H_2 gazı yayılımı	H_2 gaz dedektörü yok	Patlama	**1B**	Exproof havalandırma tesisatının seçilerek kurulması
Akü Şarjı	Havalandırma tesisatında arıza	H_2 gazı yayılımı	H_2 gaz dedektörü yok	Patlama	**1D**	Havalandırma tesisatının periyodik kontrol ve bakımı için prosedür hazırlanması

Tablo 8: Örnek Ön Tehlike Analizi Risk Değerlendirme

Tarih :	12.01.2013	**ÖN TEHLİKE ANALİZİ**			Değerlendirme No:	1
Proses/Sistem :	Akü Şarj Odası Tasarım	**RİSK DEĞERLENDİRME TABLOSU**			Düzenleyen:	İş Güvenliği Uzmanı
Alt Sistem :	Havalandırma, Elektrik				Revizyon No:	1
Dizayn Rehberi:					Revizyon Tarihi:	12.01.2013
Takım:	İşveren Vekili, Fabrika Müdürü, İş Güvenliği Uzmanı, Bakım Amiri, İşletme Müh., Elektrik Müh.				Sayfa:	1
Potansiyel Tehlike Eleman	**Tehlikeli Olay Nedeni**	**Tehlikeli Durum**	**Korunma Kaybı**	**Kaza**	**Şiddet/ Frekans**	**Düzeltici Önlem**
Elektrik tesisatı	Aydınlatma lambasının ark yapması	H_2 gazı yayılımı	Uyarı sistemi arıza	Patlama	**2B**	Odada EN60079-10-1'e göre Zone hesaplaması yapılması ve uygun exproof ekipman kullanılması
Akü şarjı	Şarj esnasında problem	H_2 gazı yayılımı, asit dökülmesi vb.		Yangın ya da yanma	**2C**	Akümülatör bataryalarının bütün kutuplarını aynı anda kesecek şalter yapılması
Akü şarjı	Asit değiştirme	Asit	Eldiven ve gözlük uygun değil	Asitten yanma	**3C**	Asit gözlüğü ve eldiveni alımında CE standartı aranması
Akü şarjı	Asit değiştirme	Asit	Eldiven ve gözlük kullanılmıyor	Asitten yanma	**2B**	Kişisel koruyucuların kullanımı ile ilgili işçilere eğitim verilmesi, koruyucu kullanım talimatının oluşturulması, denetim uygulanması

11.5. İş Güvenlik Analizi – JSA (Job Safety Analysis)

İşletmelerde gerçekleştirilen risk değerlendirme çalışmalarında korumaya çalışılan en önemli husus, alınan güvenlik önlemlerinin yetersiz kalması durumunda kazaya uğraması muhtemel tehlike kaynağına yakın çalışandır.

İyi bir güvenlik analizi güvenlik problemlerini ortadan kaldırır, işyerindeki güven hissini ve güvenliği geliştirir. İş Güvenlik Analizi (JSA), kişi veya gruplar tarafından gerçekleştirilen iş görevleri üzerinde yoğunlaşır. Bir işletme veya fabrikada işler ve görevler iyi tanımlanmışsa bu metoloji uygundur. Analiz, bir iş görevinden kaynaklanan tehlikelerin doğasını direkt olarak irdeler. İş Güvenlik Analizi (JSA) olarak adlandırılan analiz dört aşamadan oluşur. İş Güvenlik Analizinin aşamaları **Şekil 26**'da verilmiştir.

İş güvenliği analizinde dikkat, bir kişi veya grup tarafından hazırlanmış iş (görevleri) üzerinde yoğunlaştırılmalıdır. Analiz, işyerinde yapılması planlanmış olan görevlerin yerine getirilmesi aşamasında kaza oluşabilecek ya da tehlike yaratabilecek durumların listelenmesi üzerine dayanmaktadır. Bu yaklaşımda kazaların nasıl oluştuğunu içeren herhangi belirgin bir model uygulanmamaktadır. Metod; çoğunlukla görevler ile ilgili oluşturulan listelerin tümü için her noktanın ve her aşamanın ayrıntılı olarak irdelenmesine ve tehlikelerin tanımlanmasına dayanmaktadır.

Analize, işyerinde çalışan ve o görevi icra eden çalışanların, iş yöneticilerinin ve işin uygulamada nasıl yapıldığını ve işin potansiyel problemlerinin neler olduğunu bilen çalışanların da katkıda bulunması oldukça önemlidir.

Yapı:

Hazırlık aşaması, analizi yapılacak iş görevlerinin sınırlarının tanımlanması ve oluşturulması ve bir görevi yerine getirirken özel önem araz eden bilgilerin ve talimatların toplanmasını içerir. İş güvenlik analizinin ilk aşamasını görev adımlarının veya alt görevlerin numaralandırılarak ayrıntılı olarak analiz edilmesi ve bu adımları bozacak durumların yani temel yapının inşaa edilmesi oluşturur. Bu adım normal olarak işte çalışan ve denenen kişileri de içermelidir. Bunun dışında normal standart iş prosedürlerinin yanında seyrek olarak üstlenilen sıra dışı görevleri de hesaba katmak gereklidir. Analizdeki yapım aşamasının amacı çalışma görevlerinin listesini elde etmektir. Yapı aşamasında; inceleme altındaki iş görevinin değişik aşamalarının detaylı bir listesi hazırlanır. Bu listeler hazırlanırken aşağıda verilen aşamalar mutlaka irdelenmelidir;

- Standart olarak iş prosedüründe veya talimatlarda belirtilen görevler,
- Çalışmaya hazırlık ve planlama aşaması ile çalışmayı bitirme aşaması,
- Önemsiz ve arada sırada yapılan sıra dışı faaliyetler,
- Görevin icra edilmesi öncesinde ve sonrasında yapılması gereken ekstra faaliyetler, Örneğin; malzeme temini, temizlik vb.
- Bu görev ile ilintili bakım ve gözden geçirme faaliyetleri,

Şekil 26: İş Güvenlik Analizi Aşamaları

- **Tehlikelerin Tanımlanması:**

Analizin en önemli parçalarından ilki iş görevlerinin listesinin oluşturulmasıdır, bu listeler bir önceki adımda yani yapı aşamasında hazırlanmış ve bitmiş olmalıdır. Bazen bu iş tehlikelerin bizzat tanımlanmasından daha uzun bir süre alabilir. Sonraki aşamada ise altgörevler birer birer gözden geçirilir. Böylece altgörevleri bozabilecek tehlikelerin özellikleri daha kolay anlaşılabilir. Çeşitli sayıda sorular tehlikelerin tanımlanmasına yardımcı olmak amacıyla sorulabilir.

- Hangi tip zarar gerçekleşebilir?
- Zarar/Tehlike için bir çeklist kullanım için hazırlanabilir mi?
- Çalışma esnasında özel bir problem veya sapma meydana çıkabilir mi?

- Görevi yapmak için diğer bir yol var mı?
- Tehlikeli materyal, techizat, makina vb. içeriyormu?
- İş görevi zor mu?

Çalışma aşamalarının hem listelerinin hazırlanması ve hem de tehlikelerin tanımlanabilmesi için bilgi gereklidir. Daha önceden belirli bir süredir kullanılmakta olan sistemler ile ilgili olarak iş yöneticileri ve çalışanlar tecrübe edinmişlerdir. Bu bilgi birikimi önemlidir, hazırlanan listelerdeki herbir faaliyet için uygun bir şekilde oluşturulmuş çalışma takımı beyin fırtınası ile tehlikeleri bu bilgi birikimini kullanarak belirleyebilir. Ayrıca aşağıda verilen bilgi kaynakları da kullanabilir.

Gerekli olan bilgiler aşağıdakiler kullanılarak da sağlanabilir.

1. Görüşmeler
2. Yazılmış iş talimatları (bazen yanlış, her zaman eksik)
3. Makine kullanım kılavuzları
4. Eğer elde edilebilirse, iş çalışmaları
5. Doğrudan yapılan gözlemler , gözlemci sadece ayakta dururken ve izlerken
6. Fotoğraflar, problemleri gösteren ve çalışma takımı içindeki tartışmalara yardımcı olan video kayıtları, özellikle nadiren ele alınan iş görevleri için değerlidir, fakat oluşturulmaları uzun zaman alması dezavantajdır.
7. Kazalar ve yakın zamanda meydana gelen kaza raporları

- **Risklere Değer Biçilmesi:**

Tehlikelerin veya problemlerin herbirinin tanımlanmasından sonra şiddetin sonucuna göre, maruz kalabilecek kişi sayına ve meydana gelme olasılığına göre değer biçilir.

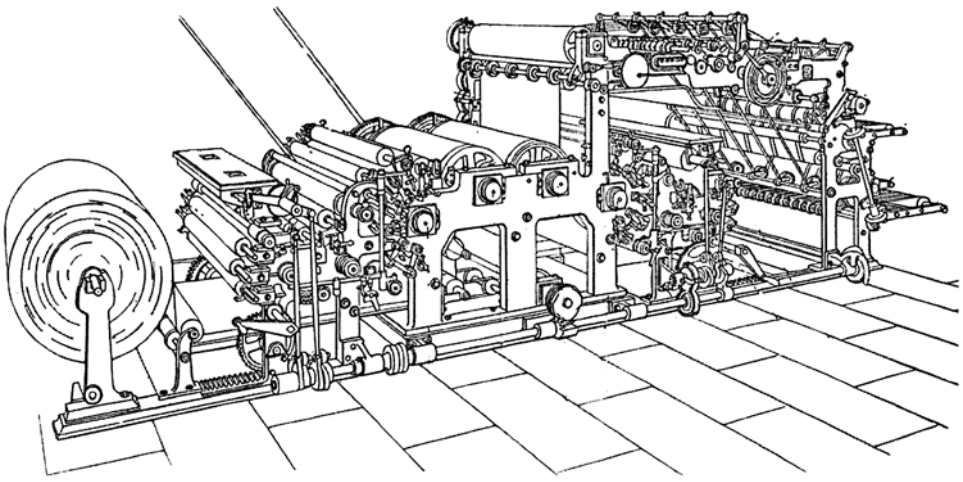
- **Güvenlik Tedbiri Önerisi:**

İş Güvenlik analizi için önerilen güvenlik ölçümünün büyük bir avantajı uygun kontrol ölçümünün oldukça kolay üretilebilmesidir. Bu aşamada yapılabilecek bir çaba da riskin azaltılması için o görevde tehlike/riske giden yol boyunca kağıt üzerinde öneride bulunmaktır. Alışılagelmiş çalışma ve metodlara kullanışlı ise alternatif metodlar sağlanır. Ölçümler şunlara başvurabilir;

- Ekipman ve yardımcı görevler,
- İş görev programı ve metodları (eğer uygulanabilir ise alternatif metod kullan),
- Belirli görevler için ihtiyaçların giderilmesi,
- İş emirleri, eğitimler vb. geliştirilip düzenlenmesi,
- Zor durumları nasıl ele almak gerektiğinin planlanması,
- Güvenlik aygıtları, dedektör vb. güvenlik cihazlarını kurulması,
- Kişisel koruyucu techizatın mutlaka kullanılmasını sağlacak tedbir alınması.

Örnek İş güvenlik analizi formları aşağıda verilmiştir.

Örnek Uygulama



Bir matbaa işyerinde kullanılan kâğıt kesme makinesinde yapılan görevler için iş güvenlik analizi uygulanılacaktır. Öncelikle makinede yapılan işlerin listelenmesi gerekmektedir. Bu işlem için makinenin iş prosedürleri, talimatları veya kullanım kavuzları vb. belgeler incelenebilir.

Yapılan çalışma sonucunda analizi yapan ekip bu makine için aşağıda verilen temel yedi görevi belirlemiştir.

1. Kâğıt makaralarının depodan makinenin yanına taşınması,
2. Makinenin yeni üretim akışı için hazırlanması,
3. Yeni kağıt rulosunun makineye yerleştirilmesi,
4. Makinenin çalıştırılması,
5. İş günü başlangıcındaki ve bitişindeki görevler,
6. Düzeltmeler ve temizlik,
7. Diğer malzemelerin taşınması.

Bu görevlerden üçüncü sırada bulunan "Yeni kağıt rulosunun makineye yerleştirilmesi" aşaması incelendiğinde; işlemler üç adet birbirini takip eden operasyondan oluşmaktadır. Bunlar;

- Makarada sarılı rulo halindeki kâğıdı açmak;
- Dar rulo halindeki makaralardan kâğıdı geçirmek,
- Son olarak da kâğıdın uç kısmını dönen bıçaklardan oluşan sisteme doğru ilerletmektir.

Bu üç operasyon makine operatörü tarafından düzenli olarak yapılmaktadır. Analiz sırasında bu üç operasyon esnasında meydana gelebilecek bütün önemli sapmaların tespit edilmesi gerekmektedir.

Tablo 9: Örnek İş Güvenlik Analizi

İŞ GÜVENLİK ANALİZİ İş Tanımı : Yeni kağıt rulosunun makineye yerleştirilmesi						
Yer: Tarih: Referans:	Potansiyel Tehlikeli Faaliyet (Kaza/rahatsızlığın potansiyel nedeni)	Evet	Hayır	Ne Kadar Sıklıkta Sık sık: 10 saat veya fazla Ara sıra: 6-9 saat Seyrek : 3-5 saat Olası olmayan	Yürüten: Etkinlik (Maruz kalınacak tehlike için yerine getirilecek etkinliği tanımla)	Risk Sınıflaması
	Kaldırma:					
A01	Yapılan işte güç uygulamak gerekiyor mu, ağırlık kaldırılıyor mu?	Evet		Sık Sık	Makinenin yeni üretim akışı için hazırlanması aşamasında, eski rulonun yerinden çıkarılması gerekiyor.	1
A02	Kaldırma veya indirme işlemleri için carraskal, vinç, forklift vb. iş ekipmanı kullanılıyor mu?	Evet		Sık Sık	Yeni ruloyu yerine takarken vinç kullanımında özel dikkat gerekiyor.	1
	Makine ve Ekipman:					
B01	Üzerinde çalıştığı iş veya makine/ekipmanın bir parçasına takılabilir mi, sıkışabilir mi?	Evet		Sık Sık	Dar rulo halindeki makaralardan kâğıdı geçirmesi gerekiyor. Sıkışan kağıtlara müdahale yapılması gerekiyor.	1
B02	Üzerinde çalıştığı iş veya makina/ekipmanın bir parçası çarpabilir mi?		Hayır			
B03	Üzerinde çalıştığı iş veya makina/ekipmanın bir parçasına kapılabilir mi? Uzuv kaybı olabilir mi?	Evet		Sık Sık	Kâğıdın uç kısmını dönen bıçaklardan oluşan sisteme doğru ilerletmesi gerekiyor.	1
B04	Yapılan işte herhangi bir el aleti kullanılıyor mu?	Evet		Ara Sıra	Yeni makaranın üzerindeki ambalaj kağıdını çıkarmak için bıçak kullanılıyor.	2

İŞ GÜVENLİK ANALİZİ İş Tanımı: Yeni kâğıt rulosunun makineye yerleştirilmesi					
Yer: Tarih: Referans:	**Potansiyel Tehlikeli Faaliyet** (Kaza/rahatsızlığın potansiyel nedeni)	**Yürüten:** **Etkinlik** (Maruz kalınacak tehlike için yerine getirilecek etkinliği tanımla)	**Tehlike**	**Sonuç**	**Güvenlik Tedbiri Önerisi**
	Kaldırma:				
A01	Yapılan işte güç uygulamak gerekiyor mu, ağırlık kaldırılıyor mu?	Makinenin yeni üretim akışı için hazırlanması aşamasında, eski rulonun yerinden çıkarılması gerekiyor.	Makara takılabilir (sıkışabilir) yada operatör dikkatini kaybedebilir, yaklaşık 40 kg ağırlıktaki makaranın yere düşmesi.	Operatörün ayağına makara düşmesi sonucu kırık veya ezik.	Makarnın çıkarılması esnasında operatör tarafından caraskal kullanılmasının sağlanması.
A02	Kaldırma veya indirme işlemleri için carraskal, vinç, forklift vb. iş ekipmanı kullanılıyor mu?	Yeni ruloyu yerine takarken vinç kullanımında özel dikkat gerekiyor.	Yaklaşık 1,5 ton ağırlığındaki yeni rulonun vinçten kayarak düşmesi.	Rulonun altında kalınması sonucu yaralanma veya ölüm.	Operatörlere ilave eğitim verilmesi. Operatörlerden başka hiçbir çalışanın vinci kullanmaması için talimat hazırlanması.

İŞ GÜVENLİK ANALİZİ İş Tanımı: Yeni kâğıt rulosunun makineye yerleştirilmesi					
Yer: **Tarih:** **Referans:**	**Potansiyel Tehlikeli Faaliyet** (Kaza/rahatsızlığın potansiyel nedeni)	**Yürüten:** **Etkinlik** (Maruz kalınacak tehlike için yerine getirilecek etkinliği tanımla)	**Tehlike**	**Sonuç**	**Güvenlik Tedbiri Önerisi**
	Makine ve Ekipman:				
B01	Üzerinde çalıştığı iş veya makine/ekipmanın bir parçasına takılabilir mi, sıkışabilir mi?	Dar rulo halindeki makaralardan kâğıdı geçirmesi gerekiyor. Sıkışan kağıtlara müdahale yapılması gerekiyor.	Hareketli makine parçalarına (silindir) sıkışma.	Sıkışma sonucu ezilme veya ağır yaralanma.	Otomatik kağıt besleyici geliştir veya alışılmış çalışma yöntemlerini değiştir. (Yeni rulonun kağıdını makinenin içine çekerken bir önceki rulo kağıdına yapıştırıp çek) Konu ile ilgili prosedür ve talimat hazırla.
B03	Üzerinde çalıştığı iş veya makina/ekipmanın bir parçasına kapılabilir mi? Uzuv kaybı olabilir mi?	Kâğıdın uç kısmını dönen bıçaklardan oluşan sisteme doğru ilerletmesi gerekiyor.	Rulo açma bıçağına kağıdı ilerletme esnasında bıçağa temas.	Bıçakla temas sonucunda kesik veya uzuv kaybı.	B03 ile aynı.
B04	Yapılan işte herhangi bir el aleti kullanılıyor mu?	Yeni makaranın üzerindeki ambalaj kağıdını çıkarmak için bıçak kullanılıyor.	Bıçak ile koli bandını keserken elin kesilmesi.	Elde kesik sonucu yaralanma.	Uygun maket bıçağı alınması.

11.6. Çeklist Kullanılarak Birincil Risk Analizi -(Preliminary Risk Analysis (PRA) Using Checklists)

Birincil risk analizinin amacı, sistemin veya prosesin potansiyel tehlikeli parçalarını tespit ederek değer biçmek ve tespit edilen herbir potansiyel tehlike için az ya da çok kaza ihtimallerini belirlemektir. Birincil risk analizini yapan bir analist, tehlikeli parçaları ve durumları gösteren kontrol listelerine güvenerek bu analizi yapar.

Bu listeler kullanılan teknolojiye ve ihtiyaca göre düzenlenir. Bu listeler mutlak surette "Ciddiyet" ve "Sonuç" başlıklarını içermelidir. “Önleyici Ölçümler” ve “Önlemlerin Yerine Getirilme Ölçümleri” başlıkları ise tehlikelerin giderilmesi yada kontrol altına alınması için gereken aşamaları mutlak suretle içermelidir.

Bu metod kapsamlı detaylar sağlamak maksadıyla dizayn edilmemiştir. Bu metodun amacı daha çok muhtemel gerçekleşebilecek önemli problemlerin acele tespit edilmesidir. Bu nedenle Birincil Risk Analizi metodu bir projeyi yerine getirme aşamasından önceki “çevresel değerlendirmeden” öteye gidemez. Birincil Risk Analizi metodu sistemin kurulması ve kullanıma geçmesi aşamasında risklerin gözlemlenmesi için kullanılabilir.

Kontrol Listeleri:

Kontrol listeleri genellikle tecrübe ile geliştirilmiş olan, önceki risk değerlendirmesi sonucu olarak veya geçmiş başarısızlıkların sonucunda elde edilen risk veya kontrol başarısızlık listeleridir. Bu tip bir analiz (PRA), Tablo 10’da ve Tablo 11'de gösterilen tipte çizelgeler kullanılarak gerçekleştirilir.

Bir kontrol listesi, tehlike ve riskleri belirlemek veya kontrollerin etkinliğini değerlendirmek için kullanılabilir. Bir ürün, süreç veya sistem kullanım döngüsünün her aşamasında kullanılabilir. Ayrıca diğer risk değerlendirme tekniklerinin bir parçası olarak da kullanılabilir ancak uygulanmış olan yeni problemleri belirleyen daha yaratıcı bir risk değerlendirme tekniği sonrasında gizli kalabilecek durumları kontrol etmek için uygulandığında daha kullanışlıdır.

Konu ile ilgili ön bilgi ve uzmanlık gerektirir, ancak bu şeklide hazırlanan kontrol listelerinin geçerliliği kabul edilebilir veya geliştirilebilir. Uygulama yaparken aşağıdaki hususlara dikkat edilmesi gerekir;

- Etkinlik kapsamı tanımlanmalıdır(elektrik, mekanik vb.),
- Bir kontrol listesi etki alanını yeterince kapsayacak şekilde hazırlanmış olmalıdır,
- Kontrol listelerinin dikkatlice seçilmesi gerekmektedir. Örneğin standart kontrollerin bir kontrol listesi yeni tehlikeleri veya riskleri belirlemek için kullanılamaz,
- Kontrol listelerini hazırlayan uzmanlar, uygulayacakları adımları, süreç veya sistemin her bir unsurunu düşünerek listeleri hazırlamaları gerekir, kontrol listeleri üzerinde kritik kontrol öğelerinin mevcut olup olmadığını da değerlendirmeleri gerekir.

Sonuçlar:

Sonuçlar uygulandıkları risk yönetim sürecinin aşamasına bağlıdır. Örneğin; yetersiz uzmanlık veya yetersiz ayrıntıda hazırlanmış olan kontrol listeleri ile yapılan değerlendirme sonuçlarının da yetersiz olacağı unutulmamalıdır.

Güçlü Yönleri:

- Uzman olmayan kişiler tarafından kullanılabilir,
- Geniş, kapsamlı uzmanlık ile iyi tasarlandığında, sistemi kolayca çek etmeyi sağlar,
- Kontrol altına alma davranışını teşvik eder,
- Ortak sorunların unutulmamasını sağlamaya yardımcı olabilir.

Sınırlılıklar:

- Risklerin belirlenmesinde hayal gücünü kısıtlama eğilimdedir,
- Bilinen tehlike kaynaklarına hitap eder, ancak bilinmeyen tehlike kaynaklarına hitap edemez,
- Gözleme dayalı olma eğilimindedir, bu sebeple kolayca görülmeyen sorunlar gözden kaçabilir.

Tablo 10: Örnek PRA Metodolojisi Temelli Risk Değerlendirmesi

PRA Kontrol Listesi			
Proses/Sistem :		Tarih :	
Alt Sistem :			
Formu Dolduran :			
Birimi :		Revizyon No :	
Görevi :			
Doküman No :		Sayfa No : 1	
TEHLİKELER	**EVET**	**HAYIR**	**AÇIKLAMA**
A. PSİKOLOJİK KAYNAKLI			
A.1. Unutkanlık			
A.2. Sıkıntı-üzüntü-keder			
A.3. Stres			
A.4. İstem dışı davranış			
A.5. Yorgunluk, uykusuzluk			
A.6. Alkol alışkanlığı			
A.6 Çevre etkisi			
B. FİZİKSEL KAYNAKLI			
B.1 Yanlış yük kaldırma/Taşıma			
B.2. Vücudu zorlayan duruş			
B.3. Sürekli tekrarlanan fiziksel hareket			
B.4. Görme bozukluğu			
B.5. Uygun olmayan mola zamanı			
B.6. Kötü vardiya zamanlaması			
B.7. Diğer işle ilgili tehlikeler			
B.8. Yapılan işe uygun olmaması			
B.9. Dinlenme süresi az			
B.10. Fazla çalışma			
B.11. Eğitim eksikliği			
C. İŞYERİ ORTAMI KAYNAKLI			
C.1. Havalandırma yetersiz			
C.2. Arızalı ekipman			
C.3. Dağınık işyeri ortamı			
C.4. Yetersiz uyarı sistemleri			
C.5. İkaz, Levha, etiket			
C.6. Bakımsızlık /düzensizlik			
C.7. Yağlı /kaygan zemin			

PRA Kontrol Listesi			
Proses/Sistem : Alt Sistem : Formu Dolduran : Birimi : Görevi : Doküman No :		Tarih : Revizyon No : Sayfa No : 2	
TEHLİKELER	**EVET**	**HAYIR**	**AÇIKLAMA**
C.8. Bozuk techizat			
C.9. Tehlikeli depolama, düzenleme ve istifleme			
C.10. İş ekipmanı arızalı			
C11. Eksik ekipman veya yetersiz ekipman			
C12. Gürültü			
C13. Vibrasyon			
C14. Sıcak yüzeyler			
C15. Soğuk yüzeyler			
C15. Aşırı Isı, nem ve hava hareketi			
C.16. Yetersiz veya aşırı aydınlatma			
D. MEKANİK KAYNAKLI			
D.1. Uygun olmayan techizat			
D.2. Malzeme kusurlarının bulunması			
D.3. Yetersiz / Uygun olmayan koruyucu			
D.4. Arızalı alet,cihaz, malzeme			
D.5. Koruyucusuz tezgah, makine			
D.6. Makine ve tezgahlardaki miller, kayışlar, çark ve dişliler			
D.7. Ezilme			
D.8 Kesme			
D.9. Dolaşma			
D.10. Sıkışma			
D.11. Çarpma / Çarpışma			
D.12. Saplanma			
D.13. Kayma / Sendeleme / Düşme			
D.14. Yüksek Basınç Enjeksiyonu			
D15. Bakım veya periyodik kontrol yok			
D.17. Makina ve tezgahı tehlike anında durduracak stop butonun yada swich yok			
D.18. Ortam Sıcaklığı Çok Fazla			

PRA Kontrol Listesi			
Proses/Sistem : Alt Sistem : Formu Dolduran : Birimi : Görevi : Doküman No :		Tarih : Revizyon No : Sayfa No : 3	
TEHLİKELER	**EVET**	**HAYIR**	**AÇIKLAMA**
D.19. Ortam Sıcaklığı Çok Düşük **D.20.** Diğer Mekanik Tehlikeler			
E. TEHLİKELİ YÖNTEM VE İŞLEMLER			
E.1. Makina veya tezgahlarda çalışırken koruyucu techizatın devre dışı bırakılması			
E.2. Baret, gözlük, siper, maske vb. kişisel koruyucuların kullanılmaması			
E.3. Aşırı yük kaldırma			
E.4. 3m'den yüksek malzeme istifleme			
E.5. Etiketlenmemiş veya yetersiz etiketlenmiş malzeme			
E.6. Uyarı,ikaz işaret ve yazılarının kaldırılması			
E.7. Yeterli ikaz vermeden araçların çalıştırılması veya durdurulması			
E.8. Elektrik kesilmeden techizat üzerinde onarım			
E.9. Onarım esnasında şalter vaya beklenmedik bir harekete karşı güç düğmesinin emniyete alınmamış olması			
E.10. Çalışır haldeki techizatın yağlanması, temizlenmesi, ayarlanması,			
E.11. Depo ve konteynerlerin tam olarak boşaltılıp temizlenmeden üzerinde onarım ve kaynak yapılması			
E.12. Yüksekten atlama			
E.13. Parlama patlama tehlikesi olam yerlerde sigara içilmesi			
E.14. Yükleme ve boşaltma işlemlerinin uygun yöntemle yapılmaması			
E.15. Malzemelerin, makinaların ve techizatın uygun yerleştirilmemesi			
F. ELEKTRİK KAYNAKLI			
F.1. Topraklanmamış tezgah veya el aleti			
F.1. Doğrudan Temas			

PRA Kontrol Listesi			
Proses/Sistem : Alt Sistem : Formu Dolduran : Birimi : Görevi : Doküman No :		Tarih : Revizyon No : Sayfa No : 4	
TEHLİKELER	**EVET**	**HAYIR**	**AÇIKLAMA**
F.2. Dolaylı Temas			
F.4. Tutuşma Kaynağı			
F.5. Diğer Elektriksel Tehlikeler			
F.6.Yıpranmış, hatalı onarılmış tesisat			
F.7. İyi yalıtılmamış el aletleri			
F.9. Devre kesicilerde kilitleme tertibatı olmaması			
F.3. Kısa Devre/Aşırı Yük			
H. KİMYASAL KAYNAKLI			
H.1. Patlayıcı maddeler			
H.2. Asitler, Bazlar nedeniyle yanma			
H.3. Toksik Sıvılar			
H.4. Toksik gazlar, organik sıvıların buharları, ergimiş haldeki metal gazları			
H.5. Toksik Tozlar			
H.6. Yanıcı Sıvılar			
H.7. Yanıcı gazlar,sis,duman			
H.8. Yanıcı Tozlar			
H.9. İnert tozlar, fibrojenik tozlar, toksik tozlar, kansorejonik tozlar, alerjik tozlar			
H.10. Biyolojik tehlikeler			
H.11. Radyasyona maruz kalma (X ışınları, doğal ve yapay radyoaktif maddeler, kızılötesi ve mor ötesi ışınlar			
H.12. Diğer tehlikeli maddeler			

Tablo 11: Örnek PRA Metodolojisi Temelli Risk Değerlendirmesi Formu

1.Firma:

2.Sunulacak Üst Birim: **5.Tarih:**

3.Risk Değerlendirmesini

Yapan İsim/Görev: İş Güvenliği Uzmanı

4.Birimi: Teknik Emniyet **6.Revizyon No:** 9

7.Değerlendirmenin Yapıldığı Proses veya Sistem :	Pres Atelyesi
5.Altsistemler veya Fonksiyonlar:	Otomatik pres makinası
6.Tehlike Kodu (çeklistte tespit edilen):	**E.1**
7.Potansiyel Kaza :	Uzuv kaybı
8.Potansiyel Kazayı Gösteren Olay :	Tehlikeli çalışma
a)Tehlikeli Parça :	Otomatik sürgü
b)Tehlikeli Durumu Gösteren Olay :	Otomatik sürgüyü devre dışı bırakma
c)Tehlikeli Durum :	Otomatik sürgü kapanmadan çalışma sonucu el, kol veya parmakta uzuv kaybı
9.Ciddiyet :	Yüksek – Uzuv kaybı
10.Sonuç :	İşçilerin uyarılması ve tekrar İSG eğitimine alınmaları, swich tertibatı takılması gerekiyor.
11.Önleyici Ölçümler :	Swich tertibatı takıldı.
12.Önlemlerin Yerine Getirilme Ölçümü :	Otomatik sürgü devre dışı olması halinde makina çalışmıyor.

İMZA:

11.7. Güvenlik Denetimi (Safety Audit)

Sistem güvenlik analizi iki metodun kombinasyonudur: Fabrika ziyaretleri yapılması ve çeklist uygulanmasıdır. Fabrika ziyaretleri ve gelişmiş kontrol listeleri ile deneyimi fazla olmayan analistler tarafından uygulanabilen ve herbir prosese uygulanabilen resmi bir yaklaşımdır. Tipik bir çeklist, spesifik alanlara dayanan tanımlamalar ile tehlikeleri belirler. Güvenlik Denetiminin PRA'dan farkı tehlikeli alanların sınıflandırılmasının ve bu alanlardaki tehlikelerin tanımlanmış olmasıdır. Güvenlik denetiminin yapılabilmesi için mutlaka risk haritalarının çıkarılmış olması ve sınıflandırmaların yapılmış olması gereklidir. Çeklistler PRA'da olduğu gibi tecrübeli uzman kişiler tarafından hazırlanması durumunda etkili olacaktır. Ancak güvenlik denetimini yapmak PRA yapmaktan daha kolaydır, çünkü tehlikeli alanlar belirlenmiş ve sınıflandırılmıştır ve o bölgeye özel çeklistler hazırlanmış, iş güvenlik uzmanının analiz yapması kolaylaştırılmıştır. Güvenlik denetiminde talimatlar, iç yönergeler ve çalışma izinlerinin de hazırlanması gerekmektedir. Kaza, olay araştırması ve raporlamasının da mutlak suretle yapılması gereklidir.

Güçlü Yönler ve Sınırlılıklar:

Çeklist kullanımından verimli sonuçlar alınabilmesi için uzun deneyimlere dayalı veya deneyimli uzmanlar tarafından hazırlanmış olması gereklidir. Çeklist kullanmanın yararlarını sıralıyacak olursak;

- Bir işletmedeki veya sistemdeki tesisatın veya ekipmanın tam olup olmadığını veya kusursuz işleyip işlemediğini saptar,
- Güvenlik denetimi kullanımı, kontrol edilecek hususların atlanılmasını engeller,
- Listelerdeki sorular işletmeye özel olarak hazırlandığı için, risk değerlendirmesi yapılan tesisin eksiklikleri saptanır,
- Listelerde belirlenen noksanlıklar için Birincil Risk Analizi uygulanarak gerekli önlenler tespit edilir.

Sınırlılıklar aşağıdakileri içermektedir:

- Tek başına kullanılarak bir işletmedeki tüm risklerin tespit edilmesi mümkün değildir. Mutlaka bu yöntemi destekleyecek başka risk değerlenedirme yöntemleri ile birlikte kullanılması gerekir,
- Sadece güvenlik denetimi kullanımı, kontrol edilecek hususların atlanıl-

masını engellediği gibi aynı zamanda sadece kontrol listesinde bulunan hususlar için kontrol yapılması yeni ortaya çıkan ya da var olan ama gözden kaçmış tehlikelerin atlanılmasına neden olabilir.

- Listelerin yeterince uzman kişiler tarafından işyeri özelinde hazırlanamaması durumunda hiçbir fayda sağlamayacaktır.

Tablo 12'de Birincil Risk Analizi için örnek bir çalışma verilmiştir. Unutulmamalıdır ki çeklistler işyerine/işletmeye özeldir ve tecrübesi, deneyimi fazla olan kişiler tarafından işletmenin yada işyerinin tehlikeleri göz önüne alınarak hazırlanmalıdır. İş Güvenliği Uzmanı öncelikle çeklistler ile işyerinde bir gözden geçirme yapar, daha sonra tespit edilen noksanlıklar için birincil risk analizi formu doldurularak gerekli önlem belirlenir, önleyici ölçümlemeler ve önlemlerin yerine getirilme ölçümü yapılır.

Güvenlik denetim metodolojisi bir tek kişi tarafından gerçekleştirilebilir, ancak bu kişinin yangın kontrolü, depolama, tehlikeli materyaller vb. konularda tecrübeli olması gerekir. Ancak, prosesin şu andaki durumu hakkındaki denetim raporunun hazırlanması için benzer işlemler içeren proseslere dayanan destek dökümanlar kullanılabilir.

Tablo 12: Örnek Birincil Risk Analiz Check List

BİRİNCİL RİSK ANALİZ ÇEKLİST			
Proses/Sistem :		**Değerlendirme No:**	
Alt Sistem :		**Düzenleme Tarihi:**	
Düzenleyen :		**Sayfa No : 1**	
KONTROL MADDESİ (Tesbitinizi uygun sütuna "X" işareti koyarak belirtiniz.)	**EVET**	**HAYIR**	**GEREKSİZ**
A- GENEL ÇALIŞMA KOŞULLARI			
1- Zemin (Yürüme Yüzeyleri)			
a) Zeminde artık malzemeler etrafa saçılmış durumda temizlenmemiş			
b) Zemin uygun değil, kayma ve düşme tehlikesi var			
c) Zemin sürekli ıslak, ıslak zeminde çalışma var			
c) Zeminde tehlike yaratacak demir talaşı, çivi, sivri uçlu malzeme vb. var			
d) Zeminde yanıcı tozlar var (talaş, un,)			
2- Geçitler ve Koridorlar			
a) Koridorlar işaretlenmiş			
b) Koridorlarda malzeme depolanmış, geçişi zorlaştırıyor			
c) Koridorlarda aydınlatma yeterli değil			
3- Acil çıkış yolları ve kapıları			
a) Acil çıkış kapıları belirlenmemiş			
b) Acil çıkışlar işaretleri görülmüyor, önlerinde engel var			
c) Acil çıkış yolları ve kapıları doğrudan dışarıya veya güvenli bir alana açılıyor			
d) Acil çıkış kapıları içeriye doğru açılıyor			
e) Acil çıkış kapıları kilitli veya bağlı			
f) Acil çıkış yollarında geçişi engelleyecek malzeme var			
d) Acil çıkışın olduğu yerde aydınlatma yetersiz			
4- İşyeri tabanı			
a) Zemin kaygan			
b) Zeminde tehlike yaratacak sivri parça, çukur, çıkıntı, pürüz vb. var			
c) Zemin hasar görmüş			
5- Koridorlar			
a) Koridorlarda geçişi engelleyecek malzeme var			
b) Koridorlarda aydınlatma yeterli değil			
c) Koridorlar temiz değil, yüzey kaygan veya aşınmış			
6- Aydınlatmalar			
a) Aydınlatma yeterli değil			
b) Aydınlatma lambası yanmış ve değiştirilmemiş			
c) Aydınlatma lambaları yanarken kırpışmıyor			
d) Ortamda buhar, toz vb. yanıcı toz ve buhar var aydınlatmalar etanj aydınlatma gerekli			
e) Parlayıcı gaz ve buharlar mevcut exproof aydınlatma gerekli			

11.8. Risk Matrisleri (L Tipi Matrisler)

Risk matrisleri, risk düzeyinin belirlenmesi veya risk derecelendirmesi için niteliksel veya yarı niceliksel sonuç/olasılık derecelendirmelerinin bir araya getirilme yöntemidir. Matrisin formatı ve kullanılan tanımlamalar, matrisin kullanıldığı bağlama dayalıdır ve koşullara uygun bir tasarımın kullanılması önem teşkil etmektedir.

Referans Standart:

MIL-STD-882C, Military Standard: System Safety Program Requirements, 1993

MIL-STD-882D Standard Practice for System Safety: Risk Management Methodology for Systems Engineering, 2000

MIL-STD-882E, Department of Defense Standard Practice: System Safety, 2012

Kullanım:

Risk matrisleri, tehlike kaynaklarını veya risk düzeyi doğrultusunda risk müdahalelerini derecelendirmek için kullanılır. Birçok risk saptandığında, söz konusu riskler arasında eleme aracı olarak sonuç/analiz matrisinden faydalanılabilir. Örneğin; hangi riskin daha fazla veya daha ayrıntılı analize ihtiyaç duyduğu, hangi risklere öncelikli olarak müdahale edilmesi gerektiği veya hangisinin daha üst düzey bir yönetime aktarılması gerektiğinin saptanması için kullanılabilir. Matris kullanımı ile aynı zamanda hangi riskin artık üzerinde durulmaması gerektiği de saptanabilir. Son olarak bu tür bir risk matrisi, matris üzerinde yer aldığı noktaya göre belirli bir riskin genel olarak kabul edilebilir veya kabul edilemez olduğunu belirlemek için de kullanılabilir.

Risk matrisleri, organizasyon bünyesindeki niteliksel düzeylerin aynı şekilde anlaşılarak aktarılmasına yardımcı olması için de kullanılabilir. Risk düzeylerinin belirlenme yöntemi ve bunlara ilişkin karar kuralları, organizasyonun risk düzeyi ile aynı doğrultuda olmalıdır.

Risk matrisinin diğer bir türü olan "Sonuç Risk Matrisi" ise, FMECA sürecinde kritiklik analizi ya da Ön Tehlike Analizi, HAZOP, SWIFT, vb. tekniklerin kullanımı sonrası önceliklerin saptanması için kullanılabilir. Ayrıntılı bir analiz için elde yetersiz veri olduğunda veya durum, daha fazla kalitatif analiz için süre ve efor garantisinde bulunmadığında da kullanılabilecek yararlı bir yöntemdir.

Ön Tehlike Analizi risk değerlendirmesi; kötü tesadüf şiddeti ve olasılığı (ya da frekansı) cinsinden risk derecelendirmesi (klasifikasyonu) bir derecelendirme matrisi kullanmak suretiyle yerine getirilir. Bir tehlike için riskin değerlendirilmesi amacıyla değişik matrisler kullanılır ve analist tarafından birleşik şiddet ve olasılığın gösterildiği hücrelerden riskin en yüksek olduğu hücre seçilir.

Bu süreç, tehlikeye maruz kalabilecek her bir unsur (personel, ekipman vs.) için ayrı ayrı işletilir. Eğer bir tehlike personel, ekipman veya işletme için birden fazla kötü tesadüf kategorisi ihtiva ediyorsa, sonuç olarak o tehlike için risk değerlendilmesinde riskin maksimum olduğu şiddet-olasılık çifti seçilir. Eğer belirlenen bir varlık için en yüksek riski temsil eden iki ya da daha fazla şiddet-olasılık çifti eşit çıkarsa, deklare edilen aksi tesadüf riski için şiddeti en yüksek olan çift seçilir.

Girdi:

Süreç girdileri, sonuç ve olasılığa ilişkin uyarlanmış ölçekler ve bu ikisini bir araya getiren bir matristir. Sonuç ölçeği (veya ölçekleri), göz önünde bulundurulacak tüm farklı sonuçları kapsamalı (örn; mali kayıplar, güvenlik veya bağlam doğrultusunda diğer parametreler) ve en olası sonuçtan en düşük olasılıklı sonuca doğru bir sıra izlemelidir. Ölçek, herhangi bir sayıda puana sahip olabilir. 3, 4 veya 5 puanlı ölçekler en yaygın şekilde kullanılanlardır.

Ancak **Tablo 13**'de verilen şekli ile hem olasılık hem de şiddet için sayısal puan kullanımı standartın ***son versiyonlarında kesinlikle tavsiye edilmemektedir.*** Standartın özellikle tavsiye etmediği matris 5x5 matrisi olarak da bilinmektedir.

Bu matris şeklinin tavsiye edilmemesi ile ilgili olarak, özellikle bu matriste olasılık ve şiddet ölçeğinin her ikisi de bir sayıda puana sahip olabilmekte olduğu için kabul edilebilirlik alanlarının birbiri ile karışması mümkün olabilmekte ve noktalar arasında ayrım yapılamıyor olmasıdır. Olasılığa ilişkin tanımlamaları mümkün olduğunca belirsiz olacak şekilde seçilmiştir.

Örnek verecek olursak; olasılığı "Çok Küçük" yani 1 olan bir tehlikenin şiddeti ise "Çok Ciddi" yani 5 değerini alacaktır. Çarpım sonucu ise 5' dir. Tersi yani; olasılığı "Çok Yüksek" yani 5 olan bir tehlikenin şiddeti ise "Çok Hafif" yani 1 değerini alacaktı. Çarpım sonucu ise yine 5'dir. Oysa bu iki nokta aynı değildir ve aynı şekilde de değerlendirilmemesi gerekir.

Tablo 13: Sayısal Puan Kullanımlı Risk Skor (Derecelendirme) Matrisi (L Tipi Matris)

	ŞİDDET				
OLASILIK	**1 (Çok Hafif)**	**2 (Hafif)**	**3 (Orta Derece)**	**4 (Ciddi)**	**5 (Çok Ciddi)**
1(Çok Küçük)	**Anlamsız 1**	**Düşük 2**	**Düşük 3**	**Düşük 4**	**Düşük 5**
2 (Küçük)	**Düşük 2**	**Düşük 4**	**Düşük 6**	**Orta 8**	**Orta 10**
3 (Orta Derece)	**Düşük 3**	**Düşük 6**	**Orta 9**	**Orta 12**	**Yüksek 15**
4 (Yüksek)	**Düşük 4**	**Orta 8**	**Orta 12**	**Yüksek 16**	**Yüksek 20**
5 (Çok Yüksek)	**Düşük**	**Orta**	**Yüksek**	**Yüksek**	**Tolere Edilemez 25**

Farklı olasılıkları tanımlamak için sayısal kılavuzlar kullanılırsa, ölçek birimlere ayrılmalıdır. Olasılık ölçeği, yürütülen çalışma ile ilişkili aralığı kapsamalı, en düşük olasılığın tanımlanan en yüksek sonuç için kabul edilebilir olup olmadığının değerlendirilmesi gerektiği kesinlikle unutulmamalıdır. Aksi takdirde, en yüksek sonuca sahip ancak düşük olasılığa sahip tüm faaliyetler kabul edilebilir şeklinde tanımlanabilir ki bu durum aslında asıl kabul edilememesi gereken bir durumdur.

Standartın önerdiği risk matrisi şekline örnek verecek olursak, bir eksende sonuç, diğer eksende ise olasılık yer alacak şekilde çizilir. Ancak olasılık veya şiddet kolonlarından birine sayısal değer verilmez ve matristeki her bir çarpım kodlama şeklinde matriste belirtilir. bir **Tablo 14**'de 6 puanlı sonuç ve 5 puanlı olasılık ölçeklerini içeren bir risk matris örneği gösterilmektedir.

MIL-STD- 882E'de bir önemli konuda risk kategorisidir. Teker teker tehlikelerin gruplandırılarak risk değerlendirme kategorilerine dönüştürülmesinde kötü tesadüf endekslerinin kullanımı gösterilmektedir. Bu standarta göre risk kategorisi büyüdükçe, risk kabul seviyelerine de yönetimde görev alan yöneticiler karar vermelidir. (Tek başına İş Sağlığı ve Güvenliği Mühendis veya teknik elemanının kabul kriterine karar vermesi kabul edilmiyor) Bu standartı kullanan analist veya analistlerin, kötü tesadüf risk kabulünden önce, organizasyondaki üst yönetime danışmaları zorunlu bırakılmaktadır. **Tablo 15**'de, sistem yönetiminin belirleyeceği risk endeksi, risk kategorisi ve risk kabul seviyesi listesi verilmektedir.

Tablo 14: Altı Puanlı Sonuç, Beş Puanlı Olasılık Ölçekli Risk Matris Örneği

	OLASILIK					
ŞİDDET	Kuvvetle Muhtemel A	Muhtemel B	Olası C	Olası Değil D	Mümkün değil E	İmkansız F
I Katastrofik	A1	B1	C1	D1	E1	NA
II Kritik	A2	B2	C2	D2	E2	
III Marjinal	A3	B3	C3	D3	E3	
IV İhmal edilebilir	A4	B4	C4	D4	E4	

Hücrelere verilen risk düzeyi değerleri, olasılık/sonuç ölçekleri için yapılan tanımlamalara bağlı olacaktır. Matris, sonuç veya olasılıklara ilişkin ilave ağırlıklar verecek şekilde de düzenlenebilir (gösterildiği gibi) ya da uygulama doğrultusunda simetrik bir yapıya sahip olabilir. Risk düzeyleri, yönetim ilgi düzeyi veya tepki gerektiren zaman ölçeği gibi karar kuralları ile bağlantılı olabilir.

Niceliksel ölçekler ile birlikte derecelendirme ölçekleri ve bir matris de planlanabilir. Örneğin herhangi bir güvenilirlik bağlamında olasılık ölçeği, arıza oranı göstergelerini betimleyebilir. Diğer yandan sonuç ölçeği ise, söz konusu arızanın dolar bazındaki maliyetine işaret eder.

Tablo 15: Risk Kabul Seviyeleri

RİSK ENDEKSİ	RİSK KATEGORİSİ	RİSK KABUL SEVİYESİ
A1, A2, B1, B2, C1	Yüksek	Fabrika Direktörü
A3, B3, C2, D1, D2	Ciddi	Fabrika Müdürü
A4, B4, C3, D3, E1, E2, E3	Orta	Program Müdürü
C4, D4, E4	Düşük	İşletme Müdürü

Söz konusu aracın kullanımı, ilgili uzmanlıklara sahip kişilerin (tercihen bir ekip) de çalışmaya dahil olmasını ve sonuçlar ile olasılıkların değerlendirilmesine yardımcı olacak bir takım verileri gerektirir.

Süreç:

Kullanıcı, riskleri derecelendirmek için ilk önce duruma en uygun olan sonuç tanımlayıcısını belirler ve ardından söz konusu sonuçların meydana gelme olasılığını belirler. Bu sayede risk düzeyi, matris üzerinden görülebilir.

Birçok risk vakaları, farklı bağıl olasılıklara sahip birçok sonucu beraberinde getirebilir. Genellikle küçük problemler, felaketlerden çok daha yaygındır. Dolayısıyla üzerinde durulması gereken husus en yaygın sonucu mu, en ciddi sonucu mu yoksa başka kombinasyonları mı derecelendirmek gerektiğidir. Çoğu durumda, en kapsamlı tehditleri içerdikleri ve en çok dikkati çektikleri için en ciddi sonuçlara odaklanmak uygun olacaktır. Bazı durumlarda da yaygın yaşanan problemleri ve muhtemel olmayan felaketleri birbirinden bağımsız riskler şeklinde derecelendirmek uygun olmayabilir. Burada önemli olan, olayın tüm olasılığından ziyade, seçilen sonuca ilişkin olasılığın kullanılması önemlidir. Matris yardımıyla tanımlanan risk düzeyi, riske müdahale edip etmeme konusunda bir karar kuralı ile bağlantılı olabilir.

Çıktılar:

Elde edilecek çıktı, her bir risk için derecelendirme veya önem düzeyleri belirlenmiş risklerin derecelendirme listesi olacaktır.

Güçlü ve Zayıf Yönler:

Güçlü yönler şunlardır:

- Kullanımı oldukça kolaydır,
- Risklerin farklı önem düzeylerine göre hızlı bir biçimde derecelendirilmesini sağlar,

Sınırlılıklar aşağıdaki gibidir:

- Matrisler, belirli koşullar doğrultusunda tasarlanmış olabilir ve dolayısıyla organizasyon kapsamındaki tüm tehlike kaynaklarını tanımlamak için yeterli olmayabilir, bu durumda diğer risk değerlendirme tekniklerine başvurulması gerekir. Örneğin; bir makinanın güvenlik fonksiyonlarını değerlendirmek ya da bir kimyasal prosesteki güvenlik seviyesini değerlendirmek için risk matrisi yaklaşımı tek başına yeterli olamaz,
- Ölçeği açık bir biçimde tanımlamak zordur,
- Riskler bir araya getirilemez, yani sayısal kullanımda 5x1 ile 1x5 aynı olarak değerlendirilemez. Meydana gelme ihtimali düşük olduğu düşünülen ve şiddet değeri ciddi olan bir risk ile tesis içerisinde birçok defa saptanan ve yine meydana gelme ihtimali taşıyan şiddet değeri hafif olan bir riskin aynı derecede önem seviyesine sahip olduğunu varsayar, oysa bu iki risk seviyesinin her ikisinin de aynı düzey bir riske tekabül ettiği söylenemez,
- Farklı sonuç kategorileri doğrultusunda risk düzeylerini karşılaştırmak zordur.

Sonuçlar, yapılan analizin ayrıntılarına bağlıdır. Örneğin; analiz ne kadar ayrıntılı ise, her biri daha düşük olasılıklara sahip senaryoların sayısı daha yüksek olacaktır. Bu durum, riske ilişkin gerçek düzeyin azımsanmasına yol açar. Risk tanımlama sürecinde senaryoların grup haline getirilme yöntemi tutarlılık göstermeli ve çalışmanın başlangıcında belirlenmelidir.

MIL-STD-882 E'ye göre eşik-riskler için, sistem risk değerlendirme kriterleri, uygun kabul etme otorite seviyesine bağlı olarak, 6 karar verme alanına bölünerek incelenmiştir, buna göre;

- **Minimal (İhmal Edilebilir) Risk:** Bu yaklaşım, sistem güvenlik programı için minimal eşik değerinin tanımlanması amacıyla bir doğru çizer. Bu seviyenin altında, tehlike etkisinin azaltımasına yönelik her hangi bir harcama önerilmez.
- **Düşük Risk:** Bu riskler tehlike şiddetinin azaltılması için kaynak harcamasının gerekli olduğu risklerdir. Kalan kötü tesadüf riski İşletme Yöneticisi tarafından onaya tabidir.
- **Orta Risk:** Bu riskler bazı endişeleri beraberinde taşıyacak kadar yüksek riskleri ifade eder. Kalan kötü tesadüf risk kabulünün İşletme Müdürü tarafından yapılması zorunludur.
- **Ciddi (Önemli) Risk:** Risk kabulü mutlak suretle harcama yapılmasını gerektiren ve risk kabülünün Fabrika Müdürü seviyesinde olduğu risklerdir.
- **Yüksek Risk:** Risk kabulu, sistemin bütününde değişiklik ve yatırım gerektiren risklerdir. Gerekli ise bölümde veya sistemde durdurma kararı verilebilir. Risk kabulu Fabrika Müdürü seviyesinde olan risklerdir, ancak risk seviyesinin bu seviyede tutulması hem işletme hem de Fabrika Müdürü için de risk içermektedir.
- **Kabul Edilemez (Çok Yüksek) Risk:** Bu riskler zorlayıcı bir neden olmadan kabul edilemez. Kabul seviyesi Fabrika Direktörüdür, ancak bu seviyedeki bir kabul hiçbir yönetici tarafından asla yapılmamalıdır.

Tarihçe:

Ön Tehlike Analizi'nin ve risk matrislerinin temeli ABD askeri standartları olan MIL-STD standartalarına dayanmaktadır. Haziran 1966 ila Mart 1967 yılları arasındaki çalışmalar sonucunda hava taşıtları, uzay ve elektronikle ilgili öncü sistem güvenlik standartı olan "MIL-S-38130A" yayınlanmıştır. Bu standartta risklerin değerlendirilmesi için tehlike veya olasılığa seviye verilmemiş ve matris önerilmemiştir.

1969 yılında ABD Savunma Sekreterliği, sistem tedariğinde başlıca problem alanı olarak gördüğü "Risk Değerlendirme" konusundaki yetersizliklere dikkat çeken bir rapor yayınlamıştır. Ağustos 1969'da ise endüstriyel ilişkilerde sistem güvenliği ile ilgili uygulamaları içeren ilk MIL-STD-882 standartı yayınlanmıştır. Ağustos 1969'da endüstriyel ilişkilerde sistem güvenliği ile ilgili uygulamaları içeren ilk MIL-STD-882 standartında risk değerlendirmesi ile ilgili ilkeler bulunmaktadır.

Yine aynı tarihte Savunma Müsteşarı David Packard, askeri servislere sistem tedariklerinde yanlış risk değerlendirmelerinin çok büyük bir sorun haline geldiğini yazdığı bir rapor ile duyurmuştur. Risk değerlendirme konusunda görülen bu yetersizlikler DoD (Department of Defense)'un Temmuz 1977'de "MIL-STD-882A" standartını yayınlamasına yol açmıştır. MIL-STD-882A" standartı tehlike olasılığı ve riskin kabul edilebilirliği ile ilgili kriterleri içermesi açısından önem taşımaktadır.

Mart 1984'den Ağustos 1987'ye kadar yapılan çalışmalar sonucunda yine DoD tarafından sistemlerin bozulmalarında insani hatalarının önemini vurgulayan "MIL-STD-882B" standartı yayınlanmıştır. DoD tarafından sistemlerin bozulmalarında insani hatalarının önemini vurgulayan "MIL-STD-882B" standartının ekinde ise ilk defa kalitatif risk matrisleri verilmiştir.

Daha sonraki yıllarda DoD tarafından günümüzde de referans olarak halen kullanılabilecek standartlar yayınlanmıştır. Ocak 1996'da entegre donanım ve yazılım işlerini ilgilendiren "MIL-STD-882C" ve Şubat 2000'de ise sistem talep formlarında reform getiren "MIL-STD-882D" standartı yürürlüğe girmiştir. MIL-STD-882E (Draft – 1 Şubat 2006) standartı ile de olasılık teoremlerinin risk değerlendirme çalışmalarında kullanılması öngörülmüştür.

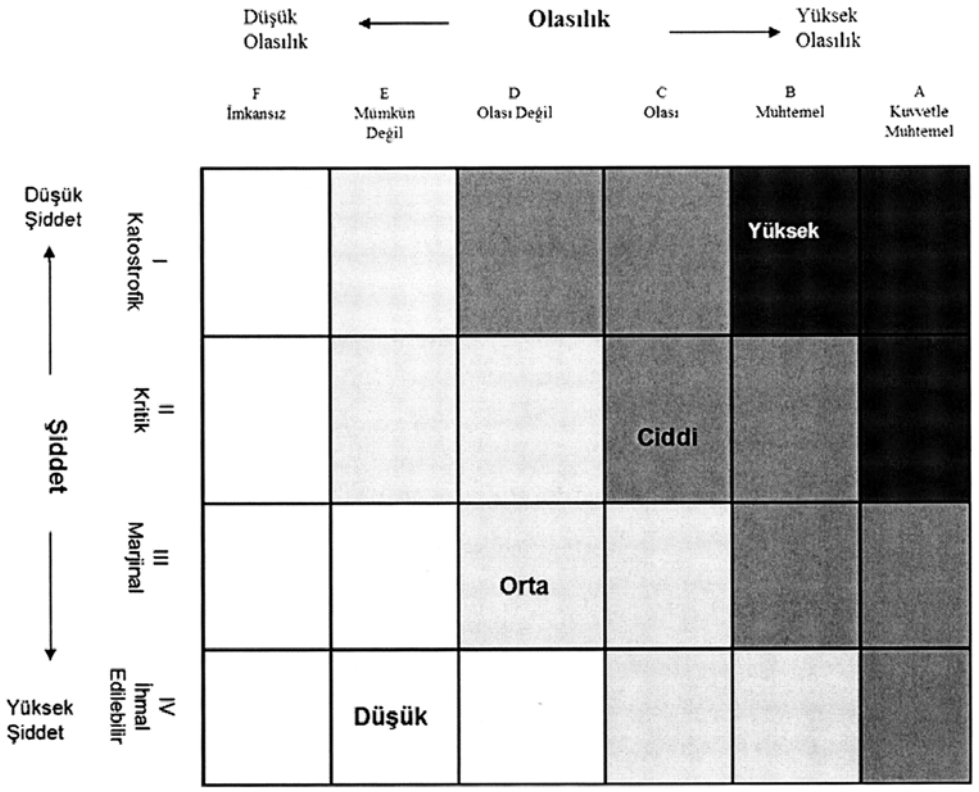
Ocak 1996'da yayınlanan ve entegre donanım ve yazılım işlerini ilgilendiren MIL-STD-882C standartınının ekinde kalitatif ve kantitatif risk matrisleri verilmiş ve risklerin kabul seviyeleri belirlenmiştir. Şubat 2000'de yayınlanan ve sistem talep formlarında reform getiren MIL-STD-882D'de ise kalitatif risk matrisi kullanılmasına rağmen olasılık seviyelerinin kantitatif olarak belirlenmesi yapılmıştır. MIL-STD-882E (Draft – 1 Şubat 2006) standartında ise çoklu matrisler ve risk seviyeleri verilmiştir.

MIL-STD-882E'de, bu standardın önceki veriyonlarının da kullanılmaya devam edilebileceği ancak özellikle kompleks ve birbiri ile ardışık ekipman ve süreçler içeren sistemler için diğer versiyonların uygun olmadığı ve bu matrislerin istenilen özelliklerin hepsini kapsamamakta olduğu belirtilmiştir. Aşağıda MIL-STD-882E standartında uygulanması önerilen değişik olasılık, şiddet tabloları ve risk matrisleri örnek olarak verilmiştir.

Kalitatif Risk Değerlendirme Matrisi:

Aşağıda verilen risk değerlendirme matrisi MIL-STD-882E standartında verilen jenerik (her duruma takbik edilebilir) risk değerlendirme matrisidir. Bu

Tablo 16: MIL-STD-882E Kabul Edilebilirlik Kriteri



4 x 6 matris sınırları belirler, rehberlik eder ve görüntüler. Kalitatif kötü tesadüf risk değerlendirme matrisi şiddet ve olasılık aralıkları, fabrika veya organizasyon onayı ile, riskin kalitatif değerlendirilmesinde kullanılmak üzere derecelendirilir. Standartta olasılık ve şiddet için sübjektif terimlerin tespit edilmesine yol göstermek için gerekli, çeşitli ibareler verilmektedir. Şiddet seviyeleri ihmal edilebilirden (IV) katastofik'e (I) kadar aşamalandırılmış ve olasılık skalası da benzer şekilde düşünülerek, imkansız'dan (F), kuvvetle muhtemel'e (A) kadar derecelendirilmiştir. Olasılık skalasındaki terimler diğer risk değerlendirme matris örneklerinde verilen ve aynı derecede öneme haiz olan frekans aralıklarından ziyade, analistlerin tecrübeleri oranında kötü tesadüflerin vuku bulma ihtimaline işaret etmektedir.

Karar verme aşamasında analizi yapan analistler tarafından, şiddet aralığının tarif edilmesi için en yüksek ve en düşük şiddet değerleri belirlenmelidir. Bu

standartı kullanan analist veya analistlerin, kötü tesadüf risk kabulünden önce, organizasyondaki üst yönetime danışmaları istenmiştir. Aşağıdaki tablo, düşük, orta, ciddi ve yüksek risk alanlarını tanımlar ve kötü tesadüfün her seviyesi için uygun karar otoritesini gösterir.

Matris skalasında bu örnek matriste olduğu gibi, sübjektif anahtar ibareleri kullanılarak şiddet ve olasılığın seviyesi belirlenebilir. Ancak aşağıda verilen diğer matris örneklerinde verildiği üzere sayısal değerler kullanılarak kantitatif bazda olasılık değerleri kullanılarak söz konusu tehlikenin değerlendirilmesi daha doğrudur. Çünkü analizi yapan uzmanın veya analistin tecrübesi söz konusu tehlikenin veya kötü tesadüfün daha düşük olasılıkta gerçekleşebileceği şeklinde algılanabilmektedir.

Kantitatif Risk Değerlendirme Matrisi:

MIL-STD-882 E standartında verilen bir diğer risk değerlendirme matrisi ise kantitatif risk değerlendirme matrisidir. Bu matrisi yukarıda verilen 1. Örnek matristen ayıran en önemli farklardan biri olasılık bölümünde frekans aralıklarının verilmiş olmasıdır, ayrıca şiddet bölümünde tesiste söz konusu olabilecek hasar durumları da derecelendirilmiştir.

Tablo 17: Risk Seviyesi ve Karar Verme Yetkilisi

RİSK DEĞERLENDİRME KODU	RİSK SEVİYESİ	KARAR VERME YETKİLİSİ
IA, IB, IIA	Yüksek	İşletme Direktörü
IC, ID, IIB, IIC,IIIA, IIIB, IVA	Ciddi	İşletme Müdürü
IE, IID, IIE, IIIC, IIID, IVB, IVC	Orta	İşletme Yöneticisi
IIIE, IVD	Düşük	Bölüm Yöneticisi
IF, IIF, IIIF, IVF	NA Uygulanamaz	Hiç (Gerek Yok)

Toplam Sistem Risk Ölçümü:

Bir sistemi, belirtilen kriterler bazında incelemek için, sistem riskinin (R) bir ölçüsü olmalıdır. Sistem riskinin çizilebilmesi için, bu ölçümün hem şiddet boyutunda hem de meydana gelme olasılığı boyutunda incelenmesi gerekir. Bu ölçüler, toplanmış tehlikelerin tümüyle bağımsız olduklarını varsaymaktadır. Sistem riskinin geçerli olduğu ölçütler aşağıda verilmiştir. Bu matriste kullanılan herbir sistem riski için olasılık ve şiddet değerleri arasında bir doğru çizilir. Analistler tarafından bir sistemin içerdiği tüm riskler incelenerek en yüksek risk seviyesi tespit edilir ve "Toplam Risk" olarak kabul edilir. Toplam risk için aşağıda verilen kriterler değerlendirilir. Özellikle kimya sanayi, nükleer sanayi veya petrol tesisleri vb. tesisler için büyük endüstriyel kaza sonuçlarının değerlendirilmesi için sıklıkla toplam riske başvurulur.

- **Beklenen Kayıp Oranı:** Bu ölçüm, bir dizi ömür döngüsü boyunca işletilmiş bir sistemde, bir dizi sistem çökmesi bazında, bu maruziyet aralığında oluşacak sistem başına ortalama kayıp olarak ifade eder. Çizilecek olasılık değeri 1.0'dir çünkü bu metod, sistemin belirlenen maruzuiyet aralığı boyunca işletilmesi durumunda oluşacak ortalama kaybı tahmin etmeye yöneliktir.
- **Azami Kayıp:** Bu ölçüm, şiddet komponentinin, en şiddetli tek bir tehlikenin oluşması durumunda meydana gelecek kayıp seviyesine karşılık gelen kayıp olarak işaretlenmesi (belirlenip çizilmesi) ile oluşur. Azami kayıp olasılığı, beklenen kayıp oranının azami kayıp seviyesine bölünmesiyle hesaplanır.
- **En Muhtemel Kayıp:** Bu ölçümü çizmek (işaretlemek) için, her bir şiddet seviyesindeki tehlikelerin olasılıkları toplanır. Olasılığı en yüksek olan şiddet seviyesi en muhtemel kayıptır. Bu şiddet seviyesi, beklenen kayıp oranının en muhtemel kayıp seviyesine bölünmesiyle elde edilen olasılık değeridir.
- **Şarta Bağlı Kayıp Seviyesi:** Olasılık değeri, tüm tehlikeler için olasılıkların toplamıdır. Şiddet değeri de şarta bağlı beklenen kayıptır. Bu değer, beklenen kayıp değerinin olasılıklar toplamına bölünmesiyle bulunur. Bir kötü tesadüfün oluşma olasılığını ve oluşması durumunda şiddetini içeren bir değerdir.

Şiddet kategorileri, kaza sonucu ölüm, yaralanma, mal kaybı/hasarı, çevresel etki veya diğer kayıplar vb. parametrelerle oluşan kötü tesadüf sonuçlarının etki aralıklarının belirlenmesi için tanımlanmışlardır. Şiddet kategorileri Tablo 18'de gösterilmektedir, bu tabloda gösterilen USD değerleri sistemler bazında, söz konusu olabilecek en yüksek ve en düşük şiddetli kötü tesadüf dikkate alınarak saptanmalıdır.

Olasılık, kötü tesadüfün spesifik bir maruziyet zaman aralığı süresince meydana gelme ihtimalidir. Olasılık matematiksel olarak sıfır ila bir arasındadır. Frekans ise kötü tesadüfün oluşma hızıdır (veya sıklığı). Frekans, riskin bir parçasını oluşturduğundan, olasılık yerine de kullanılabilir. Olasılık kategorileri, bir ya da bir kaç kötü tesadüfün belirli bir maruziyet süresi içerisinde meydana gelme olasılığını veya kötü tesadüf frekansının zaman birimi, olay, popülasyon,veya aktivite içinde meydana gelme sayısını tarif etmek üzere kullanılırlar.

Tablo 18: Şiddet Kategorileri

TANIMLAMA	KATEGORİ	ÇEVRESEL, SAĞLIK VE GÜVENLİK SONUÇ KRİTERLERİ
Katastropik (Felakete Yol Açan)	I	Ölüm, kalıcı maluliyet, 1 milyon USD üzerindeki kayıp veya kanun ya da yönetmenliğe aykırı geri dönülmesi imkansız şiddetli çevresel hasar
Kritik	II	Kalıcı kısmi maluliyet, en az üç kişinin yaralanma veya meslek hastalığı nedeniyle hastanede tedavi görmek zorunda kalması, 1 milyon ile 200 bin USD arasındaki maddi kayıp veya kanun ya da yönetmenliğe aykırı geri dönülmesi mümkün olan çevresel hasar.
Marjinal	III	Yaralanma veya meslek hastalığı sonucunda bir veya daha fazla iş günü kaybı; 20.000 USD'den fazla ancak 200.000 USD'dan az maddi kayıp, kanun ya da yönetmeliğe aykırı olmayan, restorasyon faaliyetlerinin başarılabileceği hafifletilebilir çevresel hasar.
İhmal Edilebilir	IV	İş günü kaybına neden olmayan yaralanma veya haslalıklar, 2.000 USD'dan çok 20.000 USD'dan az maddi kayıp, kanun ya da yönetmenliğe aykırı olmayan minimal çevresel hasar.

Olasılık ya da frekansın sayısal olarak belirlenmesinin mümkün olmaması durumlarında, kötü tesadüf kategorileri kalitatif tarif ediciler (muhtemel, olası, olası değil vb.) yardımıyla tanımlanır. Veri azlığı veya yokluğu nedeniyle, zaman zaman potansiyel bir tasarım ya da prosedürel tehlike için olasılık veya frekansın kantitatif olarak belirlenmesi zor olabilir. Bu gibi durumlarda olasılık ya da frekans, benzer sistemlerden elde edilen geçmiş datalar üzerinde yapılan araştırma, analiz ve değerlendirmelerden elde edilir. Bir kötü tesadüfün olasılığı ya da frekansını tayin etmek için gerekli mantık, olasılık teoremlerinde tarif edilmiştir. Kantitafif olasılık kategori örnekleri **Tablo 19** ile **Tablo 20**'de gösterilmektedir.

Logaritmik Olasılık (Frekans) Skalalı Kantitatif Risk Değerlendirme Matrisi

Nicelik Skalası olarak şiddet ve olasılık için kalitatif terimlerin ("sık sık", "ara sıra", kritik vs.) kısıtlı bir hassasiyet sağladığı malumdur. Bu ifadelerin değişik yorumlanması, risk değerlendirmesi doğruluğundan şüphe duyulmasına ve/veya bazı tartışmalara neden olabilmektedir. Bu nedenle, riski değerlendirirken, olasılık ve şiddeti numerik (sayısal) ifadeler kullanılarak derecelendirilmesi, benzer şekilde, risk matrisi eksenlerinin mümkün mertebe kantitatif ifade edilmesi gerekmektedir.

Risk değerlendirme matrisinin eksenleri logaritmik olarak belirlenebilir. Bu demektir ki, majör skala indisleri örneğin 1,2,3 gibi tam saylarla değil ancak 10'un katları şeklinde, örneğin, (... 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4}… veya…1, 10, 100…veya…2, 20, 200…vs.) gösterilir bunlara büyüklük sırası denilir. Skala aralıkları ikişer ikişer (…10^{-8}, 10^{-6}, 10^{-4}, 10^{-2}, 1, 100, 10,000…) veya yarımşar yarımşar (10^{-7}, $10^{-6..5}$, 10^{-6}, $10^{-5.5}$…1, 3.16, 10, 31.6, 100, 316…) artacak şekilde düzenlenebilir.

Aşağıda verilen matris; şiddetin çift büyüklük olarak değerlendirildiği, logaritmik olasılık (frekans) skalalı, 6 x 8 kantitatif risk değerlendirme matrisidir ve düşük olasılık ile yüksek sonuçlar doğuran tehlikeler için kullanılması önerilmektedir. Logaritmik skalası ve 4 seviyeli karar verme otoritesi bulunmaktadır. Bu matris, *"tehlikenin kalitatif, olasılığın ise kantitatif olarak değerlendirildiği yerlerde kullanılmak üzere tasarlanmıştır"*. Bununla beraber, her aksın skalası toplamların alınması ve toplam riskin belirlenmesi için elverişlidir.

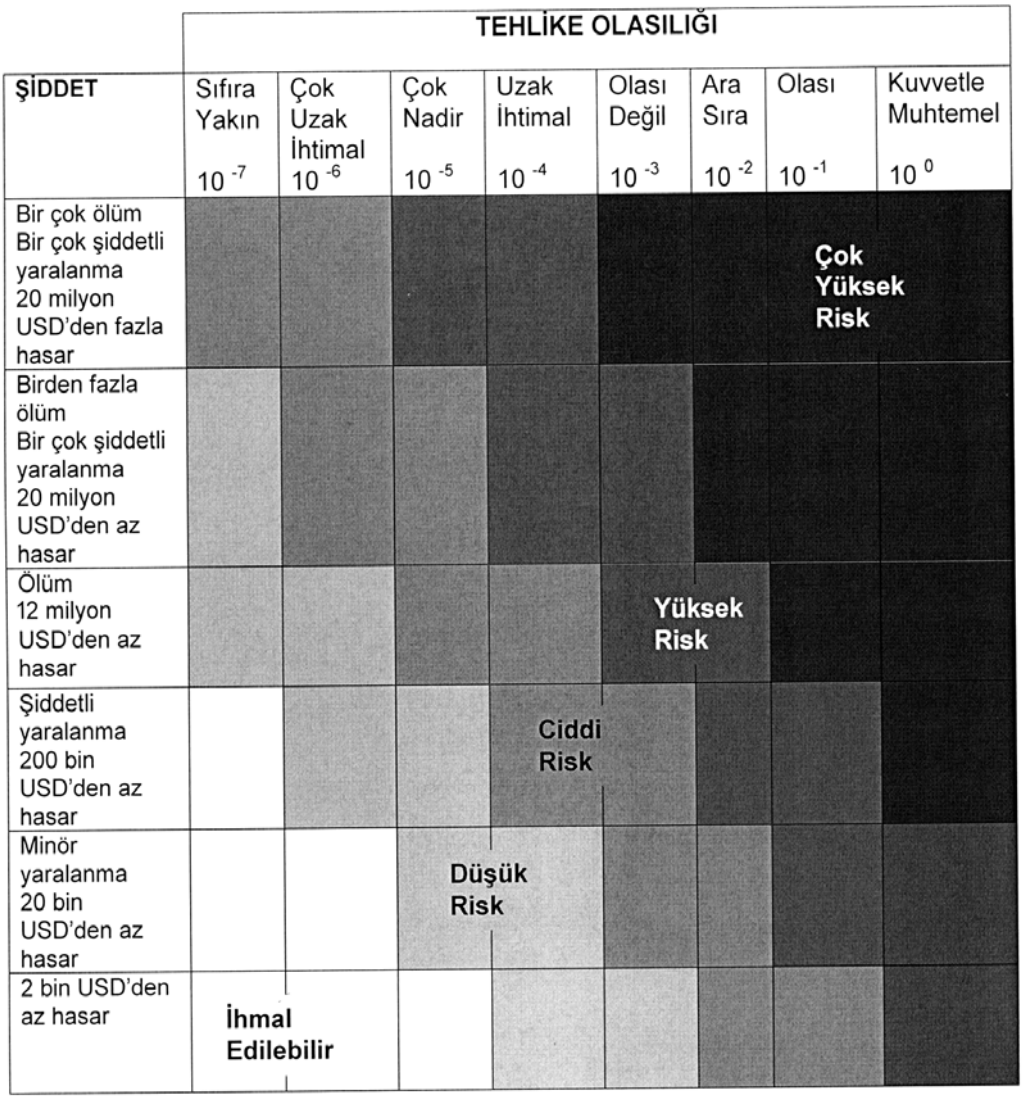
Tablo 19: Olasılık Kategorileri

AÇIKLAMA	SEVİYE	SPESİFİK BİREYSEL MADDE PARÇA	DURUM
Kuvvetle Muhtemel	A	Bir unsurun yaşam döngüsü içerisinde oluşması yüksek ihtimal dahilinde, meydana gelme olasılığı, o unsurun yaşamı boyunca 1/10'dan yüksek	Sürekli oluşur.
Muhtemel	B	Unsurun yaşam döngüsü içinde bir kaç kez oluşur, bu yaşam içinde oluşma ihtimali 1/10'dan az, 1/100'den fazla	Sık sık oluşacaktır.
Olası	C	Unsur yaşam döngüsü içinde oluşması olası olan, 1/100'den az 1/1000'den fazla.	Bir kaç kez oluşacaktır.
Olası Değil	D	Olası değil, ancak mümkün. 1/10.000'den az 1/100.000'den fazla.	Muhtemel olmayan ancak makul ve mantıklı olarak olması, ihtimal dahilinde.
Mümkün Değil	E	Muhtemel olmayan; meydana gelmesi ihtimali 1/100.000 ile milyonda bir arasında olan.	Meydana gelmesi mümkün ancak muhtemel olmayan
İmkansız	F	Meydana gelmesi mümkün olmayan. Milyonda birden az.	Bu kategori, potansiyel olarak belirlenen ancak daha sonra ortadan kaldırılan tehlikeler için kullanılır.

11.9. Makine Risk Değerlendirme (Machine Risk Asessment)

İnsan-makine sistemleri çok daha karışık olan sistemlerin parçasıdır. Örnek olarak, sosyal ve kurumsal çevrede olduğu gibi ve fiziki bir çevre (gürültü, aydınlatma, vb.).de insan-makine sistemlerinin verimli çalışmasına tesir eder. Çalışan için tehlike oluşturacak, yaralanmalarına hatta ölümlerine yol açabilecek herhangi bir mekanik tehlikeye karşı koruma önlemleri alınmalıdır. Eğer bir

Tablo 20: Tehlike Olasılığı



makinenin çalışması veya bu makineyle bir temasın olması, o makinenin operatörü veya çevresindeki bir başka kişi için tehlike yaratma ihtimali varsa, mevcut tehlikelerin tümü ya kontrol altına alınmalıdır veya ortadan kaldırılmalıdır.

Bir makinenin güvenilirliğini onaylama şartlarına bir örnek makinalar için risk değerlendirmesi TS EN ISO 12100:2010 standardında verilmiştir. Özet ola-

Tablo 21: Risk Matrisi ile Risk Değerlendirme Örneği

Tarih :	01.02.2013	RİSK DEĞERLENDİRME TABLOSU					Değerlendirme No:	3
Proses/Sistem :	Preshane						Düzenleyen:	İSG Uzmanı
Alt Sistem :	Pres Makinası						Tarih:	01.02.2013
Dizayn Rehberi:							Revizyon Tarihi:	
Risk Değ. Takımı:	İşveren Vekili, Fabrika Müdürü, İş Güvenliği Uzmanı, Bakım Amiri, İşletme Müh., Elektrik Müh						Sayfa:	1
Sistem/ Parça/ Yapılan İş	**Tehlike**	**Tehlikenin Sonucu**	**Olasılık**	**Şiddet**	**RÖS**	**Kontrol Var mı?**	**Alınması Gerekli Önlem**	
60 tonluk presde açık kalıpta delik açma	Çift el kumanda ile çalışırken, butonlardan birinin iptali	Parmaklarda uzuv kaybı	**B**	**3**	**B3**	Orta	Prese fotosel tertibatı takılması EN 13849'a göre değerlendirme yapılması	
Giyotin Makas	Giyotinin makasın korkuluğu yok	Parmaklarda veya elin tamamının kaybı	**B**	**4**	**B4**	Yok	Giyotin makasa uygun korkuluğun taktırılması EN 13850'ye göre değerlendirme yapılması	
Merdane Şekillendirme Tezgahı	Tezgahın ön korkuluk switch'i çalışmıyor	Elin veya kolun tamamen kaybı, ağır yaralanma veya ölüm	**C**	**4**	**C4**	Yok	Merdane şekillendirme tezgahının ön korkuluk switch'inin tamiri	
Kaynak işlemi	Atölye içinde kapalı ortamda kaynak yapılıyor, kaynak gazları ortama yayılıyor	Kaynak gazlarının solunması, meslek hastalığı	**C**	**3**	**C3**	Yok	Kaynağın bir bölüme alınarak havalandırma tertibatı kurulması	
ONAY : **İMZA :**								

rak, risk azlatmanın aşağıdaki şartların sağlanması durumunda mümkün olacağını ifade eder:

- Tehlikeler ve riskler tasarım ve koruma ile ortadan kaldırılabilir,
- Koruma tipi kullanıma uygun olmalıdır,
- Makinenin kullanım amacına ilişkin bilgiler açık olmadır,
- Makinenin kullanma prosedürleri, kullanacak kişi ile uyumlu olmalıdır,
- Makinenin güvenli kullanımına ilişkin talimatlar yeterince açıklanmalıdır,
- Kullanıcı makinanın kullanım ömründe oluşabilecek tüm risklerle ilgili yeterince bilgilendirilmelidir,
- Kişisel koruyucu kullanımı tavsiye ediliyor ise bunlar yeterince açıklanmalıdır.
- Ek uyarı ve önlemler yeterli olmalıdır.

Makine Risk Değerlendirmesi; makinenin yaşamının iki ana aşamasında yapılmalıdır. Bunlardan biri tasarım diğeri ise kullanım aşamasıdır. Bir makinenin tasarımı hatalı olabilir. Hatalı bir tasarıma uygun imal edilen korunma ekipmanı da hatalı yada etkisiz olabilir. Bu nedenle tasarım aşamasında risk değerlendirmesinin yapılması ne kadar önemli ise kullanım aşamasında da yapılması o kadar önemlidir.

Makineler için risk değerlendirmesinin yapılmasının asıl amacı güvenlik gereksinimlerinin belirlenmesidir. Risk değerlendirmesinin yapılması gereken ilk nokta, tasarım prosesinin başlangıcı olmalıdır. Ancak ürünün pazara sunulmasından sonra bile risk değerlendirmesinin tekrar gözden geçirilmesi gerekmektedir. Örneğin, risk değerlendirmesi operatörün davranışı hakkında varsayımlarda bulunuyor ve bu varsayımlar ürünün kullanımı esnasında gerçekleşmiyorsa değerlendirme de geçersizdir ve düzeltici faaliyet gereklidir.

Risk değerlendirmesi, makinedeki tehlikelerin, sistematik bir yolla gözden geçirilmesine imkan veren bir dizi mantık adımıdır. Gerekli olduğu durumlarda risk değerlendirmesini müteakip risk azaltılması yapılır. Bu işlemin tekrar tekrar yapılması ile tehlikelerin mümkün olduğu kadar giderilmesi ve güvenlik tedbirlerinin alınması gerçekleştirilir.

11.9.1. Makine Risk Değerlendirmesi Nasıl Yapılmalı?

Makinelerde risk değerlendirmesi çalışmalarında kullanılacak en önemli araç, TS EN ISO 12100:2010 standardı ile TS EN ISO 13849:2010'dur. Makina Emniyeti Direktifi'nin temelini de bu standartlar oluşturur. TS EN 12100 ve TS EN 13849'a göre risk değerlendirmesinde hedefler şöyle sayılabilir:

- ➢ Riski azaltmak veya ortadan kaldırmak,
- ➢ Uygun güvenlik seviyesini seçmek,
- ➢ Çalışanın korunmasını sağlamak.

11.9.2. Makine Sınırlarının Tayini

Makine ve elektrik-elektronik cihazların ve işlevesel ekipmanlarının risk analizi uygulamasında ilk aşama tehlike tipi ve yerinin kesin olarak belirlenmesidir. TS EN ISO 12100:2010'e göre; risk değerlendirmesi makine ömrünün bütün safhalarını kapsamılıdır. TS EN ISO 12100:2010' de tanımlanmış olduğu gibi amaçlanan kullanma şartlarını yani hem makinenin doğru kullanılmasını ve çalıştırılmasını hem de tahmini kötü kullanma ve düzensiz çalışma neticesinde ortaya çıkma durumlarını dikkate alarak makinenin sınırlarının tayin edilmesi gerekl idir. Makinenin tahmini kullanılma durumlarına ait bütün bilgilerin belirlenmesi gerekir, örneğin;

- ➢ Kullananların cinsiyeti,
- ➢ Daha çok hangi ellerini kullandıkları veya fiziki kabiliyetlerinin sınırı (mesela görme veya işitme özürlüler, anatomik boyutlar ve mukavemet),
- ➢ Operatörlerin eğitim tecrübe veya kabiliyetlerinin beklenen seviyeleri,
- ➢ Beceri sahibi bakım personeli veya teknisyenlerin varlığı,
- ➢ Stajyer ye çırakların varlığı;
- ➢ Makul şartlarda orada bulunması tahmin edilen tehlikeye maruz olabilcek diğer işyeri personelinin varlığı.

11.9.3. Tehlikenin Tanımlanması

Makinelerdeki bütün tehlikeler, tehlikeli durumlar ve hadiseler tanımlanmalıdır. Bu işleme yardımcı olmak gayesiyle Makine Emniyeti Yönetmeliği ve TS EN ISO 12100:2010'den yararlanılmalıdır. TS EN ISO 12100:2010; tehlikelerin sistematik analizinin yapılması için en uygun metetotları; Olası Hata Türleri

Şekil 27: Risk Analizi ve Risk Tetkikinin Adımları

ve Etkileri Analizi (FMEA) ile Hata Agacı Analizi (FTA) olarak vermiştir. Belirlenen tehlikeler listelenir ve tehlikelerin mevcut olup olmadığı ihtimali tespit edilir.

11.9.4. Risk Tahmini

Tehlikelerin tanılanmasından sonra, her bir tehlike için risk elemanlarının tayin edilmesi suretiyle risk tahmini yapılmalıdır. Mevcut bulunan tehlike ihtimallerinin nedenleri sıralanır ve bunların risk kategorileri belirlenir. Bu aşamada işlevsel güvenliğin de TS EN ISO 13849:2010'a göre sorgulanması ve PL derecelendirilmesinin de yapılması gereklidir.

EN 13849-1 harmonize standardında; makinelerin kontrol sistemlerin güvenliği ve bu sistemlerin hatalara karşı gösterdiği direnç ile ilgili 5 kategori tanımlanmıştır. Bunlar şunlardır:

Kategori B

Güvenlik Kategorisi	Genel Sistem Güvenlik Gereksinimleri	Genel Sistem Güvenlik Davranışı
B	Güvenlik Sistemi kullanım gereksinimlerini karşılayacak ve beklenilen dış etkilere dayanabilecek şekilde tasarlanmıştır. (Bu Kategori gereksinimleri genelde ortam koşullarına uygun komponent kullanılarak sağlanır. Örneğin Yük, sıcaklık, gerilim v.s.)	Güvenlik Sistemindeki tek bir hata ya da bir eksiklik güvenlik işlevinin yitirilmesine yol açabilir.

Bu kategoride tek bir hata güvenlik fonksiyonunun yerine gelmemesine yol açabilir. Kontrol sisteminin parçaları kullanım sırasında beklenilen gerilmelere ve malzemenin işlenmesi sırasında oluşan etkilere maruz kaldığında buna direnç göstermek zorundadır. Ayrıca dış etkilere karşı da direnç göstermelidir. Uygunluğun doğrulanması için kullanılan standartlar ve test raporları yeterli olur. Güvenlik fonksiyonun yitirilmesine neden olan bir hata önlem alınarak giderilebilir. Bu da TS EN ISO 12100:2010'da tanımlanan gereksinimlerini karşılayacak bir güvenlik kontrol devresi kurulanılarak gerçekleştirilebilir.

Güvenlik Kategorisi	Genel Sistem Güvenlik Gereksinimleri	Genel Sistem Güvenlik Davranışı
1	Güvenlik Sistemi Kategori B'deki gereksinimleri karşılamalı ayrıca buna ek olarak ancak iyi bilinen güvenlik prensipleri ve komponentleri kullanılmalıdır.Bunlar şunları içerir: • Belirli hataları engellemelidir . Örneğin: Kısa devre • Hataların oluşma olasılığını azaltmalıdır. Örneğin: Büyük değerler verilen komponentler, boyutlandırmada yapısal bütünlük için büyük değerler seçme. • Hataları erken algılama. Örneğin: Topraklama hatası	Güvenlik Sistemindeki tek bir hata yada bir eksiklik güvenlik işlevinin yitirilmesine yol açabilir.Ancak iyi bilinen güvenlik prensiplerinin ve komponentlerin kullanılması güvenlik sisteminde yüksek seviyede güvenirlik sağlamaktadır.

	• Hata türünün güvence altına alınması.Örneğin:Gücün kesilmesinde ortaya çıkan güvenli olmayan koşulların giderilmesi için açık devreyi zarar vermeyecek duruma getirmek. • Hatanın sonucunun sınırlandırılması.	

Kategori 1

Kategori B'deki tüm gereksinimler uygulanır, bunun yanı sıra güvenli ve iyi bilinen komponentler kullanılır. Artan güvenilirlik hatanın oluşma olasılığını ortadan kaldırmayı hedeflemektedir. Hatanın oluşma olasılığı Kategori B' den daha düşüktür ancak bir hata hala güvenlik fonksiyonun kaybolmasına yol açabilir. Bu alınan önlemlere ek olarak TS EN ISO 12100:2010'da tanımlanan gereksinimlerini karşılayacak bir güvenlik kontrol devresi kurarak da sağlanabilir . Kategori B ve 1 için şu net olarak söylenebilir; bu kategorilerde güvenilirlik komponentlerin güvenilirliğine bağlıdır.

Kategori 2

Kategori B'deki tüm gereksinimler uygulanır, bunun yanı sıra güvenli ve iyi bilinen komponentler kullanılır, güvenlik prensipleri ve bir güvenlik kontrolü uygulanır. Bu kontrol makine çalışmaya başlandığında gerçekleşir ve gerekirse

Güvenlik Kategorisi	Genel Sistem Güvenlik Gereksinimleri	Genel Sistem Güvenlik Davranışı
2	Güvenlik Sistemi Kategori B'deki gereksinimleri karşılamalı ayrıca buna ek olarak makine çalışmaya başlamasından itibaren yada periyodik kontrollerde ortaya çıkan hatalar önlenmelidir. (Bu kategori birçok güvenlik rölesi kullanmayı ve kendi kendini kontrol etmeyi önerir. Örneğin Koruma kilitlemeleri, Acil stoplar uygulamada test edilir.)	Bu Kategoride İki kontrol periyodu arasında tek bir hata yada eksikliğin ortaya çıkması güvenlik sisteminin yitirilmesine yol açabilir. Ancak periyodik kontroller hataları algılayabilir ve sistemin tam zamanında bakımının yapılmasına izin verir.

çalışma süresince periyodik olarak devam eder. Güvenlik işlevi elle yada otomatik olarak kontrol edilebilir ancak sistemde herhangi bir hata olmadığını gördüğünde sistemin çalışmasının devamına izin verir. Eğer bir hata tespit edilirse güvenlik işlevi kontrolü her an bir güvenli duruma gelebilecek bir hata çıktısı oluşturur . Bu kontrol ya makinanın kontrol sistemi tarafından yada bu iş için atanmış bir izleme cihazı tarafından gerçekleştirilir. Eğer bir hata oluşursa bu belki güvenlik işlevi kontrolleri arasında atlanabilir ancak bir sonraki kontrolde algılanır. Net olarak şu söylenebilir elle kontrol hatalarının algılanması için tek etkili yöntemdir. Bu spesifik kontrollerin sıklığı makinenin çalışması sırasında komponentler için yapılan başlangıç risk değerlendirmesine dayanır.

Kategori 3

Kategori B'deki tüm gereksinimler uygulanır, bunun yanı sıra güvenli ve iyi bilinen komponentler kullanılır ve güvenlik prensipleri uygulanır. Bu Kategorideki istenilen başka bir gereksinim de bir hatanın güvenlik işlevinin yitirilmesine neden olmamasıdır. Uygulanabildiğinde bir kritik güvenlik hatası güvenlik işlevinin sonraki işlevi, istemi sırasında yada ondan önce algılanabilmelidir. Ancak bu tüm hatalar algılanacak anlamına gelmez, hala hataların toplamı güvenlik işlevinin yitirilmesine neden olabilir. Bunun önüne geçmenin pratik yolu birçok sayıda devre kullanmaktır.

Güvenlik Kategorisi	Genel Sistem Güvenlik Gereksinimleri	Genel Sistem Güvenlik Davranışı
3	Güvenlik Sistemi Kategori B'deki gereksinimleri karşılamalı ayrıca buna ek olarak güvenlik sistemi bir tek hatadan dolayı işlevini yitirmeyecek ve pratikte hata algılayabilecek şekilde tasarlanmalıdır. Tek bir hata pratikte algılanmalıdır. (Bu Kategori güvenlik devresinin mutlak suretle izleme modülüne gereksinim duyar. Örneğin Koruma kilitleme swiçi, Acil stop düğmeleri, güvenlik röleleri v.s.)	Bu Kategoride Güvenlik Sistemindeki tek bir hata veya eksiklik "Güvenlik İşlevinin" yitirilmesine yol açmaz ve oluştuğunda algılanır.

Kategori 4

Kategori B'deki tüm gereksinimler uygulanır, bunun yanı sıra güvenli ve iyi bilinen komponentler kullanılır ve güvenlik prensipleri uygulanır. Kategoride 4'de ayrıca sistemin güvenlik ile ilgili olan herhangi bir kısmında oluşabilecek bir hata sistemin güvenlik işlevinin kaybolmasına neden olmamalıdır. Bu hata güvenlik işlevinin sonraki işlevi, istemi sırasında yada ondan önce algılanmak zorundadır. Bu imkansız ise hataların toplamı güvenlik işlevinin yitirilmesine neden olmamalıdır. Hatların toplanması iki hata olarak değerlendirilir, ancak bu çoğunlukla sistemin karmaşıklığına ve teknolojisine dayanır. Benzer hatalar tanımlanması için farklı ve özel işlemler uygulanarak ortadan kaldırılmak zorundadır. Bir hata algılandığında güvenlik işlevinin yitirilmesine olanak tanımamalıdır. Bu nedenlerden dolayı Kategori B ve 1 Kategori 2,3 ve 4 'e göre daha az güvenirliğe sahiptir. Ancak şu da unutulmamalıdır ki Kategori B ve 1 diğer Kategoriler tarafından kapsanmaktadır ve sistemde güvenlik gereksinimi az olan swiçlerde yada çevresinde uygulanır. Bu şu anlama gelmektedir, güvenli bir kontrol sisteminde birden farklı kategori uygulanabilir.

Güvenlik Kategorisi	Genel Sistem Güvenlik Gereksinimleri	Genel Sistem Güvenlik Davranışı
4	Güvenlik Sistemi Kategori B'deki gereksinimleri karşılamalı ayrıca buna ek olarak hata güvenlik işlevinin sonraki işlevi istemi sırasında yada ondan önce algılanmak zorundadır. Bu imkansız ise hataların toplamı güvenlik işlevinin yitirilmesine neden olmamalıdır. (Bu Kategori güvenlik devresi izleme modülünün aşırısına gereksinim duyar. Örneğin: Koruma kilitleme swichi, Acil stop düğmeleri, güvenlik röleleri v.s. Bu Kategoride kabul edilebilir hatalar uygulama ile, teknoloji kullanarak tanımlanır.)	Bu Kategoride Güvenlik sistemindeki tek bir hata veya eksiklik güvenlik işlevinin yitirilmesine yol açmaz ve tam zamanında kontrol yapılarak hatanın önüne geçilir.

11.9.5. Makinenin Kategorisinin Bulunması

Eğer makine ve ekipmanlar gerektiği gibi tasarlanır, tesis edilir, işletilir ve bakılırsa arızalanmazlar ve kullanım ömürleri neredeyse sonsuzdur. Nadir

olmakla beraber, eğer, meydana gelirse felakete yol açan arızalar tesadüfü olarak oluşur ve operatör hatası veya doğru biçimde yapılmayan tamiratlar gibi bir dış etken arızalara yol açar. Operatörün yaptığı çok ciddi hatalardan kaynaklanan ansızın ortaya çıkan arızalar veya tamamen olağandışı bir dış etki nedeniy-

Tablo 22: Performans Seviyesi

PL	Saat Başına Tehlikeli Hata Olasılık Ortalaması
a	$10^{-4}>PL \geq 10^{-5}$
b	$10^{-4}>PL \geq 10^{-5}$
c	$10^{-5}>PL \geq 3x10^{-6}$
d	$3x10^{-6}>PL \geq 10^{-6}$
e	$10^{-7}>PL \geq 10^{-8}$

Tablo 23: Performans Seviyesi ile SIL Arasındaki Bağıntısı

PL	SIL (IEC 61508-1'e göre derecelendirme)
a	Geçerli Değil
b	1
c	1
d	2
e	3

le ortaya çıkan arızalar hariç işletme dinamikleri analizi metodolojisi sistem hatalarını belirleyebilir, izole edebilir ve önleyebilir.

Bu aşamada eski standart EN 954 ile yeni standart EN 13849:2010 arasında büyük fark olduğu gözlenmektedir. Eski standartta kategori sadece "Risk Graf" yöntemi ile bulunurken, yeni standartta "Performans Seviyesi", "Risk Graf" ve "Hata Bulma Kapsamı" ile kategorilerin tespiti uygun görülmüştür. Aşağıda EN 13849:2010'da kullanılması öngörülen "Performans Seviyesi" (Performance Levels -PL) verilmiştir;

Bu prensip, bir fonksiyonu gerçekleştirmek için, amaçlanan kullanma şartları altında donanımın kullanılması ile ilgili bütün karışıklıklara ve zorlamalara dayanabilecek birleşenler kullanıldığı zaman, kullanım için tespit edilen bir süre içinde makinenin tehlikeli bir şekilde çalıştırılmasına sebep olan arıza olmaksızın güvenliğin sağlanmasının istendiğinde uygulanmalıdır. Dikkate alınması gereken çevre stresleri örnek olarak şunlardır: Darbe, titreşim, soğuk, toz, tahrip edici maddeler, statik elektrik, manyetik ve elektriki alanlar.

11.9.6. Her Parçanın Tehlikeli Hata Yapma Ortalama Zamanı (Mean Time to Dangerous Failure of Each Channel - $MTTF_d$)

Her sistemde bütünü oluşturan parçalar birbirlerini etkilediği gibi bütünü de etkilemektedir. Alt sistemlerden herhangi birinde aksaklık, bütüne de yansımaktadır. Sistemdeki bir durumu anlayabilmek, onu oluşturan alt sistemleri ve bu sistemlerin birbirleriyle olan ilişkilerini inceleyerek mümkün olabilmektedir.

Tablo 24: Makinenin Parçalarının Ortalama Hata Yapma Olasılığı

SEVİYE	$MTTF_d$ ARALIKLARI
Düşük	3 yıl ≤ $MTTF_d$ < 10 yıl
Orta	10 yıl ≤ $MTTF_d$ < 30 yıl
Yüksek	30 yıl ≤ $MTTF_d$ < 100 yıl

Sistem teorisi, makinelerin parçalardan oluştuğu ve bu parçaların makinelerin amaçlarını gerçekleştirmek üzere birbirleriyle etkileşim içinde olduğu düşüncesini taşımaktadır. $MTTF_d$; makinedeki her parça nedeniyle; hatalar arası düzeltilemeyen normal operasyon süresinin matematiksel olarak hesaplanmasıdır. Makine güvenilirliğinde; makinenin parçalarının ortalama hata yapma olasılığının saatle göstergesidir.

EN 13849'a göre, $MTTF_d$ **Tablo 24**'e göre derecelendirilir;

11.9.7. B_{10d}'den Hareketle, Komponentler (Parçalar) İçin $MTTF_d$'in Hesaplanması

Parçaların %10'unun ciddi olarak devre dışı kalması için gerekli olan ortalama devir (dönem) sayısı B_{10d}, parçanın üreticisi tarafından, test metodları için ilgili ürün standartlarına uygun olarak, belirlenmelidir (IEC 60957, ...)

Yani, komponentlerin (parçaların) tehlikeli çökme modları, değişim zamanlarının değiştirilmesi veya bir uç noktaya ulaşılması vb. için tanımlanmalıdır.

Eğer testlerde parçaların tamamı tehlikeli biçimde çökmezse (örneğin 7 cihaz test edilmiş, bunlardan sadece 5'i tehlikeli biçimde çökmüşse) tehlikeli biçimde çökmemiş olan komponentleri dikkate alan bir analiz yapılmalıdır.

B_{10d} ve n_{op} ile, ortalama yıllık operasyon sayısı, komponentler için $MTTF_d$ şöyle hesaplanabilir.

Burada komponent'in aplikasyonu için yapılan kabul ise,

n_{op} : günde saat cinsinden olmak üzere, ortalama operasyon süresi

Eğer b_{10}'un tehlike oranı (kesri) verilmezse, b_{10}'un %50'si kullanılabilir, dolayısıyla ;

$b_{10d} = 2 * b_{10}$ eşitliği tavsiye edilir.

d_{op} : yılda gün cinsinden olmak üzere, ortalama operasyon süresi

$t_{döngü}$: komponentin birbirini takip eden iki döngüsünün başlangıç zamanları arasındaki ortalama zaman (mesela bir vananın çevrilmesi): döngü başına saniye.

$$MTTF_d = \frac{B_{10d}}{0{,}1 \ . \ n_{op}}$$

$$n_{op} = \frac{d_{op} \ h_{op} \ 3600 \ s/h}{t_{döngü}}$$

Komponentin operasyon zamanı T_{10d}'i geçemez, komponentlerin %10'unun tehlikeli biçimde çökmesi için ortalama zaman ise;

$T_{10d} = \frac{B_{10d}}{n_{op}}$ olarak verilmiştir.

11.9.8. Hata Tespit Kapsamı (Diagnostic Coverage –DC)

Makinelerde zamanında ve sıhhatli ayarlar yapılması durumunda, daha iyi verim elde edilir.

Tablo 25: Hata Tespit Kapsamı

SEVİYE	DC ARALIKLARI
Hiç	DC << %60
Düşük	%60 ≤ DC < %90
Orta	%90 ≤ DC < %99
Yüksek	%99 ≤ DC

11.9.9. Ortalama DC'nin Tahmin Edilmesi

DC, belirlenen tehlikeli çökme oranlarının, toplam tehlikeli çökmelerin oranına bölünmesiyle elde edilir. Bu tanıma göre, ortalama DC_{ort}, ortalama tespit kapsamı, aşağıdaki formülden hesaplanabilir.

$$DC_{ort} = \frac{\frac{DC_1}{MTTF_{d1}} + \ldots\ldots\ldots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \ldots\ldots\ldots + \frac{1}{MTTF_{dn}}}$$

Burada, tüm komponentleri (parçaları) hiç bir çökme dışarı bırakılmadan dikkate alınmalı ve toplanmalıdır. Her blok için MTTFd ve DC değerleri dikkate alınmalıdır. Bu formülde, DC, komponentin (parçanın) belirlenen tehlikeli çökmelerinin (parçanın çökmesine karşı alınacak önlemler hesaba katılmaksızın) çökme oranının parçanın tüm tehlikeli çökmelerinin çökme oranına bölünmesiyle oluşan kesirdir. Böylece, DC test cihazına değil test edilen parçaya işaret eder. Çökmesi belirlenmeyen parçalar (yani test edilmeyenler) için DC=0 olur.

11.9.10. Donanımın Güvenirliği Yoluyla Tehlikelere Maruz Kalmanın Sınırlanması

Makinenin bütün parçalarının arttırılmış olan güvenilirliği, kazanın olma sıklığını azaltır ve dolayısı ile tehlikelere maruz kalmayı düşürür. Bu kural, kumanda sistemlerine olduğu gibi, güç sistemlerine de, makinenin diğer fonksi-

yonlarına olduğu gibi güvenlik fonksiyonlarına da uygulanır. Güvenilir olduğu bilinen güvenlik bakımından kiritik parçalar (mesela, sensörler, bariyerler vb.) kullanılmalıdır. Koruyucunun parçaları ve güvenlik tertibatları, özellikle arızalanmaları durumunda, kişilerin can güvenliği tehlikeye girdiği durumlarda güvenilir olmalı ve ayrıca güvenirliklerinin azlığı onları devreden çıkartılma imkanını vermemelidir.

Tablo 26: Makine Güvenlik ve Koruma Kategorileri

Kategori	B	1	2	2	3	3	4
DC_{ort}	Hiç	Hiç	Düşük	Orta	Düşük	Orta	Yüksek
$MTTF_d$							
Düşük	a	Kapsamaz	a	b	b	c	Kapsamaz
Orta	b	Kapsamaz	b	c	c	d	Kapsamaz
Yüksek	Kapsamaz	c	c	d	d	d	e

Güvenlik koruma tedbirleri, kişileri makul olarak kaçınılamayan veya tasarım yoluyla yeterince sınırlanamayan tehlikelere karşı koruma amacıyla kullanılmalıdır. Koruyucuların ve güvenlik tertibatlarının çeşitli tipleri, TS EN 12100:2010'da açıklanmıştır. Muayyen güvenlik koruma tedbirleri çalışanları, birden fazla tehlikelere maruz kalmaktan korunmak amacıyla kullanılır. EN 13849:2010 harmonize standardında; makinelerin kontrol sistemlerin güvenliği ve bu sistemlerin hatalara karşı gösterdiği direnç $MTTF_d$ ile DC_{ort} ilgili kategoriler aşağıda tanımlanmıştır

11.9.11. Koruyucuların ve Güvenlik Tertibatlarının Seçimi

EN 13849-1 harmonize standardının esas amacı; hareketli parçaların meydana getirdiği tehlikelere karşı güvenle korumayı sağlamak ve koruyucuların ve güvenlik tertibatlarının, makinenin tabiatına ve tehlike bölgelerine ulaşma ihtiyacına uygun şekilde seçimine kılavuzluk etmektir.

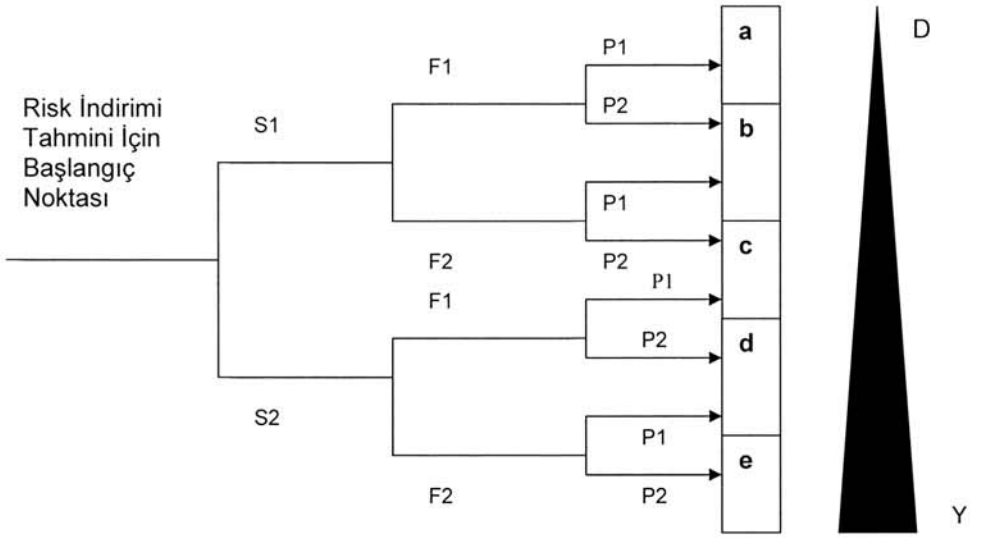
Belirli bir makine için bir güvenlik koruma tertibatının doğru olarak seçimi, bu makine için yapılan risk değerlendirilmesine dayanmalı ve seçilen güvenlik koruma tertibatı, risk değerlendirme raporunda detaylı olarak tarif edilmelidir.

Belirli bir tip makine veya tehlike bölgesi için uygun bir güvenlik koruma tertibatının seçiminde, sabit bir koruyucunun basit olması gerektiği daima akılda tutulmalı ve makinenin normal çalışma (herhangi bir yanlış çalışma olmaksızın) sırasında bir operatörün tehlike bölgesine ulaşmasının gerekmediği yerlerde kullanılmalıdır.

Sık ulaşma ihtiyacı gerektiğinde, sabit bir koruyucunun sökülmesi ve yerine takılması elverişsiz durumlar meydana getirdiğinden, bunun yerine hassas algılama tertibatı kullanılmalıdır.

Makinenin normal çalışması sırasında tehlikeli bölgelere ulaşmanın gerekmediği durumlarda güvenlik koruma tedbirleri; besleme ve boşaltma tertibatları, ara kilitleme tertibatı, kendiliğinden kapanan koruyucu, dayama, engel veya tünel koruyucu vb. sabit koruyuculardan kulanılabilir. Koruyucudaki açıklıklar ise TS EN ISO 13857'e (El ve kolların tehlikeli bölgelere erişmesine karşı güvenlik mesafeleri) uygun olmalıdır.

Koruyucuların güvenlik tertibatlarının seçiminde TS EN 13849:2010 harmonize standartında "Risk Graf" olarak belirtilen ve uygulama mantığı da IEC 61508 standartında verilen "İşlevsel Güvenlik" e bazı farklar dışında uymaktadır. TS EN 13849:2010 harmonize standartında verilen "Risk Graf" ugulaması aşağıda verilmiştir;



S Kazanın sonucu

S1 Hafif yaralanma

S2 Ciddi yaralanma, kalıcı sakatlık veya ölüm

F Tehlike bölgesinde bulunma

F1 Nadiren veya kısa sürelerle sık sık

F2 Sık sık sürekli veya uzun süreli

P Tehlikenin önlenme olasılığı

P1 Belli durumlarda mümkün

P2 Fiilen mümkün değil

Makinenin normal çalışması sırasında tehlikeli bölgelere ulaşmanın gerekli olduğu durumlarda, güvenlik koruma tedbirleri ara kilitlemeli koruyucu, hassas algılama tertibatı, kendiliğinden kapanan koruyucu, iki el kumanda tertibatı vb. koruyuculardan seçilebilir.

Makineler, üretim operatörünün korunması için sağlanan güvenlik koruma tedbirleri, mümkün olduğu kadar, operatörlerin görevlerini yürütmekte iken bir engel teşkil etmeyecek ve korunmasını temin edecek şekilde tasarımlanmalıdır.

Bu mümkün olmadığında (mesela, makine çalışıyor durumda iken sabit koruyucunun sökülmesinin veya güvenlik tertibatların etkisiz kılınmasının gerektiği durumlarda), makine, riski mümkün olduğu kadar azaltan uygun koruyucularla teçhiz edilmelidir.

Makinenin güç kaynağına bağlı kalmasını gerektirmeyen durumların veya çalışmaların (özellikle bakım ve onarım işleri) yürütülmesi durumunda, makinenin kapatılması amacıyla ayırma ve üzerindeki mevcut enerjinin sönümlenmesi işlemleri en yüksek güvenlik seviyesini sağlamalıdır.

11.9.12. Kontrol Önlemi

Belirlenen risklerle ilgili alınan ve/veya ihtiyaç duyulan önlemler belirlenerek risk azaltılır. Alınan önlemlerin yeterliliğine ve uygulanıp uygulanamayacağına karar verilir. Analiz sonucunda kontrol önlemleri belirlenirken gerek duyulması durumunda diğer analiz yöntemlerine başvurulur. (Örneğin, ETA, FTA , FMEA vb.)

Kontrol önlemi alındıktan sonra, alınan yeni güvenlik tedbirinin ilave bir tehlike yaratıp yaratmadığının analist tarafından kontrol edilmesi önemlidir.

11.10. Tehlike Analizi ve Kritik Kontrol Noktaları (Hazard Analysis and Critical Control Points - HACCP)

Tehlike analizi ve kritik kontrol noktaları analizi(HACCP), bir ürünü tehlikelere karşı korumak, kalite güvenirliğini sürdürmek ve güvenliğini sağlamak için bir işlemin tüm ilgili parçalarında, yerinde denetimler koymaya ve tehlikeyi belirlemeye yönelik bir yapı sağlar. HACCP nihai ürün denetiminden ziyade, süreç boyunca kontrol ile riskleri en aza indirgemeyi amaçlamaktadır.

Referans Standart:

- ISO 22000, *Gıda güvenliği yönetim sistemleri – Gıda zincirine yönelik kurum gereksinimleri (Food safety management systems – Requirements for any organization in the food chain)*

HACCP, NASA uzay programına gıda kalitesi sağlamak amacıyla geliştirilmiştir. Şu anda gıdaların fiziksel, kimyasal ve biyolojik kirliliğine karşı kontrol riskleri için gıda zinciri içerisinde herhangi bir yerde faaliyet gösteren kuruluşlar tarafından kullanılır. Aynı zamanda ilaç üretiminde ve tıbbi cihazlarda kullanılmak için kapsamı genişletilmiştir. Kritik parametrelerin belirlenebileceği, tehlikelerin kontrol edilebileceği ve diğer teknik sistemlere de genelleştirilerek uygulanabilecek, bir işlemdeki kritik noktaları tanımlama prensibidir.

Girdi:

HACCP, temel akış şemaları veya süreç şemaları ve ürün güvenirliğini, kalitesini, güvenliğini veya süreç sonucunu etkileyebilecek tehlikeler hakkındaki bilgileri girdi olarak kullanır.

Süreç:

HACCP aşağıdaki yedi ilkeden oluşmaktadır:

- Tehlikeleri ve bu tür tehlikeler ile ilgili önleyici kontrol adımlarını belirlemek,
- Tehlikelerin kontrol edilebileceği veya yok edilebileceği süreçte bulunan noktaları açıklamak (kritik kontrol noktaları),
- Tehlikeleri kontrol etmek için gerekli kritik sınırları oluşturmak, yani her kritik kontrol noktası için tehlikenin kontrol edilebilmesini sağlamak için belirli parametreler dahilinde çalışmaları düzenlemek,

- Tanımlanmış aralıklarla her kritik kontrol noktası için kritik sınırları belirlemek,
- Süreç oluşturulan sınırlar dışında kalır ise, düzeltici faaliyetler oluşturmak,
- Her adım için kayıt tutma ve belgelendirme prosedürlerini uygulamak.

Sonuçlar:

Bir tehlike analizi çalışması ve bir HACCP planını içeren belgeli kayıtlardır. İşlemin her adımı için tehlike analiz çalışma listeleri oluşturulur. Bu aşamada, tanıtılan, kontrol edilen veya ortaya çıkabilecek tehlikeler, tehlikenin büyük bir risk teşkil edip etmediği, bu risklerin sonuç ve olasılıkları, önem gerekçesi ile kontrol önlemlerinin bu aşamada uygulanabilir olup olmayışı raporlanır.

Tehlike Analizi ve Kritik Kontrol Noktası (HACCP) planı, özel bir tasarımın, ürünün, sürecin veya prosedürün kontrolünü güvence altına almak için uygulanacak yöntemleri açıklamaktadır. Söz konusu planda aşağıda verilen hususlar yer alır;

- Tüm kritik kontrol noktalarının bir listesi,
- Her bir kritik kontrol noktası için önleyici tedbirlere yönelik kritik limitler,
- Kontrol faaliyetlerinin belirlenmesi ve sürdürülmesi (belirleme işleminin neyi, nasıl, ne zaman belirleyeceği, işlemin kim tarafından gerçekleştirileceği dahil),
- Kritik limitlerden sapma yaşandığı tespit edilirse düzeltici faaliyetler,
- Araştırma ve kayıt tutma faaliyetleri.

Güçlü ve Zayıf Yönler:

Analizin güçlü yönleri şu hususları kapsamaktadır:

- Risk saptama/azaltma faaliyetlerine yönelik belgelendirilmiş kanıtlar sunan yapılandırılmış bir süreç izler,
- Tehlike önleme ve risk kontrolü faaliyetlerinin, belirli bir sürecin hangi noktasında ve nasıl gerçekleştirilmesi gerektiğine dair bilgi sağlar,
- Nihai ürün denetimine güvenmekten ziyade süreç boyunca gerçekleştirilecek daha etkili bir risk kontrolü içerir,
- İnsan faaliyetlerinden kaynaklanan tehlikeleri saptamaya ve söz konusu tehlikelerin baş gösterdiği aşamada veya sonrasında nasıl kontrol edilebileceğine yönelik yeterlilikler içerir.

Zayıf Yönler:

- Tehlike Analizi ve Kritik Kontrol Noktası Analizi (HACCP), tehlikelerin saptanmasını, teşkil ettikleri risklerin belirlenmesini ve süreç verileri şeklinde önemlerin anlaşılmasını gerektirir,
- Uygun kontroller de saptanmalıdır çünkü HACCP süresince kritik kontrol noktaları ve kontrol parametrelerinin belirlenmesi ve bu amaç doğrultusunda diğer araçlar ile birleştirilmesi gerekir,
- Kontrol parametreleri belirlenen limitleri aştığında gerekli adımların atılması, istatistiksel açıdan önemli olan ve dolayısıyla faaliyete geçilmesini gerektiren kontrol parametrelerine yönelik aşamalı değişikliklerinin gözden kaçırılmasına yol açabilir.

11.11. …Olursa Ne Olur? (What If..? SWIFT Tekniği)

Risk değerlendirme çalışmalarında ilgili tarafların en önemlilerinden biri de tasarımcılar ve mühendislerdir. Risk yönetimi tüm mühendislik boyutlarının entegre bir parçası olmalıdır. Sistematik bir şekilde uygulanabilmeli ve kontrol edilebilmelidir. İşyerindeki potansiyel tehlikeler, hatalar ve risklerin ortaya çıkarıldığından emin olunmalıdır. Bunlar, işyerindeki güvenliği birçok açıdan etkiler: teknik yerleşim, proses veya sistemlerin performansı vb. Özellikle kimyasal prosesler için tasarımcılar ve mühendislerin sorumluluğu anahtar öneme sahiptir ve bu durum ancak proses tehlike analizleri ile açığa çıkarılabilir.

Bu konuda iyi bir örnek İngiltere Mühendisler Konseyinin (1993) " Risk konularında Profesyonel Uygulama Talimatları" kitabıdır. Bu kitapta on temel nokta ele alınmıştır. Bunların 4. noktasında: "Özellikle proses riskleri konularında sistematik bir yaklaşım benimsenmelidir. Risk yönetimi tüm mühendislik boyutlarının entegre bir parçası olmalıdır. Sistematik bir şekilde uygulanabilmeli ve kontrol edilebilmelidir. İşyerindeki ve özellikle de kimyasal proseslerdeki potansiyel tehlikeler, hatalar ve risklerin ortaya çıkarıldığından emin olunmalıdır." denilmektedir. Proses tehlike analizi, tasarım ve mühendislik faaliyetlerinde bir araçtır ve aşağıdaki hususlar ile ilgili fayda sağlar;

- Şartların gerek resmi gerek gayrı resmi olarak sağlanmasına yardım eder,
- Güvenlik çalışmalarının ciddi şekilde yürütüldüğünü gösteren dökümanlar üretir,
- Proses veya sistem daha güvenli olur.

SWIFT Tekniği de proses tehlike analizi olarak sıklıkla kullanılan bir tekniktir. Aslına bakıldığında SWIFT Tekniği, Tehlike İşletilebilirlik Çalışmasına (HAZOP) bir alternatif olarak geliştirilmiştir. Sistematik ve ekip bazlı bir çalışmadır. Yönetici, katılımcıları riskleri saptamaya teşvik etmek için çalışma alanında bir dizi "ipucu" kelimesi ya da kelime öbeği kullanır. Yönetici ve ekip, bir sistemin, tesis öğelerinin, kuruluşun ya da prosedürün normal işletim ve davranış sapmalarından nasıl etkileneceğini soruşturmak için ipuçlarıyla birlikte standart "Ne-Eğer" ya da "Olursa Ne Olur?" türünden soru cümleleri kullanır. SWIFT, genellikle sistem düzeyinde uygulanır ve HAZOP'a göre daha az ayrıntılıdır.

SWIFT'in başlangıçta kimyasal ve petrokimyasal tesislere yönelik bir tehlike çalışması olarak tasarlanmasına rağmen, günümüzde genellikle sistemlere, tesis öğelerine ve prosedürlere yaygın şekilde uygulanmaktadır. Özellikle de değişikliklerin sonuçlarını ve bu nedenle oluşan riskleri incelemek için kullanılır.

Bu metod, fabrika ziyaretleri ve prosedürlerin gözden geçirmesi esnasında yararlıdır, hali hazırda var olan kaçınılmaz potansiyel tehlikelerin tespit edilme oranını yükseltir. Bu metod işlemlerin herhangi bir aşamasında uygulanabilir ve daha az tecrübeli risk analistleri tarafından yürütülebilir.

Genel soru olan " .....ise Ne Olur?" ile başlar ve sorulara verilen cevaplara dayanır. Aksaklıkların muhtemel sonuçları belirlenir ve sorumlu kişiler tarafından herbir durum için tavsiyeler tanımlanır. Bilgiler yazılı format ile sağlanır ve çevresel değerlendirme raporu ile birlikte derlenir.

"Ne-eğer" kalıbı, ipucu kelimesi ya da bir konu kullanılarak yöneltilen soru ile tartışma başlatılır. Kullanılacak "ne-eğer" kalıpları arasında;

- "..... olursa ne olur?",
- "Herhangi biri ya da herhangi bir şey ..... yapabilir mi?",
- "Burada bulunan herhangi biri hiç ..... ile karşılaştı mı?" gibi sorular bulunmaktadır.

Risk değerlendirme raporunda, tehlikelerin tipini tarif etmek ve tavsiyeleri değerlendirmek maksadıyla kullanılır. Bu metod ile yapılan risk değerlendirmesinde, risk analiz timinin dikkati yanlızca bir noktaya odaklanabilir yada timin tecrübesi o noktadaki tehlikeyi görmelerine olanak vermez. Bu metod çeşitli disiplinlerdeki takım üyelerinin tecrübelerine dayanması ve bu takımdaki üyele-

rin tecrübelerine göre sonuçların çok fazla etkilenmesi nedeniyle informal bir metoddur.

SWIFT'in başlangıçta kimyasal ve petrokimyasal tesislere yönelik bir tehlike çalışması olarak tasarlanmasına rağmen, günümüzde genellikle sistemlere, tesis öğelerine, prosedürlere ve kuruluşlara yaygın şekilde uygulanmaktadır. Özellikle de değişikliklerin sonuçlarını ve bu nedenle değiştirilen veya oluşturulan riskleri incelemek için kullanılır.

Girdi:

Çalışma başlamadan önce söz konusu sistem, prosedür, tesis öğesi ve/veya değişiklik dikkatli bir biçimde tanımlanmalıdır. İç ve dış bağlamlar, uzman tarafından gerçekleştirilecek olan görüşmeler ile doküman, plan ve çizim çalışmaları yoluyla oluşturulmalıdır. Normal şartlarda çalışmaya ilişkin öğeler, durum ya da sistemler, analiz sürecini kolaylaştırmak için parçalara ve ana unsurlara bölünür ancak söz konusu bölme işlemi, HAZOP için gereken tanımlama düzeyinde olduğu kadar hasas yapılmaz.

Bir diğer anahtar girdi ise ekipte mevcut olan ve büyük bir dikkatle seçilmesi gereken uzmanlık ve deneyimdir. Çalışmada yer alacak olan tüm ekip üyelerinin benzer öğeler, sistemler, değişiklikler ve durumlarda tecrübe sahibi olması gerekir.

Süreç:

Genel süreç aşağıdaki gibidir:

- Yönetici, çalışma başlamadan önce standart bir gruba dayalı ya da olası tehlike veya riskleri kapsamlı şekilde ele almak için oluşturulmuş uygun ipucu listesi hazırlar,
- Çalışma alanında prosesin, sistemin, değişikliğin ya da durumun iç ve dış bağlantıları ile çalışmanın kapsamı üzerine tartışılır ve karara varılır,
- Yönetici, şu soruların katılımcılar tarafından düşünülmesini ve tartışılmasını ister:
  - bilinen risk ve tehlikeler,
  - eski deneyimler ve vakalar,
  - bilinen ve mevcut kontroller ile muhafazalar,
  - düzenleyici gereklilikler ve kısıtlamalar.

- "Ne-eğer" kalıbı, ipucu kelimesi ya da bir konu kullanılarak yöneltilen soru ile tartışma başlatılır. Amaç, çalışma ekibinin olası senaryoları, bunların sebeplerini, sonuçlarını ve etkilerini açıklamaya sevk etmektir,
- Saptanan riskler özetlenir ve ekip, uygulanması gereken kontroller üzerinde kafa yorar,
- Riskin tanımı, nedenleri, sonuçları ve umulan kontroller ekibin onayına sunulur ve kayda geçirilir,
- Ekip söz konusu kontrollerin yeterli ve etkili olup olmadığı üzerinde durur ve risk kontrol verimliliği çizelgesi oluşturur. Verimlilik yeterli düzeyin altındaysa; ekip, risk müdahale görevleri hakkında biraz daha düşünür ve olası kontroller tanımlanır,
- Söz konusu tartışma süresince, diğer risklerin saptanabilmesi için birkaç "ne-eğer" sorusu daha yöneltilir.
- Yönetici, tartışmayı gözetim altında tutmak ve ekibin tartışması için daha fazla konu ve senaryo öne sürmek için ipucu listesinden faydalanır,
- Öncelik sırasına göre oluşturulan faaliyetleri derecelendirmek için kalitatif veya yarı kantitatif risk değerlendirme yöntemi kullanılabilir. Söz konusu risk değerlendirme çalışması, normal şartlarda mevcut kontroller ve bunların verimlilikleri göz önüne bulundurularak gerçekleştirilir.

Çıktılar:

Çıktılar; risk derecelendirmesi, faaliyet ve görevlerin yanı sıra risklerin kaydını da içerir. Böylelikle, söz konusu görevler aksiyon planı için bir temel oluşturur.

Güçlü ve Zayıf Yönler:

SWIFT'e yönelik güçlü yönler şunlardır:

- Proses veya sistem, durum veya olay, organizasyon veya faaliyetin bütün şekillerine yaygın olarak uygulanabilir,
- Ekip tarafından minimal hazırlığa ihtiyaç vardır,
- Nispeten hızlıdır, büyük tehlikeler ve riskler hızlı bir şekilde çalışma oturumu içerisinde su yüzüne çıkar,
- Çalışma 'sistem odaklıdır' ve sadece bileşen arızasının ya da hatasının sonuçlarını incelemek yerine; katılımcılara sistem yanıtındaki sapmalara bakma olanağı tanır,

- Süreç ve sistemlerin iyileştirilmesi adına fırsatları belirlemek için kullanılır ve genellikle süreç ve sistemlerin başarıya ulaşma olasılıklarını geliştirme imkanı tanır,
- Mevcut kontrollerin verimliliğinin sorgulanmasına, risklere daha fazla müdahale gerekip gerekmediğinin irdelenmesine fırsat tanır,
- HAZOp'a göre daha az bir çabayla bir tehlikelerin ve risk önceliğinin oluşturmasını sağlar, ancak HAZOP kadar detaylı bir inceleme olmadığı için hassas detayların kaçırılmasına neden olabilir,
- SWIFT tekniği, sadece kalitatif bir çalışma içinde riskler ve tehlikeleri tanımlamak için kullanılabilir.

SWIFT Sınırlamaları:

- Yeterli olması için deneyimli ve yeterli bir kolaylaştırıcıya/uzmana ihtiyaç duyar,
- Çalışma ekibinin zamanın boşa harcanmasını önlemek üzere dikkatli bir ön hazırlık gerektirir,
- Çalışma ekibi yeterince geniş bir deneyim ve birikimine sahip değilse veya veri kaynakları kapsamlı değilse, bazı risk ve tehlikeler tanımlanamayabilir,
- Teknik HAZOP tekniğinde olduğu gibi yüksek-seviyeli uygulama sağlamaması sebebi ile özellikle karmaşık, ayrıntılı veya bağlantılı proseslerde tüm normal şartlardan sapma nedenlerini su yüzüne çıkaramayabilir.

Tablo 27: Örnek What If Risk Değerlendirmesi

"What If?"	Sonuç	Tavsiye	Sorumlu Personel	Alınan Eylemin Zamanı
Fırındaki basınç artar ise ne olur?	Yüksek basınç – patlama	- Basınç artışı durumunda gaz akışını durduracak acil durum kapatma sistemi kur. - Emniyet valfini yedekle.	Plan Mühendisi	
Emniyet valfi kaçak yapar ise ne olur?	- Duman fırındaki boşluklardan sızabilir. - Karbon Monoksit (CO) seviyesi artabilir - Çalışanlar CO gazına maruz kalabilir.	- Duman ve CO detektörleri tak ve acil durum alarmına bağla. -Emniyet valfini "Güvenilirlik Merkezli Bakım" çerçevesinde kritik ekipman listesine dahil et.	Bakım Amiri	

11.12. Tehlike ve İşletilebilme Çalışması Metodolojisi (Hazard and Operability Studies- HAZOP)

Kimyasal işleme endüstrisinde, sık sık büyük kazalar olma potansiyeli vardır. Genel seviyede özellikle kimya sanayii ve kimyasal proseler için, kanunlar, yönetmelikler ve sandartlar karşılanması gereken birtakım kriterleri koyarlar. Bu karmaşık bir konudur ve uygulamada tümüyle yerine getirilmeleri oldukça zordur. Bununla birlikte, genel bir risk değerlendirme stratejisi ile mevcut yükümlülüklerin yerine getirildiğini göstermek de oldukça zordur. Yine genel bir risk değerlendirme tekniği ile de proseslerin tasarım veya işletilmesi aşamasında tüm tehlikelerin tanımlamasını yapmak ve kontrol önlemlerinin yeterliliğine ve güvenilirliğine karar vermek de oldukça zor bir süreçtir.

HAZOP'un ana fikri zararlı sonuçları olabilecek sapmaların araştırmasının yapılmasıdır. HAZOP tekniği tasarımcıların akla yatkın tehlikeleri belirlemesini sağlamak üzere belirli bir mantık çerçevesinde düşüncelerini canlandırmaktır.

Proses endüstrileri için risklerin kabul edilmesi ile ilgili nitel kriterleri sayacak olursak;

- Parçaların ve güvenlik bileşenlerinin sağlamlığı gibi bir performans şartı, örneğin güvenlik valfleri.
- Güvenli durumda kalma şartı, yani belli bir parça çalışmasa bile güvenli durum zarar görmez,
- Kapsama şartı, güvenlik sisteminin tasarım aşamasında iken tüm sapmalarının tanımlanması,
- Tek veya çift hata kriteri, belli bir kazayı önlemek için kaç tane farklı güvenlik sisteminin bulunması gerektiğini tanımlar.
- Kapsamlı savunma şartı, tek hata kriterinin sistemi savunmasız bırakmaması gerekir.

Bu tipte kriterler, güvenlik kriterlerinin sağlandığını gösteren özel bir analizi gerektirirler, yani Proses Tehlike Analizleri…

HAZOP, Tehlike (HAZard) ve İşletilebilirlik (OPerability) çalışmasının kısaltmasıdır. Planlı veya mevcut ürünün, sürecin, prosedürün veya sistemin yapısal ve sistematik olarak incelenmesidir. Kişilere, ekipmana, çevreye ve/veya organizasyonel hedeflere yönelik risklerin belirlenmesine yönelik bir yöntemdir. Çalışma takımından, aynı zamanda risklere müdahale edilmesi için mümkün olan en iyi çözümün üretmesi beklenir.

Referans Standart:

- *IEC 61882, Tehlike işletilebilirlik çalışmaları (HAZOP çalışmaları) – Uygulama rehberi (Hazard and operability studies (HAZOP studies) – Application guide)*

HAZOP süreci, tasarımın, sürecin, prosedürün veya sistemin her aşamasında tasarım planının veya çalışma koşullarının nasıl başarısız olabileceği sorgulayan kılavuz kelimelerinin kullanımına dayalı niteliksel bir tekniktir. Genellikle bir dizi toplantı esnasında çoklu bir disiplin takımı ile gerçekleştirilir.

Kimya endüstrisi tarafından,bu sanayinin özel tehlike potansiyelleri dikkate alınarak geliştirilmiştir. Multi disipliner bir tim tarafından,kaza odaklarının saptanması, analizleri ve ortadan kaldırılmaları için uygulanır. Belirli anahtar ve kılavuz kelimeler kullanarak yapılan sistemli bir beyin fırtınası çalışmasıdır. Çalışmaya katılanlara,belli bir yapıda sorular sorulup,bu olayların olması veya olmaması halinde ne gibi sonuçların ortaya çıkacağı sorulur. "Tehlike ve İşletilebilme Çalışmaları" olarak adlandırılan bu metod, kimya endüstrisinde tehlikelerin tanımlanmasında yardımcı olması maksadıyla proses dizayn aşamasında ve proses işletme esnasında yaygın olarak kullanılır. Bu alanda geniş kabül görmüş bir metoddur, çünkü bir prosesteki sapmaların etkilerinin tespit edilmesini ve normal koşullar altındaki prosesle karşılaştırma yapılma imkanı sağlar.

Terminoloji ve Tanımlar:

Tekniğin nasıl uygulanacağını anlatan kapsamlı birçok kılavuz hazırlanmıştır, bunlardan bazıları IEC 61882 HAZOP Uygulama Rehberi (2001)'dir, bu rehbere göre;

Normal İşletme Koşulları (Operational States): Normal işletme ve beklenen işletme olaylarını kapsayan durumlar.

Normal İşletme (Normal Operation): İşletme sınır ve şartları ihlal edilmeksizin bir kimyasal tesisin işletilmesi.

Beklenen İşletme Olayları (Anticipated Operating Occurrences): Tesisin ömrü boyunca bir ya da daha fazla kez meydana gelmesi beklenen ve gerçekleştiğinde tesise veya güvenlik sistemlerine bir zarar vermesi veya kaza koşullarına yol açması mühendislik sistemleri ile tasarım aşamasında engellenen normal işletmeden sapmalar.

Kaza (Accident): Tasarım özelliklerine göre kabul edilebilir düzeyde tutulan normal işletme koşullarından sapma.

Ciddi Kaza (Severe Accident): Tasarım ötesi kazalardan önemli boyutlarda kimyasal veya radyolojik sonuçlara yol açan kazalar.

Kaza Koşulları (Accident Conditions): Beklenen işletme olaylarının ötesinde, tasarıma esas ve tasarım ötesi kazaları da kapsayan normal işletme koşullarından tüm sapmalar.

Tasarıma Esas Kazalar (Design Basis Accidents): Tesisin tasarımı sırasında güvenlik sistemlerinin sınırlarını belirleyen kazalar.

Kaza Yönetimi (Accident Management): Tasarım ötesi kazaların gelişimleri sırasında kazanın ciddi kazaya dönüşmesini engellemek, ciddi kazaların sonuçlarını hafifletmek ve uzun dönem güvenli ve dengeli duruma dönebilmek için alınan önlemler.

Tasarım Ötesi Kazalar (Beyond Design Basis Accidents): Bir tasarıma esas kazadan daha ciddi kaza koşulları.

Olağan Dışı Olay: Normal işletmeden sapmalardan ciddi kazalara kadar bütün işletme olayları ve nükleer güvenliğe ilişkin yetersizlikler.

Operatör (Operator): Prosesi işletmek üzere kurumdan yetki almış gerçek kişiler.

HAZOP, bir sürecin, sistemin veya prosesin hatalı yöntemlerini, bunların nedenlerini ve sonuçlarını belirleme açısından FMEA ile benzerlik gösterir. Ancak HAZOP'ta takım amaçlanan sonuçlardan ve koşullardan doğan istenmeyen sonuçları ve sapmaları dikkate alır ve bu sapmaları ortaya çıkaran olası nedenler ve hatalı yöntemler için kontrol önlemleri önermek üzere çalışma yapar. FMEA'da ise hata modları üzerinde yoğunlaşılır ve bu hata modlarını ortaya çıkaran nedenleri önlemeye yönelik kontrol mekanizmaları üretmek üzere çalışma sürdürülür.

HAZOP tekniği başlangıçta kimyasal proses sistemlerinin değerlendirilmesi için kullanılmıştır, daha sonraları ise diğer tür sistemler ve karmaşık işlemlere kadar kullanımı genişletilmiştir. Bunlar mekanik ve elektronik sistemler, prosedürler ve yazılım sistemleri, hatta organizasyonel değişiklikler ve yasal sözleşme tasarımı ile incelemesini kapsamaktadır.

HAZOP metodolojisi tasarımda, bileşen(ler)de, planlı prosedürlerde ve insan eylemlerinde bulunan eksikliklerden dolayı tasarım planından kaynaklanan her türlü sapma formları ile başa çıkabilir. Yazılım tasarımı incelemesi için yaygın olarak kullanılmaktadır. Kritik sistem güvenliği ile kontrolüne ve bilgisayar sistemlerine uygulandığında, Kontrol Tehlikeleri ve İşlerliği Analizi

(Control HAzards and OPerability Analysis or Computer HAzard and OPerability Analysis - CHAZOP) olarak adlandırılır.

Bir HAZOP çalışması, genellikle bir prosesin veya bir sistemin tasarım aşamasında proses ya da akış diyagramının mevcut olduğu aşamada yapılır, ancak tasarım değişiklikleri hala uygulanabilir ise bu mümkündür. Bununla birlikte, bir tasarım ayrıntılı olarak geliştikçe, her bir aşama için farklı kılavuz kelimeleri ile aşamalı bir yaklaşım olarak HAZOP gerçekleştirilir. Bir HAZOP çalışması aynı zamanda prosesin işletilmesi sırasında da yapılabilir, ancak gerekli değişiklikler bu aşamada pahalıya mal olabilecektir.

Girdi:

Bir HAZOP çalışması için gerekli olan girdiler, sistem ile ilgili mevcut bilgiyi, incelenecek prosedür veya işlemi ve tasarım planı ile performans özelliklerini içermektedir. Girdiler aynı zamanda çizimleri, P&ID sayfalarını, akış diyagramı çizimlerini, işletim kontrolü bilgilerini, mantık diyagramlarını, plan çizimlerini, işletme bakım prosedürlerini ve acil müdahale prosedürlerini vb. kapsamaktadır.

Süreç:

HAZOP, bir prosesin veya sistemin "tasarım" ve "işletim şartları" veya çalışılan sistem özelliklerini ele alır. Oluşması amaçlanan performanstan doğan sapmaları ve potansiyel sapmaların neler olabileceğini ve ayrıca bir sapmanın muhtemel sonuçlarının neler olabileceğini keşfetmeye yönelik prosesin ya da sistemin her parçasını gözden geçirir. Bu çalışma, uygun kılavuz kelimeleri kullanılarak sistemin, işlemin veya sürecin her bir parçasının anahtar parametrelerdeki değişikliklere nasıl cevap vereceğini sistematik bir şekilde inceleyerek elde edilir. Kılavuz kelimeler özel bir sistem, işlem veya süreç için özelleştirilebilir ya da her türlü sapmayı kapsayan genel kelimeler kullanılabilir.

Bazı hallerde, "Beyin fırtınası- What if?" metodundan çok daha formal bir metoddur. Anahtar kelimeler, dizayn parametreleri ve tablolar kullanılır. Proses denetimine yardımcı olmak maksadıyla, tehlikeli sapmaları normal değerlerle karşılaştırmak maksadıyla anahtar kelimeler kullanılır, bu grup "Fazla ", "Az", "Hiç" vb. gibi kelimeleri içerir. Bu anahtar kelimeler basınç, sıcaklık, akış vb. gibi parametrelerin (kılavuz kelimeler) durumlarını nitelemek için kullanılır. "Çok erken", "çok az", "çok uzun", "çok kısa", "yanlış yönde", "yanlış nesne" ve "yanlış eylem" gibi benzer kelimeler insan hata modlarını tanımlamak için kullanılır.

Bir HAZOP çalışmasındaki normal adımlar şu şekildedir:

- HAZOP çalışma ekibi oluşturulur,

- Amaçların tanımı ve çalışmanın kapsam yapılır,
- Gerekli belgelerin toplanması yapılır,
- Çalışma için bir dizi anahtar veya kılavuz kelimeler oluşturulur,
- HAZOP çalışmasında ortaya çıkan her türlü sapma için kontrol eylemleri önerilir,
- Ortaya çıkan kontrol önlemlerinin hayata geçirilmesi ve planlama yapılabilmesi için aksiyon planları oluşturulur,
- Kontrol faaliyetlerini gerçekleştirecek gerekli sorumluluk ve yetkiye sahip kişiler belirlenir,

Çalışma ekibinin çalışmasını kolaylaştırmak maksadı ile aşağıda verilen uygulamaların yapılması önerilmektedir;

- İncelemeyi daha somut hale getirmek için sistemi, işlemi veya prosesi daha küçük öğelere, alt sistemler içerisine, alt süreçlere veya alt öğelere bölmek;
- Bir kimya prosesini mümkün olduğu kadar node'lara (fiziksel ve kimyasal özellikleri aynı olan parçacıklar) bölmek,
- Her bir alt sistem, alt süreç veya alt öğe için ve daha sonra istenmeyen sonuçlara neden olacak olası sapmaları öne sürmek için kılavuz kelimelerini birbiri ardına uygulayarak bu alt sistem veya öğede bulunan her bir madde için amaçlanan tasarıma karar vermek,

İstenmeyen bir sonucun belirlendiği her koşulda neden ve sonuçları kabul etmek, bunların oluşmasının nasıl önlenebileceği konusunda karar kılmak ya da mümkünse sonuçları hafifletmek için belirli eylemleri kabul etmek.

HAZOP Ekibi:

Analiz çok disiplinli bir takım tarafından gerçekleştirilmelidir ve bir takım lideri tarafından yönetilmelidir. HAZOP ekibi genellikle çoklu disiplinli bir ekiptir ve amaçlanan veya mevcut tasarımdan doğan sapmaların etkilerini değerlendirmek için uygun teknik uzmanlığa sahip operasyon personelini ve tasarım personelini içermelidir. Ekibin inceleme altındaki tasarım, işlem veya sürece doğrudan dahil olmayan kişilere de sahip olması önerilmektedir. Herbir durumda analistler, sebebler, sonuçlar, belirleme metodları ve düzeltici hareketler (yatıştırma ölçüsü) ile tanımlama yapar. HAZOP takımı aşağıda belirtilen çalışma gurubundan oluşur.

HAZOP Takımı:

➢ Fabrikanın işveren vekili

➢ Fabrika müdürü

➢ İş sağlığı ve güvenliği mühendisi

➢ İşletme (proses) mühendisi

➢ Sistem ve otomasyon mühendisi

➢ Elektrik mühendisi

➢ İnşaat Mühendisi (gerekli ise)

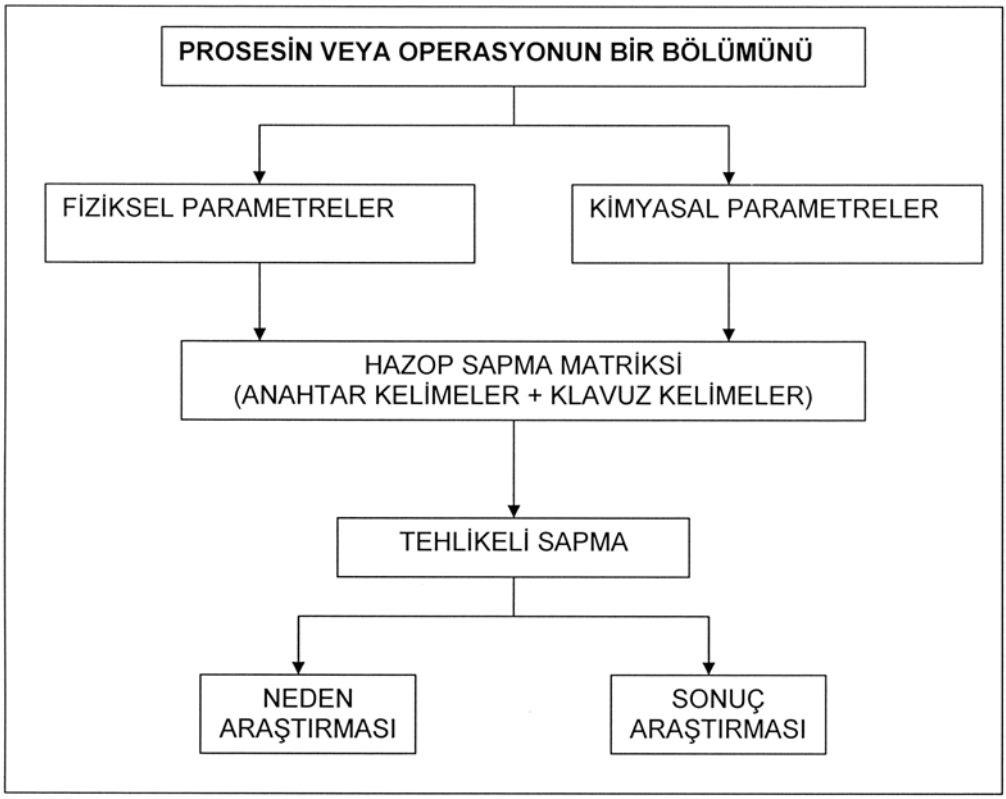
HAZOP Takımı, öncelikle prosesin veya operasyon adımının bir değişkenini seçer, anahtar kelimeleri kullanarak anlamlı tehlikeli sapmayı belirler. Tanımlanan sapma için neden araştırması ve paralel olarak sonuç araştırması yapılır.

HAZOP metodolojisi uygulamasında kullanılan klavuz kelimeler şunlardır;

KLAVUZ KELİMELER	ANLAMI
FAZLA (MORE)	Kantitatif çoğalma
AZ (LESS)	Kantitatif azalma
HİÇ (NONE)	Mevcut Değil, Amaçlanan sonucun hiçbir bölümü elde edilemez
Ters (Reverce)	Öngörülen yönün aksine
PARÇASI (PART OF)	Sistemin bir bölümü olması gerekenden farklı
...Kadar İyi (As Well As)	Aynı derecede
...DAN BAŞKA (OTHER THAN)	Tamamen farklı
ERKEN (EARLY)	Öngörülen süreden önce
GEÇ (LATE)	Öngörülen süreden sonra

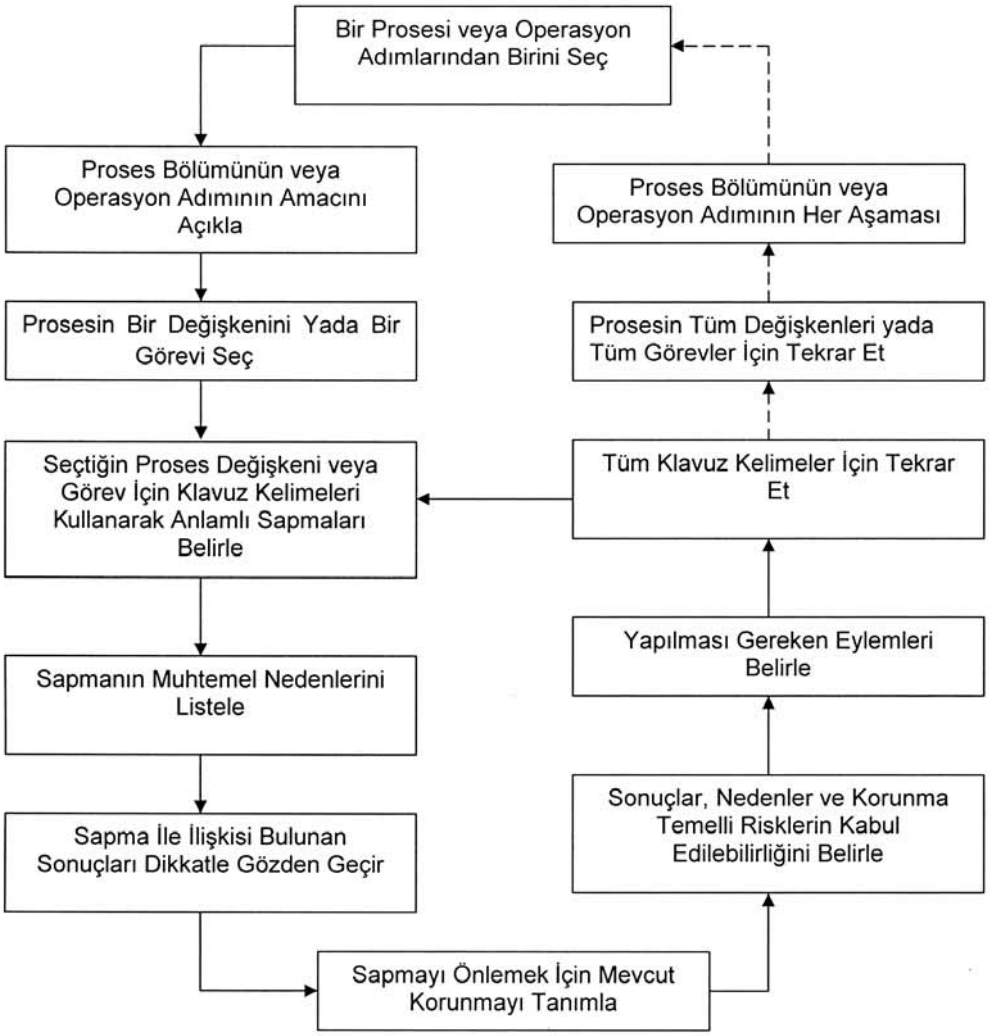
Anahtar Parametreler ise; insan faktörü, korozyon, buhar basıncı, PH, ısı kapasitesi, karışım, parlama noktası, viskozite, başlatma/kapatma, statik elektrik vb.'dir.

Tablo 28: HAZOP Uygulama Şeması



HAZOP takımının örnek bir tehlike ve işletilebilme çalışması **Tablo 29** ve **Tablo 30**'da verilmiştir. Tehlikenin saptanması proses içinde çalışanlardan yada HAZOP takım üyelerinden gelebilir. Seçilen sistem, hat, donanım veya techizatın öncelikle tehlikeli sapması tanımlanır, ölçümleme yapılır ve en son olarak da eylem belirlenir.

Şekil 28: HAZOP Takımının İzleyeceği Aşamalar



Sonuçlar:

Kaydedilen her inceleme noktası için HAZOP toplantısı/toplantıları tutanakları oluşturulur. Oluşturulan raporlarda kullanılan kılavuz kelimeler, sapma(lar), olası nedenler, belirlenen sorunlara yönelik eylemler ve eylemden sorumlu kişiler ayrıntılı olarak yazılır.

Güçlü Yönler ve Sınırlılıklar:

Bir HAZOP analizi, aşağıdaki avantajları sunmaktadır:

- Bir sistemi, prosesi, işlemi veya süreci sistematik olarak ve ayrıntılarıyla incelemek için çeşitli araçlar sağlar,
- Gerçek hayatın işletimsel deneyimine sahip ve müdahale eylemlerini yürütmekle görevli çoklu disiplinli bir ekip tarafından gerçekleştirilir,
- Çözüm ve risk müdahale eylemleri oluşturmak açısından çok etkili bir teknik içerir,
- Geniş bir sistem, proses, işlem ve prosedür yelpazesi için uygulanabilir,
- İnsan hatalarının neden ve sonuçlarının değerlendirilmesini yapabilir,
- İşletim anında gereken özeni göstermek maksadı ile kullanılabilen yazılı bir işletim kaydı oluşturulmasını sağlar.

Sınırlılıklar:

- Detaylı bir analizdir, çok fazla zaman gerektirir,
- Detaylı bir analiz olması sebebi ile belgelendirme veya sistem/işlem ve prosedür şartnamesinin yüksek düzeyde olmasını gerektirir,
- Temel problemler ile mücadele etmek yerine detaylı çözümler bulmaya odaklandığından detaylar arasında boğulabilir, (ancak bu, aşamalı bir yaklaşım ile azaltılabilir),
- Süreç, büyük ölçüde tasarımlarındaki problemleri çözmeye yönelik yeterince objektif olmakta zorlanabilen tasarımcıların uzmanlığına dayanır. Tecrübeli bir ekip ile yapılmıyor ise; bir (taslak) tasarımı, tasarım amacı, kapsamı ve ekibe verilen hedefler doğrultusunda sınırlı kalabilir.

HAZOP metodolojisi genellikle teknolojik kazalar ile uğraşan veya acil durum planı geliştirmek isteyen şirketler tarafından kullanılır. Basit teknolojik proseslerde çevresel risk değerlendirilmesinde de kullanılır. Bu metod, teknik sekreteryanın yardımına güvenildiği ve tecrübeli bir liderin yön vermesi durumunda uzman çalışma grubunun katı çoklu-disiplinli çalışması sonucunda uygulanabilir ve işlem akışı hakkında çok detaylı bilgi edinilmesini sağlar. HAZOP yaklaşımı, disiplinli, esnek ve sistematikdir.

Tablo 29: Örnek Bir Tehlike ve İşletilebilme Çalışması Formu(HAZOP):

PROSES/SİSTEM: Fırın	**REVİZYON TARİHİ:**
EYLEM NO:4	**TOPLANTI GÜNÜ:** 11.02.2013
İSTEKTE BULUNAN: Bakım Amiri **BAŞLIK:** HAZOP Değerlendirmesi	**DOKÜMAN REFERANS:**
İSTEK: Fırın alt sistemlerinin proses tehlike analizinin yapılması	
NEDEN: Havalandırma sisteminin tehlikeli sapmaları tespit edilmemiştir.	
SONUÇ: Havalandırma sistemindeki olası arıza sonucunda muhtemel patlama	
KORUNMA/AÇIKLAMA: Gaz dedektörü mevcuttur.	
ETKİ: Fırının durması, yangın, patlama vb.	
CEVAP VEREN : İş Güvenliği Uzmanı – HAZOP Takım Üyesi **YANIT:** Fırın alt sistemlerinin HAZOP analizi önemle gündeme alınmıştır. **TARİH:** 14.02.2013 **İMZA:**	

Tablo 30: Örnek HAZOP Metodolojisi –Proses Tehlike Analizi

Tarih :	01.12.2003	**TEHLİKE VE İŞLETİLEBİLME ÇALIŞMASI (HAZOP)**						HAZOP No:	3
Proses/Sistem :	Fırın							Düzenleyen:	İSG Mühendisi
Alt Sistem :	Havalandırma Sistemi							HAZOP Tarihi:	01.12.2003
Dizayn Rehberi:								Revizyon Tarihi:	
HAZOP Takımı:	İşveren Vekili, Fabrika Müdürü, İş Sağlığı ve Güvenliği Müh., Bakım Amiri, İşletme Müh., Elektrik Müh							Sayfa:	1
Anahtar Kelime	**Kılavuz Kelime**	**Tehlikeli Sapma**	**Olası Nedenler**	**Sonuç**	**Mevcut Güvenlik Önlemi**	**Olasılık**	**Şiddet**	**RÖS**	**Alınması Gerekli Aksiyonlar**
HİÇ	AKIŞ	Akış Yok	1.Enerji yok, jeneratör arızası 2. Fan arızalı çalışmıyor 3.Valfler hava filtresinin tıkalı olmasından bloke-kapalı	a)Fırında patlama meydana gelir b)Filtrasyon sistemi zarar görür	Aylık bakım esnasında kompresör durdurularak hava filtresi değiştirilmektedir				a)Fırına Acil Durum Kapatma Sistemi (ESD) kurulması b) İkincil fan ile bypass hattı kurulması c)Yedek jeneratör alınması

11.13. Tehlike Sınıflandırma ve Derecelendirme

A.B.D.'de Kimyasal Proses Güvenliği Merkezi (Center for Chemical Process Safety –CCPS,1993) kimya tesisleri için bir rehber yayınlamış ve bu rehberin temel bölümünü otomasyon ve kontrol boyutları oluşturmuştur. Otomatik durdurma ve kilit sistemleri için tasarım felsefesi on ayrı noktada ele alınmıştır.

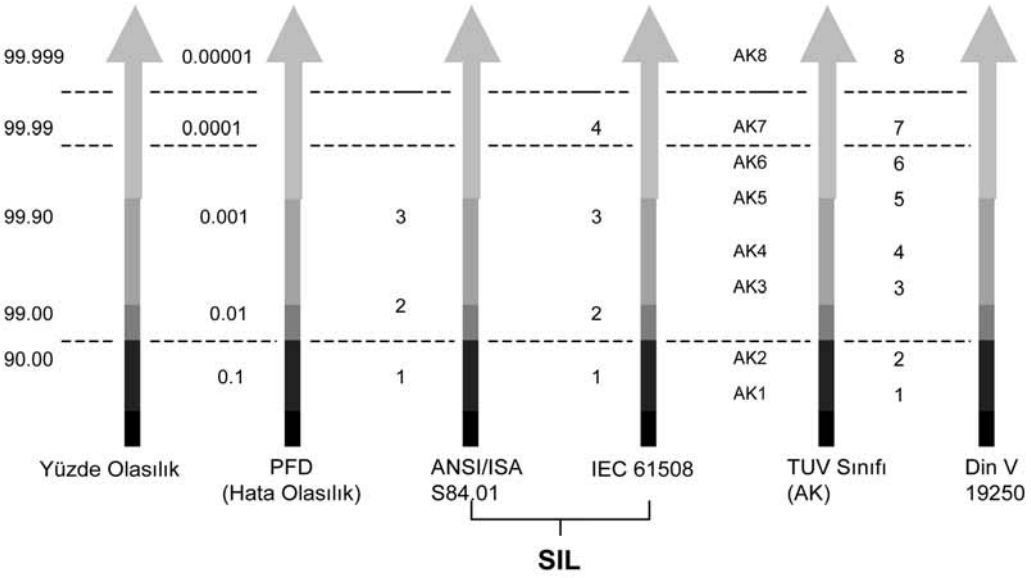
Uluslararası Elektroteknik Komisyonu tarafından hazırlanan "Fonksiyonel güvenlik: güvenlikle ilgili sistemler" (IEC 61508) isminde bir standart yayınlamıştır. Bu standart, güvenlik fonksiyonlarının elektronik sistemlerle yürütülmesi gerektiğinde başvurulabilecek ilgili boyutları kapsamaktadır. Proses, imalat, ulaştırma ve tıp sektöründen örnekler verilmiştir. Standart genelde proseslerin güvenliği ile ilgilenmiştir. Satndartta yer verilen bazı terimler:

- Güvenlikle ilgili sistem kontrol altındaki ekipmanın güvenli durumda olması için gerekli güvenlik fonksiyonlarının uygulanmasını sağlamaktadır. (Bir proseste güvenlikle ilgili sistemin parçası olabilir),
- Fonksiyonel güvenlik güvenlikle ilgili sistemin kontrol altındaki ekipmanın güvenli durumda olması için gerekli faaliyetleri yapmasıdır,
- Entegre güvenlik güvenlikle ilgili sistemin belirlenen durumda ve belirlenen zaman periyodunda gerekli güvenlik fonksiyonlarını tatminkar şekilde yerine getirebilme ihtimalidir.

Eğer firma, fabrika veya işletme bir büyüme ve genişleme planlıyorsa veya daha basit olarak bir prosesi değiştirmeyi planlıyorsa ve birincil tehlike değerlendirmesi (PHA) sizin bir koruma seviyesi olarak güvenlik ölçümleme sistemini kullanmanızı gösteriyorsa, ANSI/ISA S8.4.01, IEC 61508, TUV sınıfı vb. standartlardan birine göre "Güvenlik Ölçümlemesi" gerekir.

Neden? Çünkü bir işletme yada fabrika içerisindeki tüm bölgelerin tehlike dereceleri aynı olmayabilir, tüm fabrika veya işletmede çok özellikli tedbirleri alınması gerekmezken, fabrika veya işletmenin yanlızca bir bölümü için çok özellikli ekipmanların ve korunma tedbirlerinin alınması gerekebilir. Ayrıca güvenlik sınıflandırması yada kullanılan kimyasallara göre sınıflandırma yapılması işyerinde alınacak tedbirlerin çok daha rahat alınmasını sağlar ve bu bölümdeki risk değerlendirmesinin daha sık aralıklarla ölçümlenmesini ve değerlendirilmesini sağlar. Birçok ülkede "Proses Endüstrileri İçin Güvenlik Ölçümleme Sisteminin Uygulanması" kabul edilmiştir ve OSHA 29 CFR Bölüm 1910 tarafından da kullanılması zorunlu olmuştur.

Şekil 29: Güvenlik Ölçümleme Standartları Karşılaştırması



Hem OSHA hem de EPA milli standartlarında (örneğin ANSI- Amerikan Milli Standartlar Enstitüsü) güvenlik ölçümleme sistemine atıfta bulunulur. **Tablo 31**'de güvenlik ölçümleme sistemlerinin karşılaştırılması verilmiştir. Aşağıda üç değişik sınıflandırma standartı ANSI/ISA S84.01, IEC 61508 ve NFPA Tehlike Derecelendirme Endeksi incelenmiştir.

Tablo 31: SIL ile Prosesin Mevcudiyet Gerekliliği, PFD ve 1/PFD Arasındaki Bağlantı

Sistem Güvenlik Derecesi		Mevcudiyet Gerekliliği	PFD	1/PFD
IEC 61508	4	>99.99%	E-005 - E-004	100,000 - 10,000
ISA S84	3	99.90-99.99%	E-004 - E-003	10,000 - 1,000
	2	99.00 - 99.90%	E-003 - E-002	1,000 - 100
	1	90.00 - 99.00%	E-002 - E-001	100 - 10

11.13.1.Güvenlik Ölçümleme Sistemi (SIS) – Güvenlik Bütünlük Derecesi (SIL)

ISA ANSI tarafından akredite edilmiş bir organizasyondur.

Her hangi bir proseste, Proses Tehlike Analizi (PHA), prosesin mekanik bütünlüğü ve proses kontrol tehlike potansiyelini azaltmak için yeterli olmadığını gösteriyorsa Güvenlik Ölçümleme Sistemine (SIS) Güvenlik Bütünlük Derecesi (SIL) atanması gerekmektedir.

Prosesin tehlikeli olduğu anlaşıldığında, SIS tehlikeyi azaltmak veya prosesi güvenli duruma getirmek için gerekli olan ekipmanı ve kontrol mekanizmalarını içerir

Güvenlik Bütünlük Derecesi (SIL) ne demektir? Güvenlik Bütünlük Derecesi (SIL) ve olasılık, Güvenlik Ölçümleme Sisteminin (SIS) bütünlüğünün istatistiksel olarak ifade edilmesinde kullanılan iki parametredir.

Örneğin SIL değeri 1 olan SIS'de ekonomik risk oldukça düşüktür ve %10 hata riski (ya da %90 ayakta kalma) içeren SIS kabul edilebilir bir değerdir. Ancak; örneğin bir sıvı tankının yüksek seviyeli taşınmasında söz konusu olan SIL 1 SIS'i ele alalım. %90 ayakta kalma demek, yüksek seviyeye ulaşılan her 10 defada bir adet tahmin edilen bir hata bulunmasıdır. Sıvı tankının yüksek seviyeli taşınmasında , bu kabul edilebilir bir risk midir?

Geçtiğimiz bir kaç yıl içerisinde SIL'e niteliksel bakış açısı yavaş yavaş gelişmiş ve SIL konsepti birçok kimsayal ve petrokimyasal fabrikada uygulanmıştır. Niteliksel bakış, SIS hatasının fabrika personeli, halk ve toplum üzerindeki etkisine bağlıdır.

Bu niteliksel bakış bir tartışma yaratabilir. Minor nedir? Major nedir? Hangi noktada, teorik olarak zarar veya kaza sonucu ölüm meydana gelir. Belirli bir işletme, fabrika ünitesi veya kimyasal prosese tehlikeler için spesifik SIL tavsiye etmek maksadıyla kullanılan kesin kurallar içeren bir standart yoktur. SIL'in tayin edilmesi kollektiftir veya şirketin risk yönetim temelli kararıdır ve risk tolerans felsefesidir. SIL'in tayin edilmesi için mühendislik pratiği ve risk değerlendirme takımının tecrübesi gerekir.

Seçilen proses veya ünite için SIL seçiminin doğrulanması ve sabitliğin garanti edilmesi PHA'da dökümantasyonu azaltarak zaman kazandırır.

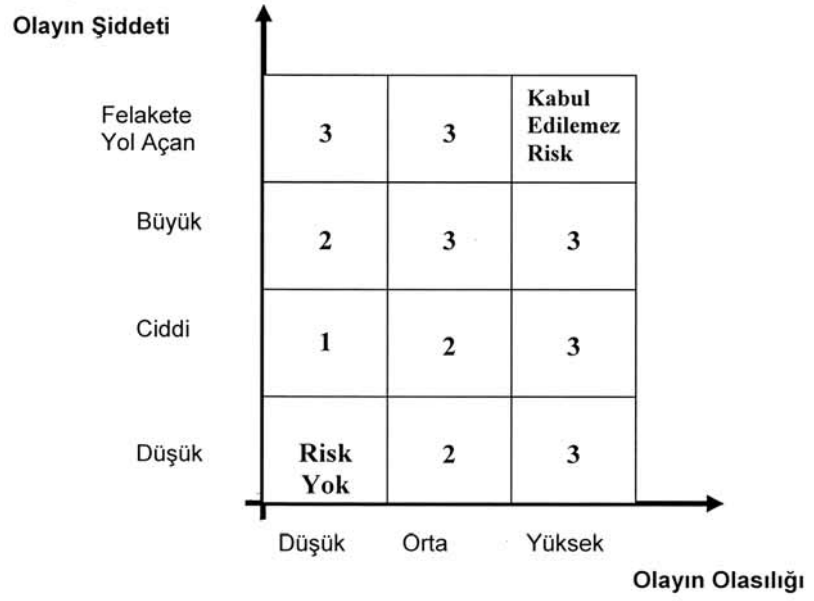
11.13.2. Risk Grafiği ile SIL; (IEC 61508)

Ancak IEC 61508 metodolojisi daha çok HAZOP uygulanan proseslerin Güvenlik Bütünlük Derecesinin (SIL) tespiti için kullanılır. SIL, maruz kalma zamanı, olayın oluşumundan kaçış ve olasılığı açısından analistin görüş açısından değerlendirilmesidir. Sonuç, içeriğin kaybı, yangın, kimyasal, zarar veya ölüm açısından ve PHA'da prosesin değerlendirilmesinde kullanılır. Sonuç için aşağıdaki sorular olay için değerlendirilir;

Tablo 32: Sonuç Metedolojisine göre SIL;

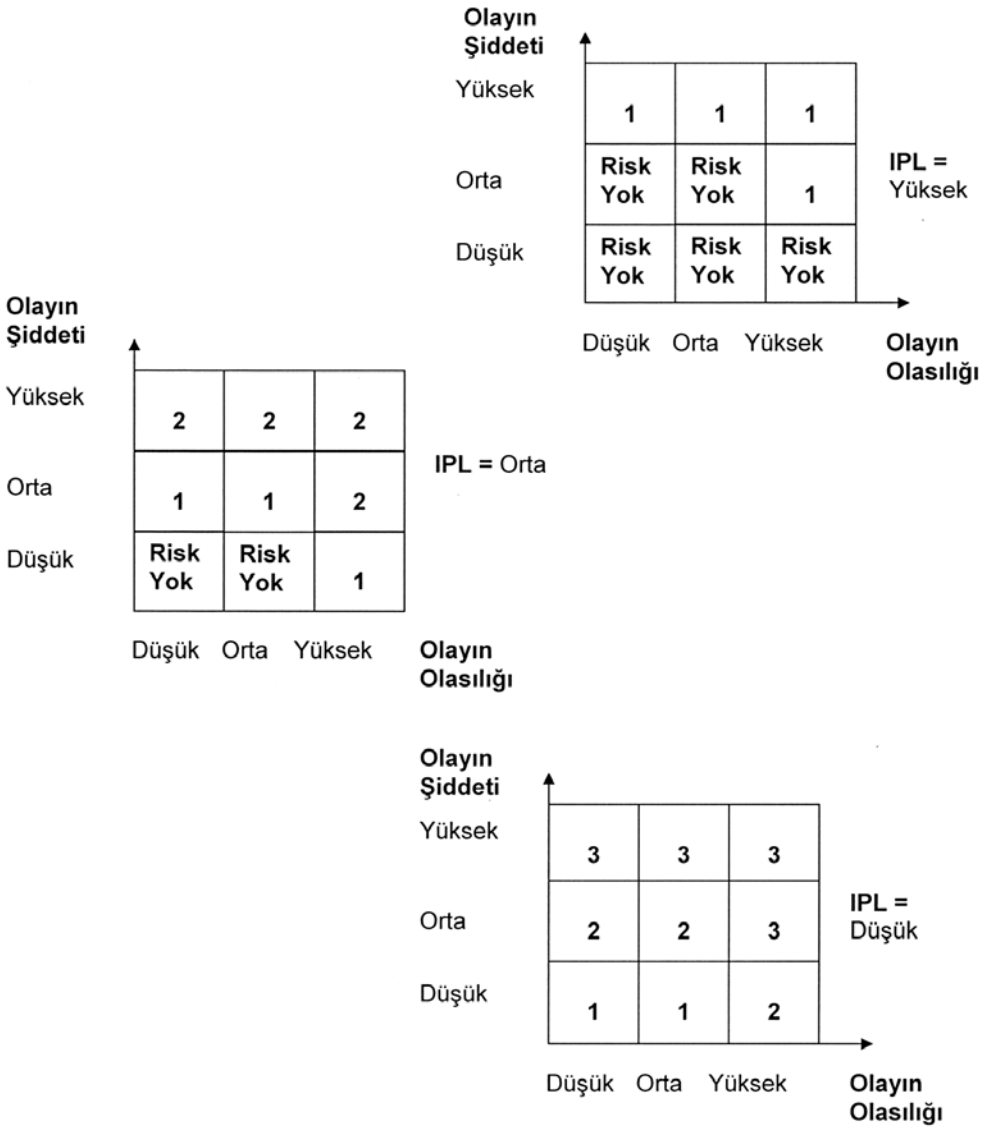
DERECE	SIL
4	Toplum üzerinde felakete yol açan etki
3	İşçiler ve toplumun korunması gerekir
2	Major özellik ve üretimin korunması gerekir. İşçiler için muhtemel zarar
1	Minor özellik ve üretimin korunması gerekir.

Risk Matris ile SIL; (ANSI/ISA S84.01 ve IEC 1508/IEC/1511(Draft))
a) İki boyutlu SIL Matrisi;



b) Üç boyutlu risk matrisi;

Üç boyutlu matris de işçilerin bağımsız korunma derecesine (***Independent Protection Layers –IPL***) göre olayın şiddeti ve olasılığına bağlı SIL değeri belirlenir. İşçilerin korunma derecesine göre SIL değerinde indirim yapılır.



Burada potansiyel zarar veya ölüm olabilir mi?

➢ Maruz kalan kişi kurtarılabilir mi / iyileşebilir mi?

➢ Maruz kalan kişi normal faaliyetlerine geri dönebilir mi?

➢ Etkiler akut veya kronik midir?

Maruz kalma frekansı için proses ünitesinde personel bulunması ve bu personelin faaliyetleri göz önüne alınarak değerlendirilir. Maruziyet sıklığı ve süresi için aşağıdaki sorular olay için değerlendirilir;

➢ Proses ünitesi uzakta mı veya esas personelin yoğunluğunun bulunduğu alanda mı?

➢ Operasyon veya bakım istasyonu nasıl kapatılabilir/durdurulabilir?

➢ Yakınında ne sıklıkta personel çalışıyor?

➢ Mühendis personel veya bakım onarım işçilerinden ne kadar destek alabiliyor?

➢ Diğer proses ünitelerine erişim için esas ulaşım alanı mıdır?

Tehlike değerlendirme takımı için kaçışın olasılığı üzerinde anlaşma sağlanması zor olabilir, çünkü mühendislik ve risk değerlendirmesini yapan kişiler, orada eğer alarm mevcutsa kişilerin herzaman kaçabileceğine inanmak isterler. Ancak zaman kaçışda önemli bir faktördür. Şu soruların mutlaka sorulması gerekir;

➢ Tehlikeli alandan nasıl kolay kaçılır?

➢ Kaçış için işaretlemeler iyi yönlendiriyor mu?

➢ Olayın oluşu, alarm ve kaçış arasındaki mevcut zamanlama nedir?

➢ Maruziyet alanı içindeki personel tehlike çıkış yerini kolaylıkla fark edebilir mi?

➢ Alarm sireni var mı?

➢ Personele kaza senaryo eğitimi verildi mi?

Olasılık ve meydana gelme; birçok HAZOP ve bir çok "Proses Tehlike Analizi" için kullanılan ve değerlendirilmesi kolay olan parametrelerdir. Mevcut tüm Güvenlik Bütünlük Sistemleri içinde olayın olasılığı hesaba katılarak değerlendirilir. Bu faktörlere karar verildiğinde IEC 61508-Risk Grafiği, minimum

risk indirgeme düzeyi ve kurumsallaşmış SIL'e karar vermek için kullanılır.

Küçük kimyasal fabrikalar tarafından benimsenen risk matris metodolojisi veya IEC 61508 en az zaman tüketen metoddur. PHA prosesi içinde, SIL seçimin doğrulanması ve proses ünitesinin bir ucundan diğer ucuna sabitliğin garanti edilmesi analizde zaman kazandırır.

Tablo 33: Risk Grafiği İşaretlemeleri

İŞARET	ANLAMI
C	Sonuç
F	Sıklık ve maruziyet süresi
P	Tehlikeli olayın gerçekleşme imkanı
W	İstenmeyen olayın olasılığı

Tablo 34: Minimum Risk İndirme Derecesine Göre Güvenlik Bütünlük Derecesi

Gerekli Minimum Risk İndirme Derecesi	Güvenlik Bütünlük Derecesi
-	Güvenlik ihtiyacı yok
a	Özel güvenlik ihtiyacı yok
b,c	1
d	2
e,f	3
g	4
h	Güvenlik yetersiz (5)

Tablo 35: Hasar Endeksi-Şiddet Tablosu

İŞARET	ÇEVRE VEYA EKİPMAN HASAR MİKTARI (%)	İNSAN AÇISINDAN ZARAR
C1	1- 10	Hafif ve kalıcı olmayan yaralanma, sıyrıklar, sisteme zararı yok, proseste ekipman kaybı yok, geçici çevre kirliliği.
C2	10- 25	Bir veya daha fazla kişi için ciddi kalıcı zarar, proseste duraklamayı gerektirebilecek kayıp, çevrede geçici ve kalıcı kirlilik oluşması.
C3	25- 60	Birkaç kişinin ölümü, proseste uzun süreli duraklamayı gerektirebilecek kayıp, çevrede geçici ve kalıcı kirlilik oluşması.
C4	60 - 100	Birçok kişinin ölümü, tesisin tümünün birden harap olmasına neden olabilecek ve çevrenin geri dönülemeyecek derecede kirlenmesine sebeb olabilecek hasar.

Tablo 36: İstenmeyen Olayın Olasılık Tablosu

İŞARET	ANLAMI	GÜVENİLİRLİK (%)
W3	Küçük Olasılık	97,8 – 99,9
W2	Orta Olasılık	93,6 – 97,8
W1	Yüksek Olasılık	79,4 – 93,6

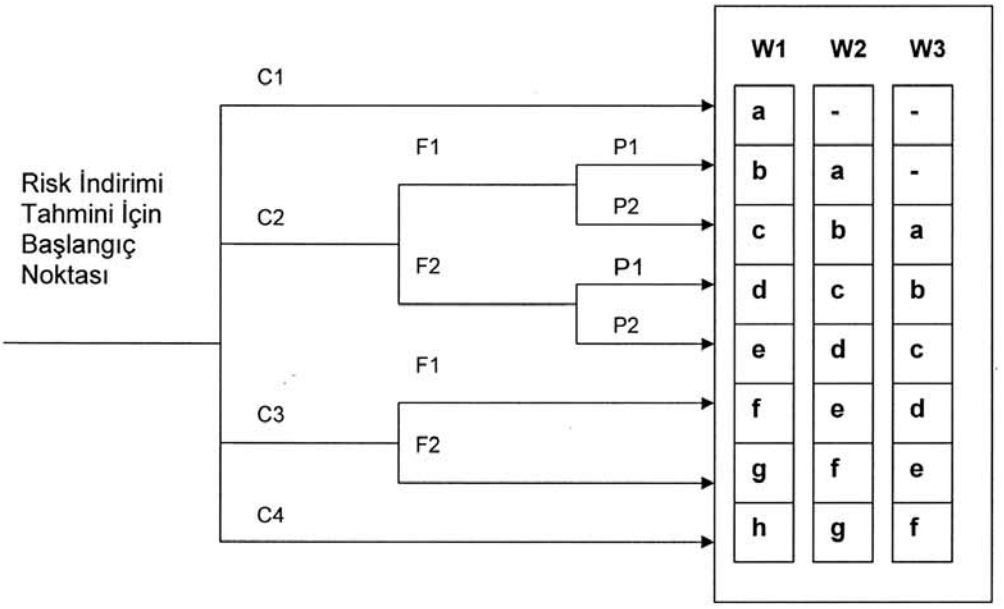
Tablo 37: Sıklık ve Maruziyet Süresi

İŞARET	ANLAMI
F1	Nadiren veya kısa sürelerle
F2	Sık sık sürekli veya uzun süreli

Tablo 38: Tehlikeli Olayın Gerçekleşme İmkanı

İŞARET	ANLAMI
P1	Belli durumlarda mümkün
P2	Fiilen mümkün değil

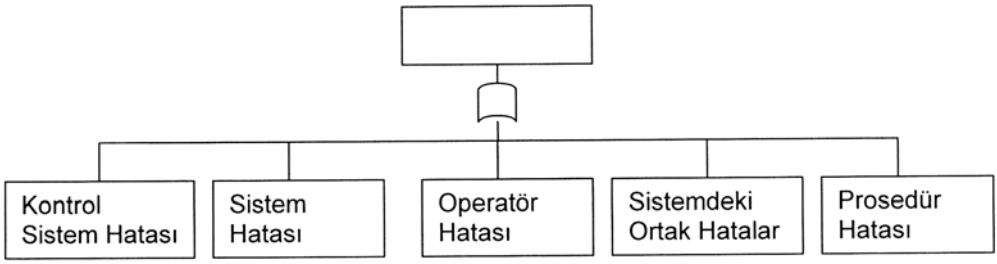
Şekil 30: Risk Grafiği



11.13.3. Kantitatif Analiz

Risk Graf tekniği, SIL'i kantitatif yaklaşımla tayin etmek için çok dikkatli bir tekniktir. SIL, prosesin işlem talebleri veya olay olasılığının kantitatif olarak belirlenmesi ile tayin edilir. Olayın potansiyel sebebleri, bir kantitatif risk değerlendirme metodolojisi kullanılarak **Şekil 31**'de gösterildiği gibi belirlenir. Kantitatif teknik, olasılığın kalitatif olarak belirlenmesinin çok güç olduğu, prosesin geçmişi hakkında çok sınırlı bilginin bulunmadığı durumda sık sık kullanılır. Metod, esas olayın potansiyel sebeblerinin ve herbir potansiyel sebebin olasılığının belirlenmesini gerektirir.

Şekil 31: Proses Taleplerinin Kantitatif Analizi



SIL'in belirlenmesinde, kabul edilebilir risk frekansının, proses talebine bölünmesi ile "İstenen Hata Olasılığı (Probability to Fail on Demand – PFD) " hesaplanır.

$$\textbf{PFD} = \frac{\text{Kabul Edilebilir Frekans}}{\text{Proses İsteği}}$$

Denklemin tersinden ise "Risk İndirme Faktörü- (Risk Reduction Factor-RRF)" hesaplanır.

$$\textbf{RRF} = \frac{\text{Proses İsteği}}{\text{Kabul Edilebilir Frekans}}$$

Son teknik, en az zaman gerektiren metoddur ve SIL metodolojisi için çok fazla insan gücü gerektirmediğinden bir çok küçük kimyasal fabrika tarafından benimsenmiştir.

11.13.4. Kollektif Zorunlu Seçim

Son teknik, SIL atama yöntemlerine yüksek miktarlarda insan gücü ayırmak istemeyen bir çok küçük, özellikli kimyasal fabrikalar tarafından adapte edilmiş bulunan "en az zaman alan" yöntemdir. Bu metod ile, SIL'in SIL 1'den büyük seçilmesi kararı verildiğinde maliyetlerde büyük artış olduğunun farkına varılır. SIL 2 veya SIL 3'ün seçilmesi, SIS tasarımını prosesteki cihazların yedeklemesi ve çeşitliliği yönünde zorlar.

Bu kabulden yola çıkıldığında, bir çok küçük firma " güvenlikli bir sistem, güvenli sistemdir" ve dolayısıyla SIL 3 olmalıdır görüşüne eğilim gösterirler. SIL'in 3 seçilmesi ile; kaçış mümkün olmayabilir, birileri yaralanabilir veya ölebilir veya etki ön kısımda yada arka kısmda olabilir gibi sorular dikkate alınmamış olur.

Bu yaklaşımlar, PHA prosesinde zaman kazanılmasını sağlar, SIL seçiminin gerekçelerinin belirtildiği dokümantasyonu azaltır ve proses üniteleri arasındaki tutarlılığı sağlar.

Tablo 39: Çökme Derecelendirmesi

BI SEVİYESİ	ÇÖKME SÜRESİ	ORTALAMA ARIZALAR ARASI SÜRE (gün)	AÇIKLAMA
1 – ÇOK AZ	0 – 1 Gün	0,5	Tesiste veya ekipmanda küçük çökme, tamir gerektirmez. Ancak temizlik gerekir.
2 - AZ	1- 10 Gün	5	Tesiste veya ekipmanda kayda değer çökme, fakat büyük tamir gerektirmez
3 - ORTA	10 – 30 Gün	20	Tesiste veya birçok ekipmanda kayda değer çökme ve tamir gerekli. Bir çok ekipmanın parçalarının değişmesi gerekebilir.

4 - AĞIR	30 – 90 Gün	60	Büyük çaplı çökme, ekipmanlarda tamir veya değiştirmek gerekebilir.
5 - BÜYÜK	90 – 270 Gün	180	Büyük çaplı ve tesiste yaygın çökme, ekipmanların birçoğunda kapsamlı tamir veya değiştirmek gerekebilir.
6 - TAMAMI	270 – 360 Gün	300	Tesisin tümüyle çökmesi, yaklaşık 1 yıl boyunca tamir, tadilat veya inşaat gerekebilir.

Tablo 40: Prosesin Çökme Seviyesi

	BI SEVİYESİ					
SIL	1	2	3	4	5	6
5	C	C	C	D	D	D
4	C	C	C	D	D	D
3	B	C	C	D	D	D
2	B	B	C	C	C	C
1	B	B	C	C	C	C
-	A	A	B	B	B	B

Tablo 41: Prosesin Kabul Edilebilirlik Seviyesi

RİSK SINIFI	DERECE	AKSİYON
A	Kabul Edilebilir Risk	Kabul edilebilir seviye, ayrıca bir önlem alınmasını gerektirmez. Mevcut önlemlerin izlenmesi gerekir.
B	Orta Riskli Olay	Riskleri önlemek üzere, tedbirlerin alınması zaman alabilir.
C	Orta – Yüksek Riskli Olay	Tespit edilen risklerin acilen düşürülmesi için tedbirler derhal yürürlüğe konmalıdır.
D	Yüksek Riskli Olay	Kabul Edilemez Bölge. Söz konusu proses durdurularak "Derhal" önlem alınmalıdır.

11.13.5. Kontrol Önlemleri Önerilmesi

Özellikle Risk Öncelik Sayısına göre ciddi sonuçlar doğurabilecek tehlikeli sapmalar için, kontrol önlemlerini bulmak HAZOP takım üyelerine düşmektedir, hiçbir HAZOP klavuzunda bu önlemler tanımlanmamıştır. Bu önlemleri bulmak takım üyelerinin proses kontrolü konusundaki tecrübelerine kalmaktadır.

11.13.6. Aynı Prosedürün Prosesin Diğer Ekipmanlarına Uygulanması

Prosesin veya operasyonun bir adımında seçilen bir değişken için uygulanan çalışma diğer değişkenler içinde uygulanmalı, bu adım tamamlanınca prosesin veya operasyonun diğer adımlarına geçilmelidir.

11.14. İş Etki Analizi (Business Impact Analysis -BIA)

İş Etki Değerlendirmesi olarak da bilinen İş Etki Analizi, anahtar iş kesinti risklerinin, bir kurumun faaliyetini nasıl etkileyebildiğini analiz eder, tanımlar ve onu yönetmek için gerekli olacak yeteneklerin ölçülerini belirler. BIA, özellikle aşağıdaki hususların kararlaştırıldığı şekilde anlaşılmasını sağlar:

- Anahtar iş süreçlerinin, fonksiyonların, ilgili kaynakların ve anahtar bağımlı iş adımlarının kritikliği ve tanımlanması,

- Aksatıcı olayların kritik iş hedeflerine ulaşma kapasitesini ve kabiliyetini nasıl etkileyeceği,
- Aksaklığı kontrol altına alma ve kararlaştırılan işletim düzeyinde organizasyonu iyileştirme bakımından gerekli olan kapasite ve yeterlilik.

BIA, hedeflerin devam eden başarısını sağlamak için ilgili kaynak ve süreçlerin zaman dilimlerini iyileştirmek ve kritiklik durumuna karar vermek için kullanılır. Buna ek olarak BIA, süreçler, iç ve dış taraflar ve herhangi bir tedarik zinciri bağlantıları arasındaki bağlılıkların ve karşılıklı ilişkilerin belirlenmesinde yardımcı olur.

Girdi:

Girdiler arasında şunlar bulunmaktadır:

- Bir plan veya proses geliştirmek üzere yapılan tüm çalışma belgeleri (proses akım şemaları, hammadde bilgileri, P&ID, vaziyet planları, elektrik devre şemaları, vb.),
- Kurumun hedefleri, çevresi, operasyonları ve sistemlerin birbirine bağlılıkları ile ilgili bilgiler,
- Diğer paydaşlar, dışardan sağlanan tedarik bilgileri,
- Organizasyonlar ile kaynakları, ilişkileri destekleyen süreçleri içeren organizasyonun operasyonları ve eylemlerindeki ayrıntılar,
- Kritik süreç kaybının finansal ve operasyonel sonuçları.

Süreç:

Bir BIA kritik sürecinin, bu işlemlerin ve gerekli kurtarma zaman dilimleri ve destekleyici kaynaklarının kaybının etkilerine yönelik bir anlayış elde etmek için sistemin veya prosesin dizaynında görev yapan uzmanlar, sistem çeki için kullanılan çeklistler, operatör görüşmeleri, bu üçünün kombinasyonları veya atölye çalışmaları kullanılarak yapılır.

Anahtar adımlar şunlardır:

- Süreçlerin kritikliliğine karar vermek için sistemin/prosesin çıktıları ve anahtar süreçlerin onaylanması ve hassasiyet değerlendirmesi,
- Belirlenen süre boyunca, finansal ve/veya operasyonel dönemlerde belirlenen kritik süreçlerde bozulma sonuçlarının belirlenmesi,
- Temel iç ve dış operasyonlar ile bağlılıklarının belirlenmesi. Bir tedarik zinciri boyunca bağlılıkların türü için haritalama,

- Geçerli mevcut kaynakların ve aksaklık sonrası minimum kabul edilebilir düzeyde faaliyetin sürdürülmesi için gereken temel kaynak düzeylerinin belirlenmesi,
- Şu anda kullanımda olan veya geliştirilmesi planlanan alternatif geçici çözümler ve süreçlerin belirlenmesi. Alternatif geçici çözümler ve süreçler, bozulma süresince kaynaklar veya yeteneklerin erişilemez veya yetersiz olduğu yerde geliştirilmeye ihtiyaç duyabilir.
- Tanımlanan sonuçlara ve fonksiyon bakımından kritik başarı faktörlerine bağlı her bir süreç için maksimum kabul edilebilir hizmet dışı kalma süresinin (Maximum Acceptable Outage time -MAO) belirlenmesi. MAO, yeterlilik kaybını tolere edebilen organizasyon zamanının azami süresini temsil eder.
- Herhangi bir özel ekipman veya bilgi teknolojisi için kurtarma zamanı (Recovery Time Objective- RTO) hedeflerinin belirlenmesi. RTO, özel ekipman veya bilgi teknolojisi kabiliyetini iyileştirmeyi amaçlayan organizasyon içerisindeki zamanı temsil eder.
- Bir aksaklık yönetimi için kritik süreçlere yönelik hazırlığın mevcut seviyesinin belirlenmesi. Bu süreç (örneğin, yedek ekipman) veya alternatif tedarikçilerin varlığı içerisindeki yeterlilik seviyesinin değerlendirmesini içerir.

Çıktılar:

Çıktılar aşağıdaki gibidir:

- Kritik süreçler ve ilgili bağlılıklarının bir öncelik listesi,
- Kritik süreçlerin bir bir kaybından doğan güvenlik kayıpları, doğabilecek felaketler, finansal ve operasyonel etkiler,
- Belirlenen kritik süreçlere ihtiyaç duyan destekleyici kaynaklar,
- Kritik süreç ve ilgili bilgi teknolojisi iyileştirme zaman dilimlerine yönelik kesinti zaman dilimleri.

Güçlü Yönler ve Sınırlılıklar:

BIA' nın güçlü yanları şunlardır:

- Organizasyona, belirlenen hedeflerine ulaşması için devam etme yeterliliği sunan kritik süreçlerin anlaşılması sağlar,

- Gerekli kaynakların belirlenmesini temin eder,
- Organizasyonun toparlanmasına yardımcı olması için işlemsel süreçlerin yeniden belirlenmesine yönelik fırsatıları tanımlar.

Sınırlılıklar ise şunları içerir:

- Dizayn aşamasını yürüten uzmanlardan gelen bilgi eksikliği, görüşme veya atölye inceleme çalışmalarını üstlenen katılımcıların bilgi eksikliği başarı sağlanmasını imkânsız hale getirebilir,
- Grup dinamikleri kritik bir sürecin tüm süreçlerinin analiz edilememesine neden olabilir,
- Toparlama gereksinimlerinin basit veya aşırı iyimser beklentiler nedeniyle gerçeğinden daha iyiymiş gibi belirlenmesi.

11.15. Kök Neden Analizi (Root Cause Analysis -RCA)

Bir hatanın gelecekte tekrarlanmasını önlemek için yapılan, genel olarak Kök Neden Analizi (Root Cause Analysis - RCA), Kök Neden Hata Analizi (Root Cause Failure Analysis - RCFA) veya temel kayıp analizi olarak adlandırılır. Kayıp analizi başlıca dış faktörler veya felaketler nedeniyle finansal ya da ekonomik kayıplar ile ilgiliyken; RCA, arızaların çeşitli türlerinden kaynaklanan ekipman kayıplarına odaklanır. Sadece acil belirgin semptomlar ile ilgilenmek yerine kök veya orijinal nedenlerini tanımlamaya çalışır. Düzeltici faaliyetin her zaman bütünüyle etkili olamayabileceğini ve sürekli gelişim sağlama gereksinimini öne sürer. RCA temel bir kaybın değerlendirmesi için sıklıkla uygulanır ve çoğunlukla, hangi alanlarda iyileştirme yapılabileceğine dair karar vermeye yönelik daha küresel bazda ki kayıpları analiz etmek için kullanılır.

RCA geniş kullanım alanını takiben farklı bağlamlarda uygulanır.

- Emniyet Tabanlı RCA iş sağlığı ve güvenlik ile kaza soruşturmaları için kullanılır.
- Arıza analizi, güvenilirlik ve bakım ile ilgili teknolojik sistemlerde kullanılır.
- Üretim bazlı RCA, sanayi üretimi için kalite kontrol alanında uygulanır;
- Süreç bazlı RCA, iş süreçlerine odaklanır.
- Sistem-bazlı RCA, değişim yönetimi, risk yönetimi ve sistem analizi uygulaması ile karmaşık sistemler ile ilgilenen önceki alanların bir birleşimi olarak gelişmektedir.

Girdi:

RCA için temel nitelik taşıyan bir girdi, arıza veya kayıptan elde edilen tüm delillerdir.

Süreç:

Bir RCA için ihtiyaç tespit edildiğinde, analizi gerçekleştirmek ve önerilerde bulunmak için bir uzman grup tayin edilir. Uzmanlık türü, çoğunlukla başarısızlığı analiz etmek için gerekli özel uzmanlığa bağlı olacaktır.

Analizi gerçekleştirmek için farklı yöntemler kullanılmasına rağmen, RCA' nın yürütülmesindeki temel adımlar birbirine benzerdir ve şunları içerir:

- Takımı oluşturma,
- RCA' nın kapsam ve hedeflerini oluşturma,
- Başarısızlığa ya da kayba ait veri ve delil toplama,
- Temel sebebi belirlemek için yapısal bir çözümleme gerçekleştirme,
- Çözümler geliştirme ve önerilerde bulunma,
- Önerileri yerine getirme,
- Yerine getirilen önerilerin başarısını doğrulama.

Yapısal analiz teknikleri aşağıdakilerden birini içerebilir:

- "5 neden'' tekniği, örn. nedeni ve alt nedeni ortaya çıkarmak için devamlı olarak 'neden?' sorusunu yöneltme;
- Arıza modu ve etki analizi,
- Hata ağacı analizi;
- Temel sebep haritalandırması.

Sebeplerin değerlendirilmesi genelde, önceden belli olan fiziksel sebeplerden başlayarak, insan kaynaklı sebeplere ve son olarak da temelde yatan yönetim veya temel nedenlere kadar devam eder. Düzeltici faaliyetin etkili ve faydalı olabilmesi için, rastlantısal faktörler, ilgili taraflarca kontrol edilebilmeli ya da ortadan kaldırılmalıdır.

Çıktılar:

RCA'dan gelen sonuçlar aşağıdakileri içermektedir:

- Toplanan veri ve delillerin belgelendirilmesi;

- Dikkate alınan hipotezler;
- Başarısızlığın ya da kaybın en muhtemel ana sebeplerine yönelik sonuç;
- Düzeltici faaliyete dair öneriler.

Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler ve sınırlılıklar aşağıdakileri içermektedir:

- Uygun uzmanların bir takım çalışması içerisinde bulunması gerekir,
- Yapısal çözümleme geliştirir,
- Tüm muhtemel hipotezleri göz önünde bulundurmayı sağlar,
- Nihai önerilerde bulunma gereksinimi ile ilgili sonuçların belgelendirilmesini etkili şekilde sağlar.

RCA'nın sınırlılıkları:

- Analizi yapabilecek bilgi birikimi olan gerekli uzmanlar mevcut olmayabilir,
- Önemli bir arızaya ait delil, arıza sırasında zarar görmüş ya da bakım/düzeltme esnasında bildirilmemiş olabilir,
- Takımın, bu durumu tamamen değerlendirmek üzere yeterli kaynağı ya da zamanı kullanmasına izin verilmeyebilir.

11.16. Hata Ağacı Analizi (Fault Tree Analysis-FTA)

Hata ağacı analizi kavramı (FTA), 1962 yılında Bell Telefon Laboratuvarlarında, Minutemen kıtalararası balistik füze hedefleme kontrol sisteminin güvenlik değerlendirmesini gerçekleştirmek maksadıyla dizayn edilmiştir.

Referans Standartlar:

- IEC 61025, Hata ağacı analizi (Fault tree analysis - FTA)
- IEC 60300-3-9, Güvenilebilirlik Yönetimi — Kısım 3: Uygulama Rehberi— Bölüm 9: Teknolojik sistemlerin risk analizi (Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems)

FTA, istenmeyen belirli bir duruma katkı sağlayan faktörleri analiz etmek ve tanımlamak için kullanılan bir tekniktir ('zirve olay' olarak adlandırılır). Doğal faktörler çıkarımsal olarak tanımlanır, mantıklı bir şekilde organize edilir, doğal faktörleri ve bunların zirve olay ile olan mantıksal bağlarını tasvir eden bir ağaç

grafiğinde resimli bir şekilde sunulur. Ağaç grafiğinde tanımlanan faktörler, bileşen donanım arızaları, istenmeyen duruma sebebiyet veren diğer ilgili durumlar ya da insan kaynaklı hatalar ile ilgili durumlar olabilir.

Bir hata ağacı tasarlanırken, bir grup sembol kullanılır. Hata ağaçlarında, olaylar (kök nedenler) ve mantıksal kapılar temel kavramlardır. Hata Ağacı Analizinde bir VE - VEYA yaklaşımı benimsenmiştir. Bir olay ya oluşuyordur ya da oluşmuyordur. Daha sonra olay ifadesi "doğru" veya "yanlış" olarak belirtilebilir. Bu aynı zamanda ikili mantığın ve yanlış veya doğru şeklinde değer alan cebirin uygulanabileceği anlamına gelen mantıksal değerler "1" ve "0" şeklinde de ifade edilebilir.

Bir hata ağacı, hataya (üst durum) giden yolları ya da potansiyel nedenleri kalitatif olarak tanımlamak için kullanılabilir. Ayrıca yine hataya neden olan durumların olasılıklarının da kullanılması vasıtasıyla analizi yapılmak istenen üst olayların meydana gelme olasılığını kantitatif olarak hesaplamak için de kullanılabilir.

Bir sistemin tasarım aşamasında, hatanın potansiyel nedenlerini tanımlamak için ve buna bağlı olarak farklı tasarım seçenekleri arasından seçim yapmak için de yaygın olarak kullanılır. İşlem sürecinde zirve olaya giden farklı yolların bağıl önemini ve ana hataların nasıl meydana geldiğini tanımlamak için kullanılır.

Bir hata ağacı ayrıca, farklı durumların hatayı oluşturmak için nasıl bir araya geldiklerini grafiksel olarak göstererek, meydana gelen hatayı analiz etmek için de kullanılır. Hata ağacı metodolojisi, sistem hatalarını ve sistem ve sistem bileşenlerinin hatalarındaki özgül sakıncalı olaylar arasındaki bağlantıyı gösteren mantıksal diyagramlardır. Bu metod, tümden gelimli mantığa dayanan bir tekniktir. Sakıncalı olay, daha önceden tanımlanmış olay ile hataların nedensel ilişkileridir. FTA, bir işletmede yapılan işler ile ilgili kritik hataların veya ana (majör) hataların, sebeperinin ve potansiyel karşıt önlemlerinin şematik gösterimidir. Ayrıca düzenleyici hareketleri veya problem azaltıcı hareketleri tanımlar.

FTA'nın amacı hataların gidiş yollarını, fiziksel ve insan kaynaklı hata olaylarını sebep olacak yolları tanımlamaktır. FTA, belirli bir hata olayı üzerine odaklanan analizci bir tekniktir. Daha sonra muhtemel alt olayları mantıksal bir diyagramla şematize eder. Grafik olarak insan ya da malzeme kaynaklı hasarların muhtemel kombinasyonlarını oluşturur. İhtimallerini ortaya çıkarabileceği önceden tahmin edilebilen istenmeyen hata olayını (zirve olay) grafik olarak gösterir. FTA çok geniş kapamlı olarak kullanılabilirlik, güvenlik ve risk analizinde kullanılır.

FTA kantitatif bir teknik olarak bir hatayı alt bileşenlerine ayırarak onu irdelediği için kullanışlıdır. Bu şekilde sistemi oluşturan her bir parçanın modifiye edilmesi, çıkarılması ya da elde edilmesine olanak sağlar. FTA; tanımlamada tasarımda, modifikasyonda, operasyonda, destekli kullanımda ya da bir proseste bir sistem için kullanılabilir.

Özellikle hiçbir işletim geçmişi olmayan yeni teknik proseslerin kullanımında çok yararlı olur. FTA'dan elde edilen değerler bir dizi mantık diyagramları olarak bazı kombinasyonların muhtemel hatalara nasıl yolaçabileceğini gösterir. Elde edilen değerler kalitatiftir. Elde edilen hasar verileri oranlanabilirse ya da tahminler hasar olayları için mevcutsa sonuçlar kantitatif hale getirilebilir. Bir hata ağacı bütün muhtemel bileşke hasar türlerini ya da hata olaylarını içeremez. Genellikle en üst olaya göre düzenlenirler ve zamanla kısıtlanırlar.

Hata Ağacı Analizi, sistemde tehlike olarak kendini gösteren olası tüm problem veya hataların tanımlanmasında ve analizinde kullanılan sistematik bir yolu temsil eder.

FTA her düzeyde tehlike oluşturan hataların analizini yapar ve bir mantık diyagramı aracılığı ile en büyük olayı (kaybı) yaratan hataların ve problemlerin olası tüm kombinasyonlarını gösterir. Ayrıca hatanın belirlenmesinde söz konusu aşamalara yol göstererek karmaşık ve karşılıklı ilişkiler sonucu ortaya çıkan olumsuzluğun belirlenmesini ve bu olumsuzluğun oluşma olasılığını değerlendirmeyi amaçlar. Bu yönüyle FTA, FMEA tekniği ve diğer kalite araç ve teknikleri ile amaç birliği içinde uygulanabilir. FTA'da oluşması istenmeyen olayın kökündeki sebebe kadar inilerek istenmeyen diğer olası hatalar ve onların sebepleri ortaya çıkarılır. Tüm bu hataları ve sebeplerini görüntülemede tekniğin kendine özel mantık sembollerinden yararlanılarak hatanın soy ağacı çıkarılır.

FTA'da FMEA gibi sistem analizine gerek duyar. Sistem analizi olgusunun içerdiği ön koşulları aşağıdaki şekilde özetlemek olasıdır.

- Sistem ilişkisi çerçevesinde düşünülmesi,
- Kritik sistem elemanlarının seçilmesi,
- Kritik işletme koşullarının belirlenmesi.

Ağaçlar hiyerarşik modellerdir ve bu modeler güvenlik dayanabilirlik ve risk değerleri açısından performans değerlendirmede önemli rol oynar.

Hata Ağacı Analizinin ana hedefleri şunlardır:

- Herhangi bir sistemin güvenirliğinin tanımlanması

• Herhangi bir probleme etki eden karmaşık ve biri birleri ile karşılıklı ilişki içinde bulunan olumsuzlukların belirlenmesi ve bu olumsuzlukların oluşma olasılıklarının değerlendirilmesi

Herhangi bir sistemde kendini tehlike olarak hissettiren tüm problem veya olumsuzlukların sistematik olarak ortaya konulması

Süreç:

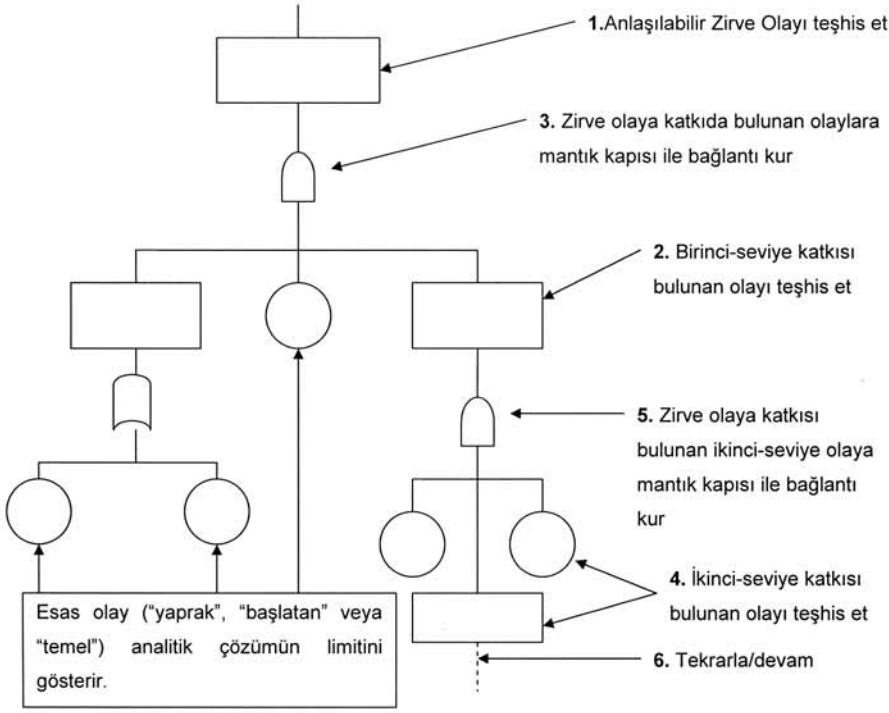
Bir hata ağacı geliştirmeye yönelik adımlar aşağıda gösterilmiştir:

- Analiz için bir proses veya bölüm seçilir ve bileşenler içine listelenir.
- Analiz edilecek olan "zirve olay" tanımlanır.
- Bu zirve olay, bir hata ya da bu hatanın daha geniş kapsamlı bir sonucu olabilir. Sonucun analiz edildiği yerde, ağaç gerçek hatanın hafifletilmesi ile ilgili bir bölüm içerebilir.
- Zirve olay ile başlayarak, muhtemel doğrudan nedenler ya da bir üst duruma neden olan hata modları tanımlanır.
- Hataya nasıl sebep olunduğunu tanımlamak için bu hataların\hata modlarının her biri analiz edilir.
- Daha fazla analiz verimsiz olana kadar, sırası ile daha düşük sistem seviyelerine göre istenmeyen sistem işlemlerinin adım adım tanımları yapılır. Bu, bir donanım sisteminde bileşik hata seviyesi olabilir. Analiz edilen en düşük sistem seviyesindeki durumlar ve doğal faktörler temel durumlar olarak bilinir.
- Olasılıkların temel durumlara bağlanabildiği yerde, üst durumun olasılığı hesaplanabilir.
- Kantitatif değerlendirmenin bir parçası olarak, hata ağacının, benzer hata modlarına açıklama getirmek için Boole cebri kullanarak sadeleştirilmesine ihtiyaç duyulabilir.
- Zive olayın ya da bir üst olayın olasılığının bir tahmininin yanı sıra, zirve olaya giden farklı yolları şekillendiren minimal kesim kümeleri tanımlanabilir ve üst duruma olan etkileri hesaplanır.
- Yinelenen durumlar hata ağacının çeşitli yerlerinde bulunduğunda, hesaplamaları uygun bir şekilde ele almak ve minimal kesim kümelerini hesaplamak için basit hata ağaçlarının dışında, bir yazılım paketine de ihtiyaç duyulur. Yazılım araçları, tutarlılığı, doğruluğu ve doğrulanabilirliği sağlamaya yardımcı olur.

Süreci kısaca ve şematik olarak göstermek istersek;

1. Analiz edilecek olan "zirve olay" tanımlanır,
2. Proses ve bölüm ile ilgili kritik arızalar ve tehlikeler tanımlanır,
3. Riskin sebebi tanımlanır ve riskin altına muhtemel bütün sebebleri listelenir ve oval daireler içinde riske bağlanır,
4. Bir kök sebebe doğru ilerlenir. Her risk için sebeblere ulaşana kadar tanımlanır.
5. Her kök sebeb için karşıt ölçümler tanımlanır. Beyin fırtınası ile her kritik riskin kök nedeni belirlenir. Her karşıt ölçüt için bir kutu oluşur ve ilgili kök nedenin altına kutular içinde neden ile ve karşıt ölçütleri birbirine bağlanır. Tüm bu amaçlara yönelik olarak FTA diğer metedolojilerde olduğu gibi amaçların belirli olduğu sistematik bir yol izlemek durumundadır. Bu yol genel olarak tanımlama, planlama, değerlendirme ve sonuçların analizi ve önerilerin belirlendiği adımlardan ibarettir:

Şekil 32: Hata Ağacı Oluşturma Aşamaları



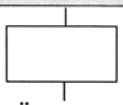
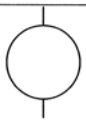
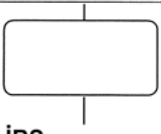
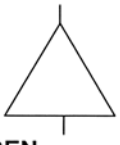
FTA DIN 25424'de standartlaştırılmış olup, oluşturulmasında bilgisayar programcılarının da sıkça başvurdukları Bool Elektronik Devre Sembolleri kullanılır. Böylelikle probleme etki eden tüm olumsuzlukların analitik olarak gün ışığına çıkarılması sağlanır.

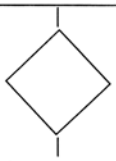
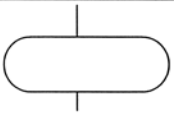
11.16.1. Ağaç Yapısı ve Semboller

Sistem performans amaçları ve hedefleri tanımlamada açık bir mantığın gerekli olduğu noktalarda kurulacak sistemi görsel olarak tanımlamada önemlidir. Ağaç yapısının asıl amacı temel insan, cihaz ve çevresel olaylar arasındaki ilişkileri gösterir.

Basit ağaç yapısı sistem hatası veya başarı serilerinin niteliksel karakterizasyonudur. Bu yapıların oluşturulmasında kullanılan semboller şunlardır:

FTA DİYAGRAMLARINDA KULLANILAN SEMBOLLER:

OLAYLAR	ANLAMI
 DİKDÖRTGEN	Mantık kapısı ile bağlı daha basit olayların, elementlerin veya faktörlerin kombinasyonu ile ortaya çıkan olay
 DAİRE	Esas olay (Yaprak, başlatan olay). Bu sembol birincil durumdaki problem için kullanılır. Daha ileri bir gelişimi gerektirmeyen, işleme gerek duyulmayan temel bir olaydır.
 ELİPS	Mantık kapısı ile bağlı yapılması zorunlu olay
 ÜÇGEN	Aktarma sembolü. Bağlantı ve birleştirme görevinde kullanılır.
 VE KAPISI	Sadece sembol altındaki tüm girdi olayların gerçekleşmesi durumunda yukarıda yer alan olayın ortaya çıkması gerçekleşir.

 VEYA KAPISI	Sembol altındaki bir veya birden fazla girdi olaydan en az herhangi birinin gerçekleşmesi durumunda yukarıda yer alan olayın ortaya çıkması gerçekleşir.
 KOMBİNASYON	N Girdi olay içinden en az M tanesi gerçekleşirse baştaki olay gerçekleşir.
 KARO	Sebebi tanımlanmamış ve belirsiz bir son olayı tanımlamaktadır.
 DARALTILMIŞ DAİRE	Analizin bu bölümünde daha fazla ilerlemeye ihtiyaç olmadığını işaret eder.

11.16.2. FTA Diyagramının Yapılandırılması

Hata Ağacı Analizinde öncelikle grafik değerlendirmesi yapılır. Zirve olay (top event) analizin baş konusudur ve en önemli etki, performans, sakatlık, tahribat veya kaybı ifade etmektedir. FTA, prosesle ilgili faktörleri içermektedir. Yani bu faktörlerin direkt veya endirekt etkisinde gelişen diğer olay veya hatalar sonuç olarak zirve olayı oluşturmaktadır. Düşünülen faktörler diyagrama yerleştirilmek üzere listelenir. Hata ağacı analizi diyagramı, diyagramın tüm alt faktörlere kadar oluşturulmasıyla tamamlanır.

Zirve olayın tespiti;

- Geçmiş yangın veya patlama kayıtları (sistemin kendine veya başkalarına ait),
- Enerji kaynaklarına ait olay veya kaza kayıtları,
- Potansiyel kayıp hatalar ile ilgili veriler,

- "What İf" senaryoları geliştirilmiş ise bu veriler,
- "Çeklist"'ler den elde edilen hatalara ait veriler,

Sonuçlar:

Hata ağacından gelen sonuçlar aşağıda gösterilmektedir:

- İki ya da daha fazla eş zamanlı olayın meydana geldiği durumda, etkileşim yollarını gösterecek şekilde, zirve olayın nasıl oluştuğunun grafik ile gösterimi,
- Her birinin meydana gelme olasılığı (verinin mevcut olduğu yerde) ile minimal kesim kümelerinin (arızaya giden özgün yollar) analizi,
- Zirve olayın olasılığı (kantitatif olarak uygulanırsa).

Güçlü Yönler ve Sınırlılıklar:

FTA'nın güçlü yönleri:

- Son derece sistematik bir metodolojidir, aynı zamanda, insan ilişkileri ve fiziksel olayları da içeren çeşitli faktörlerin analizini sağlamaya yönelik disiplinli bir yaklaşıma sahiptir,
- Tekniğe dahil olan ''tepeden aşağı'' yaklaşımının uygulaması, zirve olay ile doğrudan ilgili olan hatanın etkileri üzerinde yoğunlaşır,
- FTA, özellikle birçok ara yüz ve etkileşimler ile karmaşık sistemleri analiz etme konusunda çok başarılıdır,
- Grafiksel anlatım, insan davranış ve diğer alt faktörlerin dahil olduğu sistemlerin kolayca kavranmasını sağlar, ancak ağaçlar büyüdükçe, hata ağaçlarının işleyişi, bilgisayar sistemlerine ihtiyaç duyabilir,
- Bu özellik, daha karışık mantıksal ilişkilerin de dahil edilebilmesini sağlar (kombinasyon), ancak hata ağacının doğrulanmasını zor hale getirir,
- Hata ağacının ve kesim kümelerinin tanımlamalarına yönelik mantık analizi(Boole cebiri), zirve olaya neden olan durumların belirli kombinasyonlarının bulunduğu çok karmaşık sistemlerde yer alan hata yollarını tanımlama konusunda faydalıdır.

Sınırlamalar aşağıdakileri içermektedir:

- Temel durumların olasılıklarındaki belirsizlikler, zirve olayın olasılığının hesaplanmasını zorlaştırır. Kök olayların hata olasılıklarının kesin olarak bilinmediği durumlarda belirsizlik nedeni ile hesaplama yapılamayabilir. Belirlenen olasılıklara yüksek derecede güven duygusu, ancak iyi şekilde kavranan bir sistemde mümkündür,

- Bazı durumlarda, doğal olaylar birbirlerine bağlı değildir ve zirve olaya giden bütün önemli yolları tespit etmek zor olabilir,
- Hata ağacı sabit bir modeldir; zamana bağımlı durumlara değinilmez,
- Hata ağaçları sadece ikili durumlar (hatalı-arızalı\hatasız-arızasız) ile ilgilenir.
- İnsan kaynaklı hata modlarına olasılık atamak için ciddi gözlem veya başka insan hataları ile ilgili risk değerlendirme yöntemleri ile birlikte kullanım gerekebilir,
- Bir hata ağacı, domino etkilerinin ya da koşullu hataların kolayca tespit edilmesini sağlayamayabilir.

11.16.3. Kantitatif Analiz

Hata ağacı analizi diyagramında listelenmiş faktörlerin, olayın veya problemin oluşabilirliğinin gerçekten ortaya koyabileceğinden ve herbir faktör veya alt faktörün pratikte ortaya konabileceğinden emin olunmalıdır. Kantitatif analiz ile;

- P_F değeri saptanır.
- P_F ile R arasında ilişki kurulur.
- Üstel hata dağılımları belirlenir.
- Mantık kapısından diğer mantık kapısına yayma tespit edilir.

11.16.4. Güvenirlik ve Hata Olasılık Bağlantıları

S = Başarılar (Successes)

F = Hatalar (Failures)

R = Güvenirlik

$\mathbf{P_F}$ = Hatanın Olasılığı (Failure Probability)

$$\mathbf{R} = \frac{\mathbf{S}}{(\mathbf{S} + \mathbf{F})}$$

$$\mathbf{P_F} = \frac{\mathbf{F}}{(\mathbf{S} + \mathbf{F})}$$

$$\mathbf{R} + \mathbf{P_F} = \frac{\mathbf{S}}{(\mathbf{S} + \mathbf{F})} + \frac{\mathbf{F}}{(\mathbf{S} + \mathbf{F})}$$

KAPILARA GÖRE R VE P_F :

2 GİRDİ İÇİN

VEYA KAPISI

İki bağımsız elementten herhangi biri sistem hatası meydana getirebilir.

$R_T = R_A \cdot R_B$

$P_F = 1 - R_T$

$P_F = 1. (R_A.R_B)$

$P_F = 1 - [(1 - P_A).(1-P_B)]$

$P_F = P_A + P_B - P_A \cdot P_B$

Birleşme

VE KAPISI

İki bağımsız elementten her ikisi birlikte sistem hatası meydana getirebilir

$R_T = R_A + R_B - R_A \cdot R_B$

$P_F = 1 - R_T$

$P_F = 1 - (R_A + R_B - R_A \cdot R_B)$

$P_F = 1-[(1-P_A)+(1-P_B)-(1-P_A)(1-P_B)]$

$P_F = P_A \cdot P_B$

Kesişme

$R + P_F \equiv 1$

$P_{A,B} \leq 0.2$
Eror ≤ %11

⟹

$P_F \approx P_A + P_B$

3 GİRDİ İCİN

$P_F = P_A + P_B + P_C$

$- P_A.P_B - P_A.P_C - P_B.P_C + P_{A..}P_B.P_C$

⟸ İHMAL EDİLECEK DÜZEYDE

$P_F = P_A.P_B.P_C$

KAPILARA GÖRE P_F'İN TÜRETİLMESİ:

VE KAPISI

ZİRVE

$P_T = \Pi P_e$ → **$P_T = P_1.P_2$**

Kesişme

1 2

P_1 **P_2**

VEYA KAPISI

ZİRVE

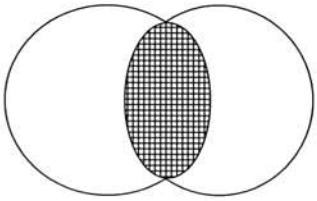
$P_T \approx \sum P_e$ → **$P_T \approx P_1 + P_2$**

Birleşme

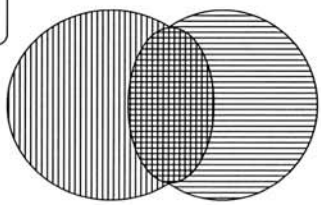
1 2

P_1 **P_2**

1 & 2 Bağımsız Olaylardır



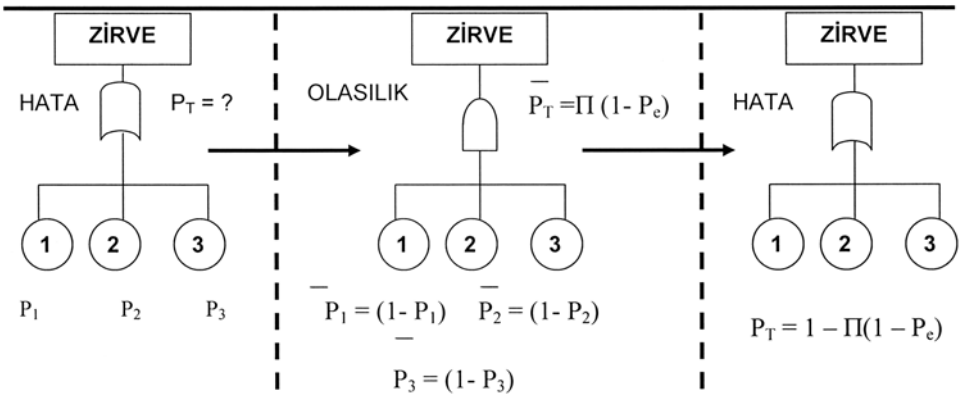
$P_T = P_1 \cdot P_2$



P_T **$- P_1 \cdot P_2$**

İhmal Edilebilir

"VEYA" KAPISININ ÇÖZÜMÜ:



VE KAPISI $\Longrightarrow$ $P_T = \prod_{i=1}^{n} (1 - P_i)$

VEYA KAPISI $\Longrightarrow$ $P_T = 1 - \prod_{i=1}^{n} (1 - P_i)$

KALİTATİF ANALİZ:

Bu nedenlede hatanın olasılığının değerlendirilmesinin yapılması ve daha iyi sonuç alabilmek, sistemdeki asıl hataları tespit edebilmek için "minimal cut set" değerlendirmesi yapılarak "Azaltılmış Hata Ağacı - Mantık Eşit Hata Ağacı" 'nın tespit edilmesi ve "path set" değerlendirilmelerinin yapılması gerekir.

MİNİMAL CUT SET:

Hata ağacı analizinde "minimal cut set" araştırması neye yardımcı olur?

1. Sistemin tanımlanması
2. Sistem zaaflarının azaltılması
3. Sistemin başarılı kılınması

CUT SET: Bir "Cut set", hepsi oluştuğu takdirde, zirve olayının (top event) meydana gelmesine neden olan herhangi bir hata ağacı grubudur.

MİNİMAL CUT SET: Bir "minimal Cut Set" hepsi oluştuğu takdirde, zirve olayının (top event) meydana gelmesine neden olan asgari hata ağacı grubudur.

Minimal Cut Set uygulaması yapılırken Boolean Matematiğinin bilinmesi gerekmektedir. Teorem kullanılarak cut set, minimal cut set'e indirgenir.

11.16.5. Boolean Matematiği

Boolean matematiği devre matematiği olarak da bilinir, George Boole (1815-1864) tarafından 1847' de mantığın, matematiksel analizi üzerine yazmış olduğu tezle ortaya çıkmıştır. Ancak bu düşünce, 1938 'den sonra Beel laboratuvarı tarafından yapılan röleli devrelerle, telefon işletmelerinde uygulama alanı bulabilmiştir. Boolean matematiği basit bir matematiktir. Boolean matamatiği Hata Ağacı Analizinde, bu analizi yapan analiste iyi bir analiz yapabilmesinde yardımcı olur. Boolen matematiği ile hata ağacının indirgenmesi sağlanır.

Basit Tarifler:

VE (AND) işlemi: Ve işleminde iki Boolean değişkeni vardır. A ve B çıkışı, (A.B) şeklinde yazılır.

VEYA (OR) işlemi: Veya işleminde A ve B gibi iki Boolean değişkeni vardır. (A+B) şeklinde yazılır.

Boolean Kuralları

Boolean matematiğinde kullanılan teoremleri işler duruma getirebilmek için aşağıdaki Boolean kurallarının bilinmesi gerekir.

A	B	A . B
0	0	0
0	1	0
1	0	0
1	1	1

Lojik VE (AND) işlemi

A	B	A + B
0	0	0
0	1	1
1	0	1
1	1	1

Lojik VEYA (OR) işlemi

Kural
1. A = 0 veya $\tilde{A}$ = 1
2. 0.0 = 0
3. 1 + 1 = 1
4. 0 + 0 = 0
5. 1.1 = 1
6. 1.0 = 0.1 = 0
7. 1 + 0 = 0 + 1 = 1

TEOREM

T_1: Commutative Kanunu Değişebilirlik

a) A+B = B+A

b) A.B = B.A

T_2: Associative Kanunu Birleşme

a) (A+B) + C = A + (B+C)

b) (A.B).C = A. (B.C)

T_3: Distributive Kanunu Dağılma

a) A.(B+C) = A.B +A.C

b) A+(B.C) = (A+B) (A+C)

T_4: Identity Kanunu Özdeşlik

a) A+A = A

b) A.A = A

T_5: Redudance Kanunu Fazlalık Yasası

a) A.(A+B) = A

T_6: Absorpsiyon Kanunu Soğurma

a) (A.B) + A = A

b) (A+B).B = B

T_7: Morgan Teorem

a) (A+B) = (A.B)

b) (A.B) = (A+B)

11.16.6. Mantık Matematiğinde İşlem Basitleştirilmesi

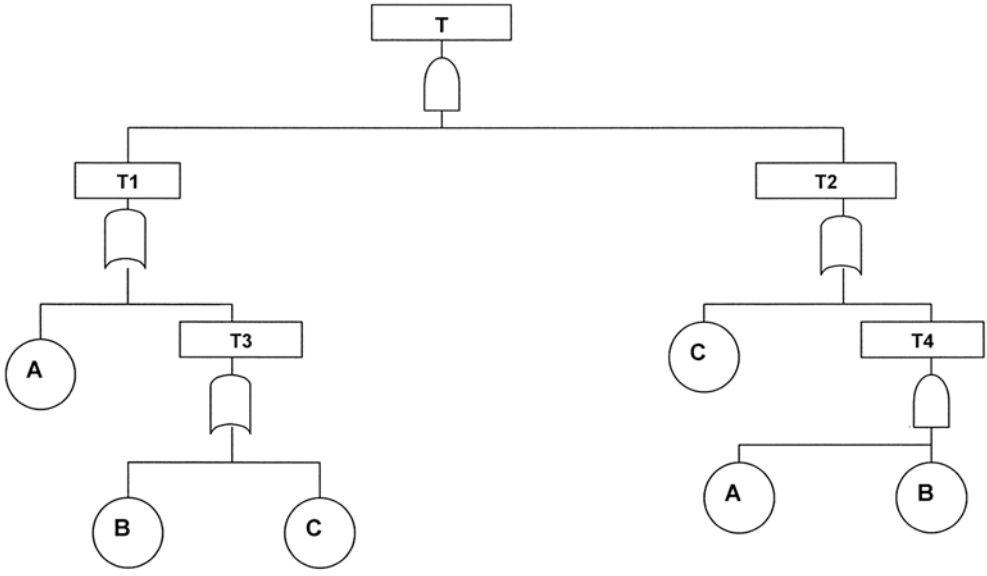
Çeşitli karmaşık işlemler yukarıdaki teoremlerden faydalanılarak basitleştirilebilir. Dolayısıyla aynı işlem birçok mantık kapısı yerine az kapı kullanılarak gerçekleştirilebilir. Böylece hata ağacı üzerinde hatalar daha basit olarak görülebilir. (Minimal Cut Set).

Cut Set'in bulunması ve Minimal Cut Set'e indirgenmesi için Boolean matematiği kullanılarak aşağıda iki yöntem verilmiştir.

DENKLEMİN İNDİRGENMESİ İLE MİNİMAL CUT SET ARAŞTIRMASI:

1. Hata ağacındaki, zirve olaya "T" harfi verilir.
2. Zirve olayın altıdaki, birbirine mantık kapıları ile bağlı basit olaylara "T1" 'den başlamak kaydıyla harf verilir.
3. Zirve olayın altındaki birbirine mantık kapıları ile bağlı esas olaylara "A" 'dan başlamak üzere harf verilir
4. Zirve olayın altındaki mantık kapılarına herhangi bir harf veya sayı verilmez.

Şekil 33: Örnek Hata Ağacı



Hata Ağacının Boolean Tanımlaması;

T4 = A . B

T3= B+C

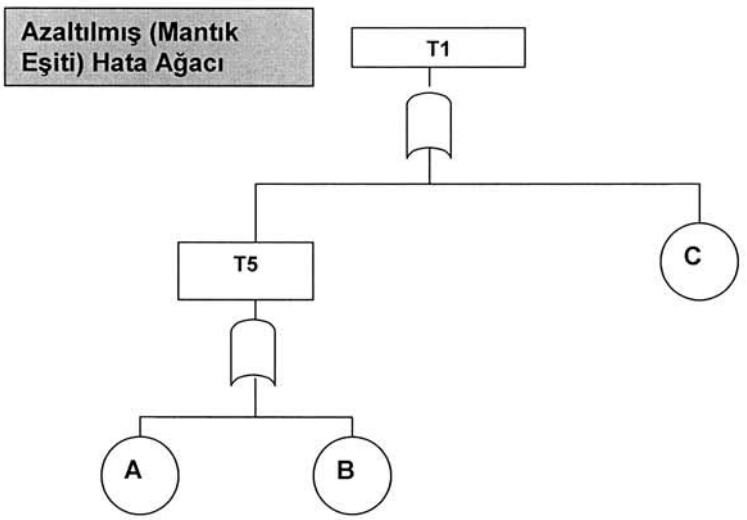
T1 = A + T3 = A + (B + C)

T2 = C + T4 = C + (A . B)

$T = T1 + T2 = (A + B + C).\ [\ C + (A\ .\ B)]$

$T = (A + B + C)\ .\ C + (A + B + C)$

$T = A\ .\ C + B\ .\ C + C + A\ .\ B + A\ .\ B + C\ .\ A\ .\ B$



MATRİS KULLANILARAK MİNİMAL CUT SET ARAŞTIRMASI:

1. Esas olay (yaprak, başlatan olay)'lar hariç ağaçdaki tüm elementleri yok say
2. Zirve olaya en yakın olandan başlamak kaydıyla, mantık kapılarına "harf", yapraklara (esas olay) "sayı" ver
3. Birinci adım olarak zirve olaydan aşağıya doğru, harfleri ve numaraları kullanarak matris oluşturulur.
4. İlk olarak zirve olayın altındaki mantık kapısının harfi matrisin en üst sol kısmına yazılır.
5. "VE" kapılarının harfleri matriste YATAY olarak yazılır, yine "VE" mantık kapılarının girdileri de matriste YATAY olarak yer değiştirilir.

6. “VEYA” kapılarının harfleri matriste DÜŞEY olarak yazılır, yine “VEYA” mantık kapılarının girdileri de matriste DÜŞEY olarak yer değiştirilir. Harfin altındaki sıralar dolu ise aşağıya doru yeni bir satıra yazılır, ancak “VEYA” mantık kapılarının girdilerini matriste yer değiştirirken harfin bulunduğu satırdaki tüm sayılar aşağıdaki yeni sırayada aktarılır.
7. Final matris sonucunda aşağıdaki değerlendirme yapılarak matris indirgenir ve “Minimal Cut Set” elde edilir:
   a) Bir satırın her elemanı yukarıdaki sütununda tekrarlanıyorsa satırı iptal et
   b) Bir satır içinde tekrarlanan bir sayı var ise sayının birini sil
   c) Birbirleriyle aynı olan satırları sil
8. Final Matris başlatıcıları gösteren bir matristir. Bu matriksin her satırı boolean cut set’i dir.

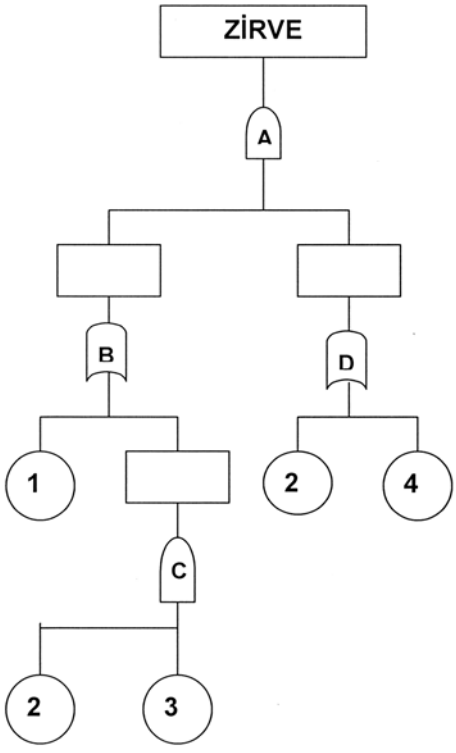
Şekil 34: Örnek1- Bir Cut Set Uygulaması

PROSEDÜR:

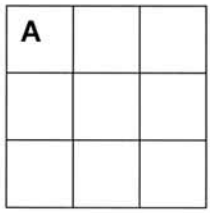
- Mantık kapılarına harf ata
(Zirvedeki mantık kapısı “A”dır.)
Esas olaylara harf verme

- Esas olaylara sayı ver. Eğer esas olaylar birden fazla ise

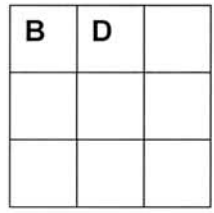
- Zirve mantık kapısı “A”dan başlayarak matris inşaa et,



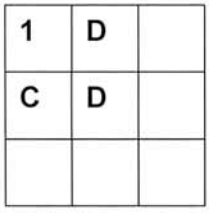
MATRİSİN OLUŞTURULMASI:



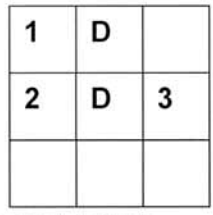
1. Matrisin sol en üst karesine zirve Mantık Kapısı olan **"A"** yazılır.



2. **"A"** bir **"VE"** kapısıdır; **"B & D"** girdileridir, yatay olarak yer değiştir.

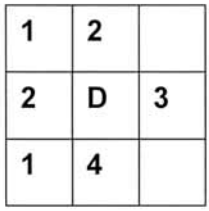


3. "**B**" bir "**VEYA**" kapısıdır. **"1& C"** girdileridir, düşey olarak yer değiştir. Yeni bir sıra açıldığından yanındaki tüm değerleri de aşağı taşı.



4. **"C"** bir **"VE"** kapısıdır. **"2&3"** girdileridir, yatay olarak yer değiştir.

Bu Boolean- Cut Set'i gösterir.



5. **"D"** (üst sıradaki), kapı bir **"VEYA"** kapısıdır. **"2&4"** girdileridir, düşey olarak yer değiştir. Yeni bir sıra açıldığından yanındaki tüm değerleri de aşağı taşı.

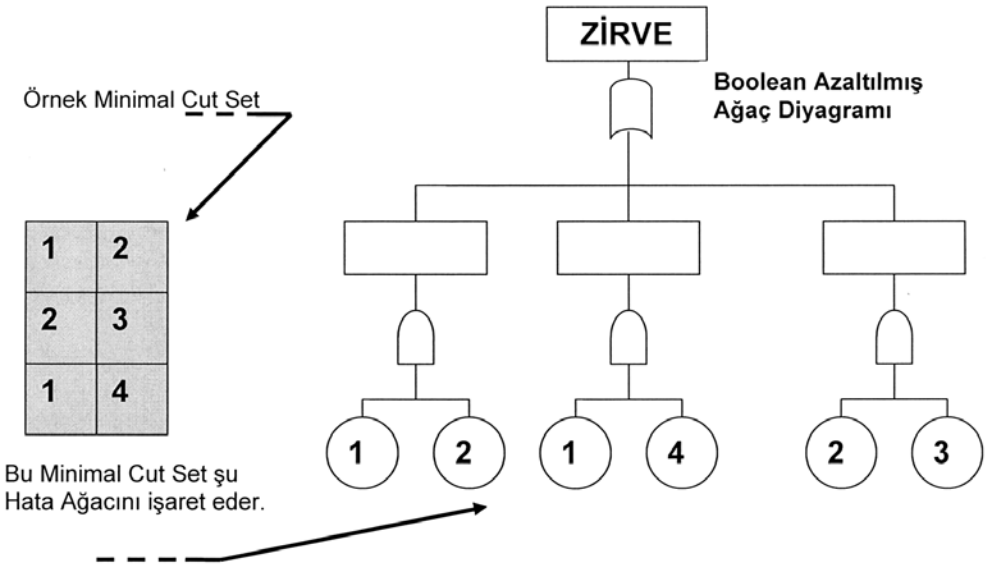
6. **"D"** (orta sıradaki), kapı bir **"VEYA"** kapısıdır. **"2&4"** girdileridir, düşey olarak yer değiştir. Yeni bir sıra açıldığından yanındaki tüm değerleri de aşağı taşı.

Minimal Cut Set'e indirge

Minimal Cut Set sıralaması, Zirve olaya neden olan asagri grup başlatıcı olaydır.

11.16.7. "Azaltılmış" Hata Ağacı- Mantık Eşiti Hata Ağacı:

Minimal Cut set ile oluşturulan azaltılmış Hata ağacı; örneğimiz için aşağıda verilmiştir:

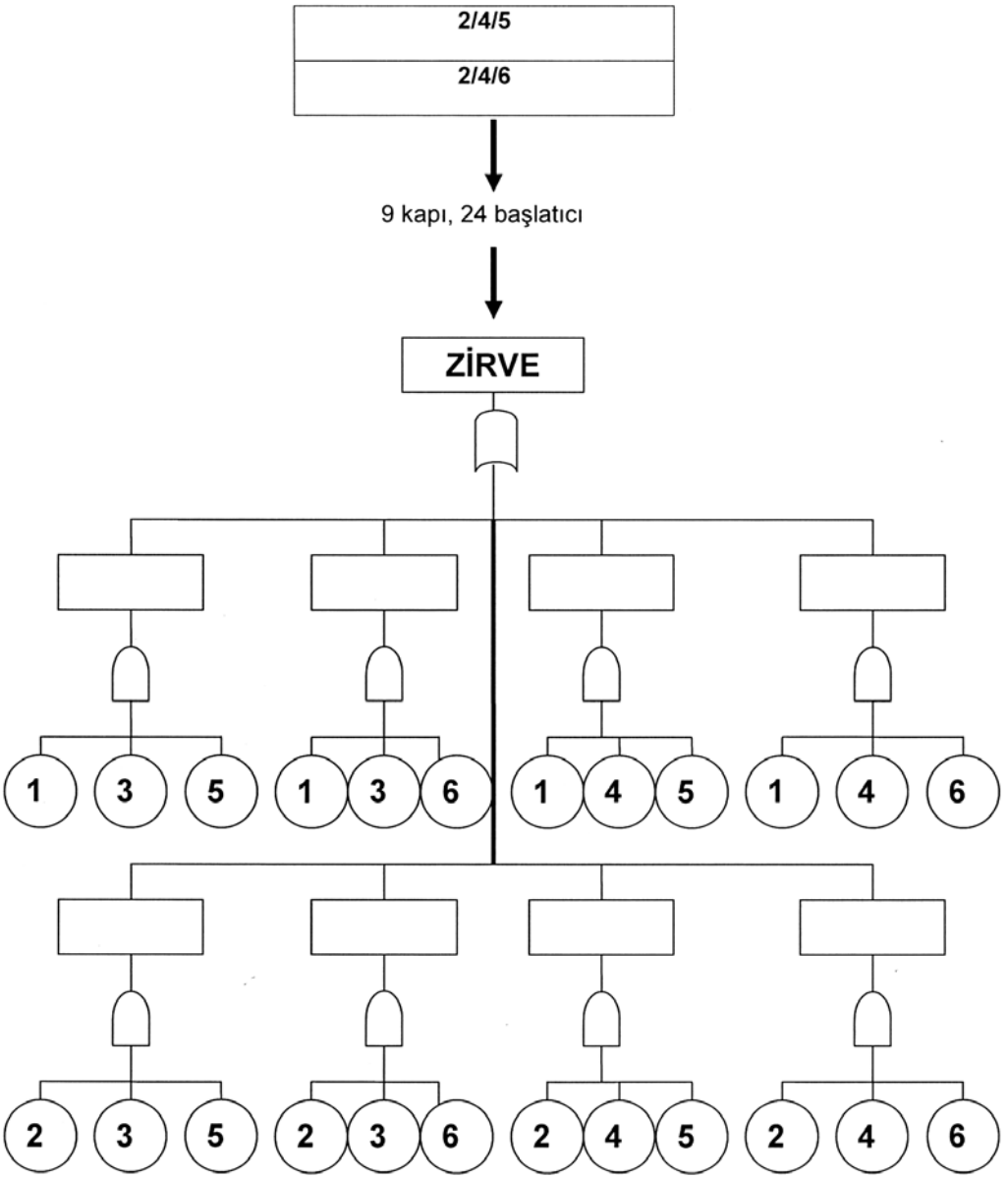


.....ve bu minimal cut setden elde edilen Hata Ağacı orjinalinin bir mantık eşitidir.

Azaltılmış eşit ağaç tek değildir. 4 Kapı ve 6 esas olay (başlatıcı) içermektedir.

Bu hata ağacı bu mantık eşitliklerini içermektedir.

MİNİMAL CUT SET
1/3/5
1/3/6
1/4/5
1/4/6
2/3/5
2/3/6



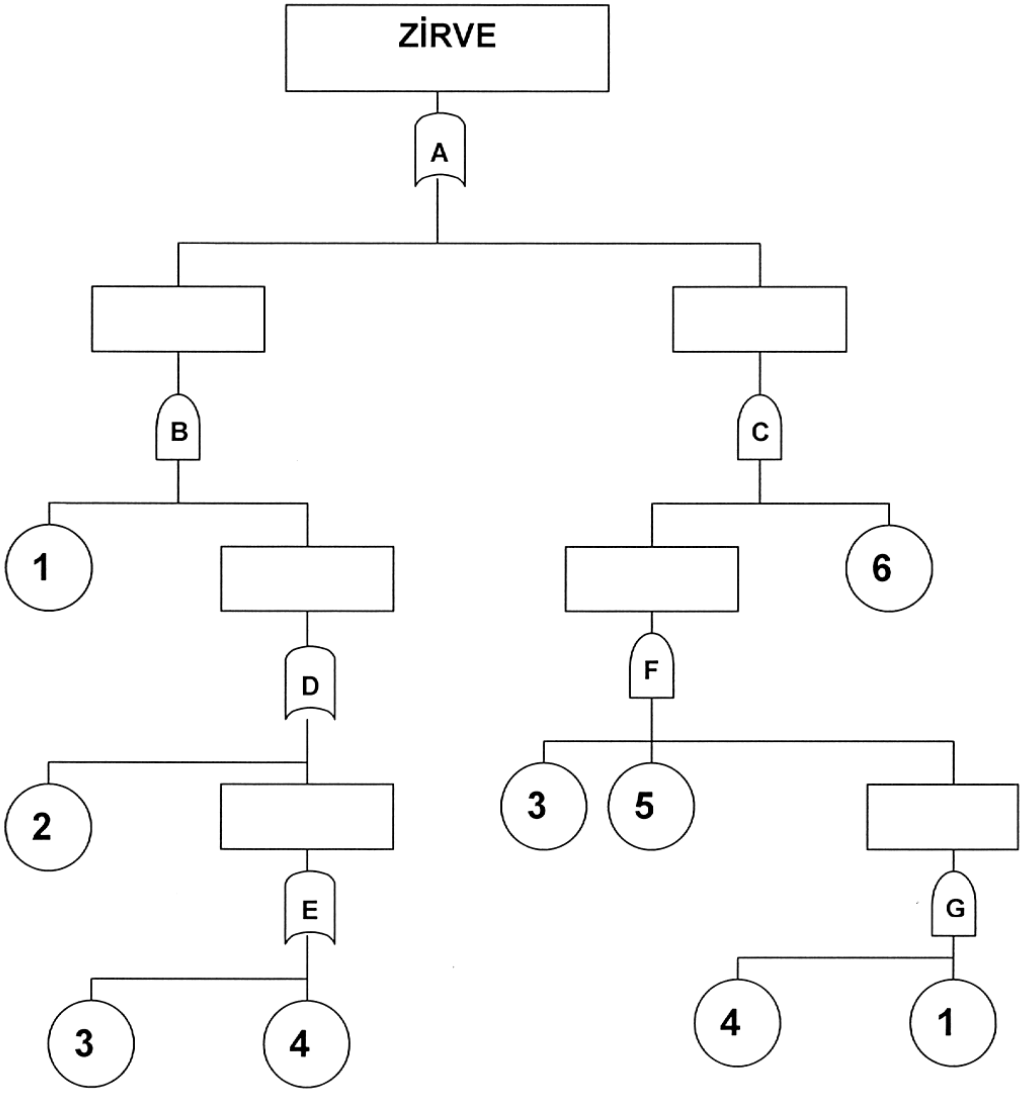
Örnek 2 – Bir başka Cut Set örneği;

PROSEDÜR:

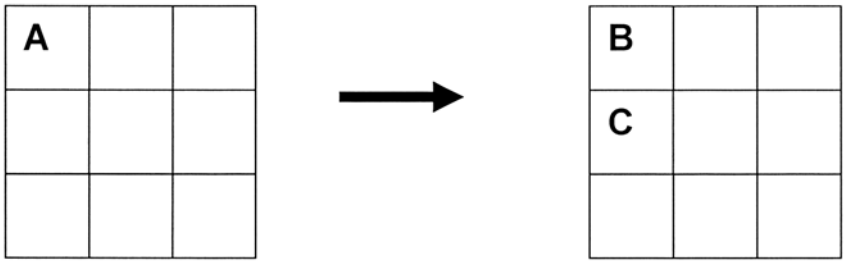
- Bu durum ilk cut set ile benzemektedir - değişik olan kısımlarını not ediniz.

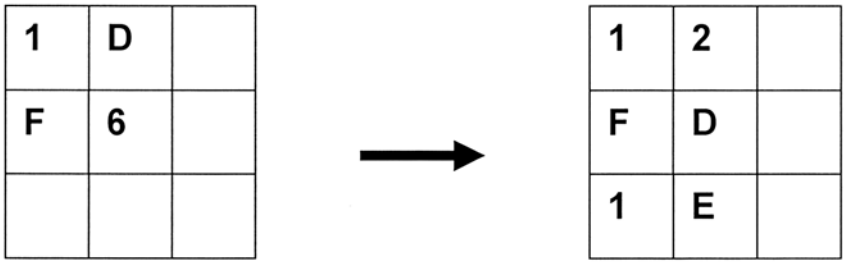
Zirve kapı “VEYA” ‘dır. İlk örnekte ise, zirve kapı “VE” ‘dir.

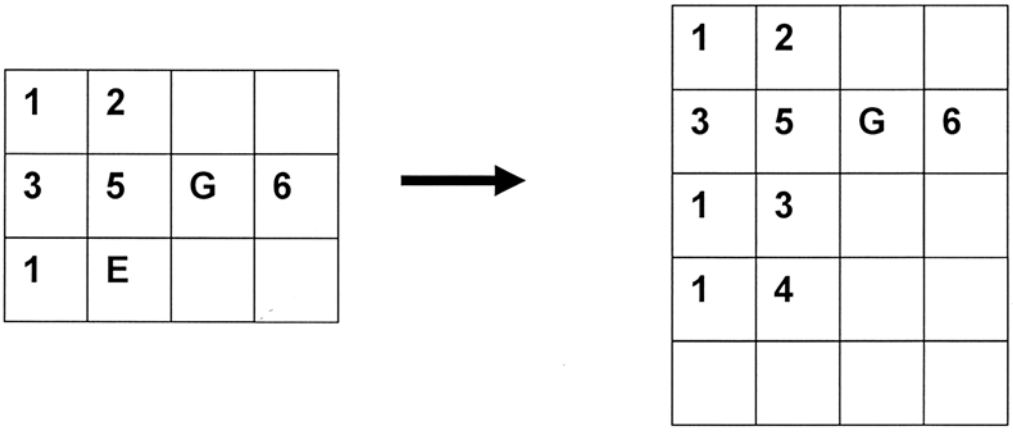
- Prosedür aynen ilk örnekte olduğu gibidir.



MATRİSİN OLUŞTURULMASI:







Boolean- Cut Set

1	2			
3	5	1	6	4
1	3			
1	4			
3	5	1	6	6

Minimal Cut Set

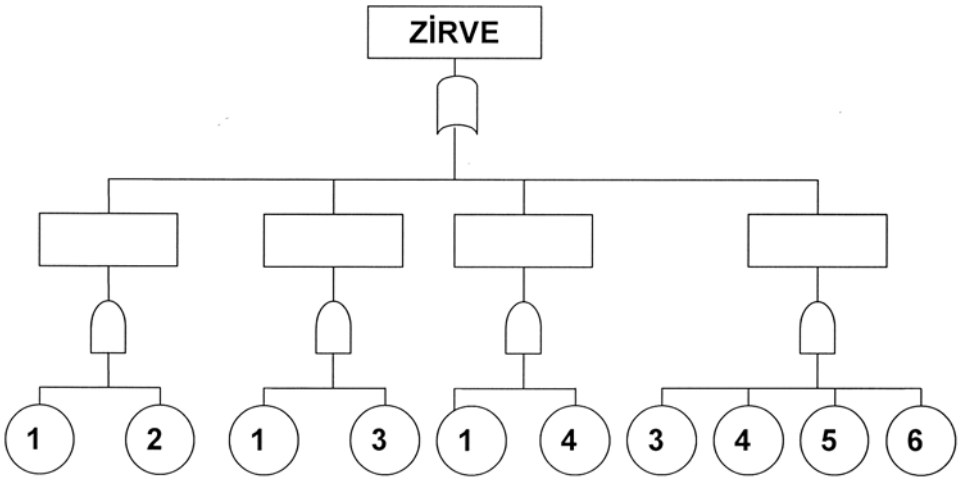
1	2		
1	3		
1	4		
3	4	5	6

Eşit Hata Ağacı Oluşturulması:

Burada dört adet Minimal Cut Set vardır.

Orjinal Hata Ağacının mantık eşiti

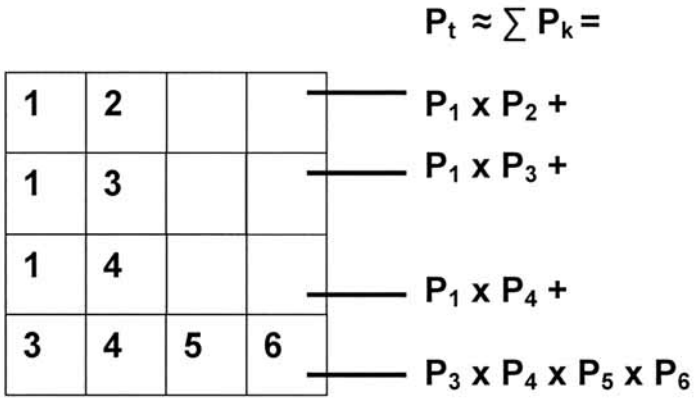
1	2		
1	3		
1	4		
3	4	5	6



Cut Set'in Kullanılması:

- P_T'nin değerlendirilmesi
- Maruz olunacak müşterek nedenlerin bulunması
- Müşterek nedenlerin olasığı analiz edilir
- Yapısal Cut Set'in ve kantatif değerlendirmenin yapılması sistemin çözümlenmesinde önemlidir
- Önemli "ETKİ" 'lerin değerlendirilmesi sağlanır.

CUT SET KULLANILARAK / P_T'NİN HESAPLANMASI;



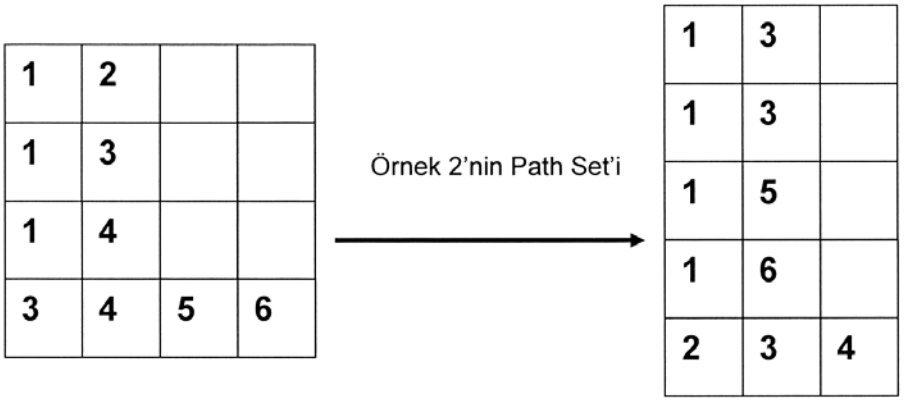
PATH SET:

- Ötedeki diyagonal ölçümleme yapılır.
- Bilgi alanının başarısına bağlantı kurulur.
- İş/Maliyet Çalışması

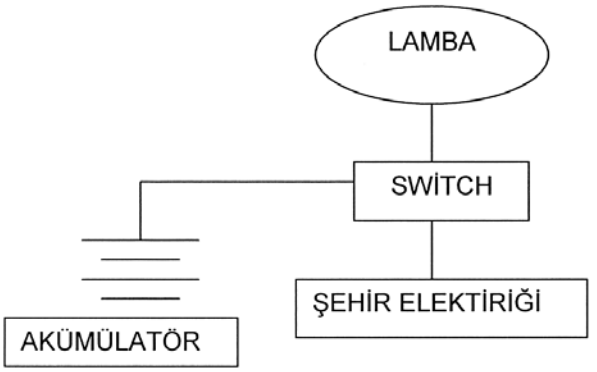
PATH SET: Bir "Path Set", hata ağacını başlatan bir gruptur ki, meydana gelmediği takdirde zirve olay garanti olarak meydana gelmez.

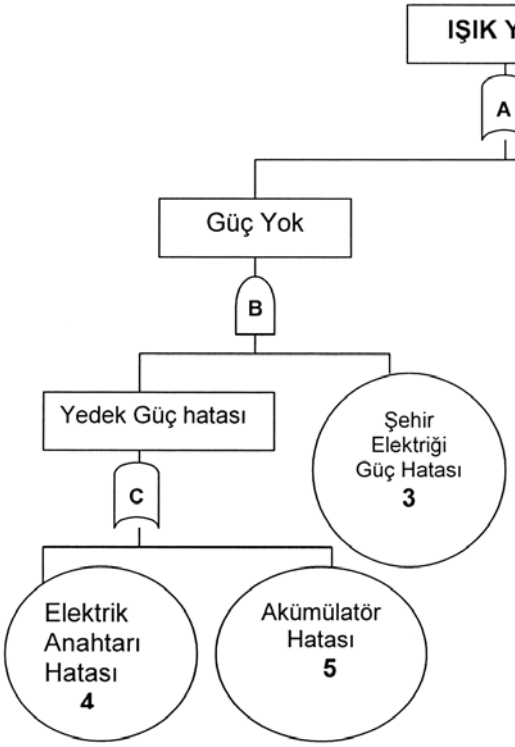
PATH SET'İN BULUNMASI: "VE" kapılarının hepsi "VEYA" kapıları ile, "VEYA" kapılarının hepsi de "VE" kapıları ile değiştirilir.

Path Set'in matriksinin oluşturulması ve prosedürü aynen cut set'in ki ile aynıdır. Matrisden alınan sonuç ise Path Set' dir. Bu Cut Set'den Path Set'e dönüştürme çift yönlü Morgan teoreminin avantajıdır. Path set, Cut Set'in tamamlayıcısıdır.



Örnek 3- Trafik lambası için şehir elektriği ile yedek güç kaynağı hataları hata ağacı analizi ile analiz edilmiştir.





P1 = 0,02 (%2 etki var, %98 yok)
P2 = 0,001
P3= 0,001
P4= 0,001
P5 = 0,002

C KAPISI İÇİN; $P_T = 1 - \prod_{i=1}^{n} (1 - P_i) = 1- (1-0.002)(1-0.001) = 0.002998$

B KAPISI İÇİN; $P_T = \prod_{i=1}^{n} (1 - P_i) = (0.002998)\ (0.001) = 2.998E\text{-}6$

A KAPISI İÇİN; $P_T = 1 - \prod_{i=1}^{n} (1 - P_i) = 1 -(1-2.998E\text{-}6)\ (1-0.001)\ (1-0.002) = 0.02098$

MİNİMAL CUT SET:

1		
2		
4	3	
5	3	

Minimal Cut Set'e göre olasılık hesabı;

$P_t \approx \sum P_k = P1+P2+P4.P3+P3.P5 = 0,02 + 0,001 + 0,001.0,001 + 0,001.0,002 =$

$0,021003 \approx$ **PT (A kapısının olasılığı)**

11.17. Hata Modu ve Etkileri Analizi (Failure Mode and Effects Analysis-Failure Mode and Critically Effects Analysis- FMEA/FMECA)

Hata modu ve etki analizi (FMEA), 1950'lerin sonundan beri kullanılmakta olan ve en iyi kurgulanmış risk değerlendirme tekniklerinden biri olarak kabul edilmektedir. Yöntem iyi dökümante edilmiştir ve kullanılışı ile ilgili birçok açıklayıcı yayın ve standart mevcuttur.

Hata modu ve etki analizi (FMEA), unsurlar, sistemler ya da süreçlerin planlanan hedeflerini gerçekleştiremediği hususları belirlemek için kullanılan bir tekniktir. FMEA metodu 60'lı yıllarda havacılık endüstrisinde kullanılmak üzere geliştirilmiştir. Bütün teknoloji ağırlıklı sektörler ile uzay sektörü, kimya endüstrisi ve otomobil sanayinde çok popülerdir. Bu metodun popüler olmasındaki başlıca sebep kullanımının kolay olması ve geniş teorik bilgi gerektirmemesidir.

Referans Standart:

- IEC 60812, Sistem güvenilirliği için analiz teknikleri- Arıza modu ve etki analizine (FMEA) yönelik prosedürler (Analysis techniques for system reliability – Procedures for failure mode and effect analysis -FMEA)

FMEA metodu genellikle parçaların ve ekipmanların analizine odaklanır. Bu metod, başarısızlığın olabildiği yer ve alanların herbirini çözümler ve kişisel fikirleri de dikkate alarak değer biçer ve sistemin parçalarının herbirine uygulanabilir.

Hata Modu ve Etki Analizi uygulaması;

- Her hatanın nedenlerini ve etkenlerini belirler,
- Potansiyel hataları tanımlar,
- Olasılık, şiddet ve saptanabilirliğe bağlı olarak hataların önceliğini ortaya çıkarır,
- Sorunların izlenmesini ve düzeltici faaliyetlerin yapılmasını sağlar.

Hata Modu ve Etki Analizi, ürünlerin ve proseslerin geliştirilmesinde öncelikli olarak hata riskinin ortadan kaldırılmasına odaklanan ve bu amaçla yapılan faaliyetleri belgelendiren bir tekniktir. Bu analiz öncelikle önleyici faaliyetlerle ilgilenmektedir.

TANIMLAR:

FMEA disiplini çalışmasında geçen ve MIL-STD-1629 askeri standartında verilen tanımlamalar aşağıda verilmiştir;

Hata Türü ve Etkileri Analizi, FMEA (Failure Mode Effect Analysis): Bir sistemdeki, prosesteki, makinedeki veya techizattaki her bir potansiyel hata türünün sistem üzerindeki sonuçları ya da etkilerinin değerlendirilerek sıklıklarına göre sınıflandırılmaları temeline dayanan teknik analiz yöntemi.

Hata Türu Kritiklik Etki Analizi, FMCEA (Failure Mode Criticality Effect Analysis): Her bir potansiyel hatanın; analiz edilerek nasıl tespit edileceği ve hangi düzeltici faaliyetlerin başlatılacağına karar verme prosedürü.

Hata Tanımı (Failure Definition): Bir sistemde, proses veya techizatta istenmeyen durum yaratan ve performans parametreleri ile izin verilebilen limitler cinsinden açıklanan genel tanım.

Hata Nedeni (Failure Cause): Süreçlerden, tasarım hatalarından, malzemenin veya techizatın yanlış kullanılmasından, kalite eksikliklerinden ya da diğer süreçlerden kaynaklanan temel nedenler.

Hata Modu (Failure Mode): Hatanın oluşma yolu ve cihazın işlevi üzerindeki etkisi olarak tanımlanabilen bir hatanın gözlendiği durum. Sistemlerde arıza veya hatalara neden olan mekanizmalar, bir bütünlük içerisinde meydana gelen rastsal veya doğal olaylar olabilir.

Hata modu, gerçekleştirilmediği veya yanlış gerçekleştirildiği gözlemlenen bir olaydır. Sistem içerisinde zarara neden olabilecek işlemler esnasında meyda-

na gelebilecek raslantısal ve doğal olaylardır. İşletmenin bütünü içerisindeki parçalar ayrı ayrı ele alınır, olası zarar verici olaylar tespit edilir, bu olaylara hata modları denilmektedir.

Zararların Etkileri- Sonuçları: Gerçekleşmesi olası durumların meydana getirdiği zararların işletme üzerindeki etkisinin belirlenmesidir.

Hata Etkisi (Failure Effect): Genellikle hataların etkileri, bütün sistemin hatadan nasıl etkilendiğine bağlı olarak sınıflandırılır. Bir hata türünün bir sistem biriminin operasyonu, fonksiyonu ya da çalışabilirliği üzerindeki sonuçları.

Çevre Etkisi (Environments Effect): Bir sistem, proses ve techizattan kaynaklanan ve malzemenin depolanması, kullanılması, taşınması, test edilmesi, kurulması ve kullanımı sırasında oluşan koşullar, etkiler, yayılımlar, atıklar ve bunların bir araya geldiğinde oluşturduğu çevresel etki.

Tek Hata Noktası (Single Failure Point) : Bir sistemde, operasyonel yöntemlerle ya da ekstra yapılan işlemlerle düzeltilemeyen bir birimin oluşturduğu hata.

Tespit Sistemi (Detection System): Normal çalışma koşullarında operatör tarafından ya da üretim elemanları tarafından, bir hatanın bazı özel tanıma faaliyetleriyle keşfedilmesini sağlayan yöntem.

Şiddet (Severity): Belli bir hata türü nedeniyle oluşmuş hatanın sonucu. Şiddet değerlendirilirken daima hatanın olabilecek en kötü sonucu düşünülür.

Kritiklik (Criticality): Bir hata türünün oluşum sıklığıyla ve etkisi ile ilgili bir ölçüm.

Kritiklik Analizi (Criticality Analysis): Hata türlerinin, hatanın önem ve oluşma olasılığı ile birlikte değerlendirilmesi.

Tespit Edilemeyen Hata (Undetectable Failure): Ekipman veya makinede, operatörün oluşan hatadan haberi olmasını sağlayacak herhangi bir tespit etme metodunun bulunmadığı durumlarda meydana gelen hata.

Çalışma Raporları (Study Reports): Sistemdeki olası hata türlerinin belirlenmesinde rehber olacak, tasarım sınırlamaları hakkında marjinal bilgileri veren rapor.

Blok Diyagramları (Block Diyagrams): Bir sistemdeki ekipmanların ve altsistemlerin birbirleriyle olan bağımlılığı, ilişkileri ile operasyonların sırasını göstermek için kullanılan diyagramlar.

Fonksiyonel Blok Diyagramları (Functional Block Diyagrams): Dizayn ve mühendislik akım şemalarında belirtilen operasyonlar ile fonksiyonların birbirleriyle olan ilişkilerini gösterir diyagram.

Güvenilirlik Blok Diyagramları (Reliability Block Diyagrams): Bir sistemin, prosesin, makinenin yada techizatın her birinin, çalışma koşulları içerisinde bütün fonksiyonlarının birbirleriyle bağlı oldukları ya da olmadıkları noktaların gösterildiği diyagramlar.

HTEA Raporu (FMEA Report): FMEA'nın sonuç tablosunun işlendiği ve diğer ilgili kaynak dokümanlarının, blok diyagramlarının, analiz yapılırken kullanılan tekniklerin ve sistemin tanımının da yapıldığı rapor.

FMEA, aşağıdaki işlemleri gerçekleştirmek için kullanılabilir;

- Bir sistemin çeşitli bölümlerinin potansiyel hata modları,
- Bu arızaların sistem üzerinden gösterebileceği etkiler,
- Hata mekanizmaları,
- Hataların nasıl engelleneceği ve/veya arızaların sistem üzerindeki etkilerinin nasıl azaltılabileceğini belirlemek,
- Tasarım alternatifleri seçiminde yüksek güvenilirlik sağlanmasına yardım etmek,
- Sistemlerin ve süreçlerin bütün hata modlarının ve işlevsel başarı üzerindeki etkilerinin dikkate alındığından emin olmak,
- İnsan kaynaklı hata modlarını ve etkilerini tanımlamak,
- Fiziksel sistemlerin bakımına, planlamasına ve denenmesine bir zemin hazırlamak,
- Prosedür ve süreçlerin tasarımını geliştirmek,
- Hata ağacı analizi gibi analiz teknikleri ile birlikte kullanım ile sistemlerin kantitatif analizini yapmak, sistemler hakkında kantitatif bilgi sağlamak.

FMEA, parçalardan büyük fonksiyon bloklarına kadar birçok sistem seviyesinde kullanılabilir. Bu yöntem teknik sistemlerin analizinde kullanılmaktadır. Prensipte, sistemde bulunan herbir bileşen incelenmekte ve iki temel soru sorulmaktadır.

- Birim nasıl çalışmaz?

- Bundan sonra ne olur?

Bunun anlamı, analitik prosedürün detaylarının farklılık göstereceğidir. Analizin ana aşamaları aşağıdaki gibidir.

- Sistem, blok diyagramı veya listesi şeklinde farklı birimlere ayrılır,
- Çeşitli birimler için hata modları tespit edilir,
- Muhtemel sebepler, sonuçlar ve aksaklığın önemi her bir hata modu için değerlendirilir,
- Hatanın nasıl tespit edileceğine ilişkin araştırma yapılır,
- Uygun kontrol önlemleri için tavsiyelerde bulunulur.

Analiz için özel bir kayıt dökümanı kullanmak en iyisidir. IEC 60812 tarafından 12 kolondan oluşan bir versiyon yayımlanmıştır. Bu versiyondaki tablo başlıkları aşağıda verilmiştir.

- Tanımlama-bileşen tasarımı, fonkisyonu,
- Hata modu,
- Hata sebebi,
- Hata etkisi,
- Hata tespiti,
- Muhtemel faaliyetler,
- Olasılık ve/veya kritik seviye

FMEA kullanılırken oldukça fazla sayıda muhtemel hata tespit edilecektir. Bunları önemlerine göre sıralamak pratik olabilir fakat bu sınıflandırma, yöntem için "kritik" olarak kabul edilmektedir. Bu, meydana gelme ihtimalini veya etkilerin ciddiyetini tartmak gibi birçok yolla başarılabilir. Bazen, yöntem Hata Modu, Etkiler ve Kritiklik Analizi (FMECA) olarak adlandırılmakta, bu kritiklik analizini ön plana çıkarmaktadır.

IEC(1985) tarafından kritiklik ölçeği için bir örnek verilmiştir. Burada en ciddi seviye: "Birincil sistem fonkisyonlarının kaybına neden olabilen, sonuçta sistemde veya çevresinde hasarlar yaratabilecek ve/veya insanların hayatlarını veya uzuvlarını kaybetmelerine neden olabilecek olay" olarak tanımlanmıştır.

Daha detaylı bir analiz, daha kapsamlı olabilir. Sistem fazla sayıda bileşene sahip olabilir ve bu bileşenler farklı şekillerde etkisiz kalabilir. Örneğin; bir röle

15 farklı hata moduna sahip olabilir. Standart açıklamada (IEC 60812) 33 genel hata modu listelenmiştir.

FMECA, FMEA'yı genişleten bir analiz şeklidir, böylece tanımlanan her bir hata modu, önem ve kritikliğine göre sıralanabilir. FMEA analizi, genelde kalitatif ya da yarı kantitatiftir, ancak, gerçek hata oranlarını kullanarak kantitatif FMECA uygulanabilir.

FMEA'nın birtakım uygulamaları bulunmaktadır: Unsur ve ürünler için kullanılan Tasarım (ya da ürün) FMEA, sistemler için kullanılan Sistem FMEA, üretim ve montaj süreçleri için kullanılan Süreç FMEA, Hizmet FMEA ve Yazılım FMEA. FMEA/FMECA, fiziksel bir sistemin tasarımı, üretimi ve işleyişi esnasında uygulanabilir. Ancak, sistemi geliştirmek için değişiklikler genel olarak tasarım aşamasında daha kolay gerçekleştirilir. FMEA ve FMECA, ayrıca süreçler ve prosedürler üzerinde de uygulanabilir. Örneğin, sağlık hizmetlerindeki medikal hataları ve bakım prosedürlerindeki hataları tanımlamak için de kullanılabilmektedir. Hata Modu ve Etki Analizi teknigi aşağıda sıralanan şekilde bir çok çeşitliliğe sahiptir ve uygulama alanları her türlü üretim ve hizmet şeklini kapsamaktadır.

Tasarım FMEA: Potansiyel veya bilinen hata türlerini tanımlayan, ilk üretim gerçekleşmeden hataların tanımlanması ve düzeltici faaliyetlerin uygulanmasını sağlayan bir yöntemdir.

Proses FMEA: Tasarım FMEA ve müşteri tarafından tanımlanmış olan kalite, güvenilirlik, maliyet ve verimlilik kriterlerini sağlamak için mühendislik çözümleri üretmeyi hedefleyen bir yöntemdir.

Hizmet FMEA: Müşteri hizmetlerini geliştirmek amacıyla üretim, kalite güvence ve pazarlama koordinasyonu ile uygulanan bir yöntemdir

Sistem FMEA: Bütün donanımların ve tasarımın tamamlanmasının sonrasında üretim, kalite güvence gibi sistemlerin akışını en elverişli hale getirmek için kullanılan bir yöntemdir.

Yapılacak olan bir FMEA tekniği uygulaması aşağıda özetlenmiş olan fonksiyonların gerçekleştirilmesini sağlar;

- Proses ya da hizmette hataların oluşturacağı en küçük bir zararın bile oluşumunun engellenmesini sağlamak için hata türlerini sistematik olarak gözden geçirir,

- Proses ya da hizmeti ya da bunların fonksiyonelliğini etkileyebilecek her türlü hatayı ve bu hatanın etkilerini tanımlar,
- Tanımlanan bu hatalardan hangilerinin proses ya da hizmet operasyonlarında daha kritik etkilerinin olduğunu belirler, bu yüzden meydana gelebilecek en büyük hasarı ve hangi hata türünün bu hasarı üretebileceğini tanımlar,
- Montaj, montaj öncesinde, proseste hataların oluşum olasılığını ve bunun nereden kaynaklanabileceğini (dizayn, operasyon, vb.) belirler,
- Diğer kaynaklardan elde edilmesi mümkün olmayan hata oranlarını ve türlerini tanımlayarak gerekli muayene programlarının kurulmasını sağlar,
- Güvenilirliğin deneysel olarak test edilebilmesi için gerekli muayene programlarının kurulmasını sağlar,
- Bir ürün için değişikliklerin olabilecek etkilerini tanımlar,
- Yüksek riskli bileşenlerin nasıl güvenilir hale getirilebilecegini tanımlar,
- Montaj hatalarının olabilecek kötü etkisinin nasıl giderilebileceğini tanımlar.

Girdi:

FMEA ve FMECA, her bir unsur, ekipman, makine ya da proses parçasının başarı sağlayamadığı sistemlerinin analizleri için kullanılır. Bu analizi gerçekleştirmek için de, sistem unsurları hakkında detaylı bilgiye ihtiyaç duyar. Ayrıntılı bir Tasarım FMEA için söz konusu unsur ayrıntılı bağımsız bileşen düzeyinde olabilirken; yüksek düzeydeki Sistem FMEA için unsurlar, daha üst bir düzeyde tanımlanabilir. Bilgiler şunları içerebilir:

- Analiz edilen sistemi, bileşenlerini ya da süreç aşamalarını içeren bir akış diyagramı ya da çizimler,
- Bir sistem bileşeninin ya da sürecinin her bir aşamasının işlevinin kavranması,
- İşleyişi etkileyebilecek çevresel ve diğer parametrelerin ayrıntıları,
- Belirli arızalara yönelik sonuçların kavranması,

- Mümkün olan yerlerde verileri ve arıza oranını içeren, arızalar üzerindeki tarihsel bilgi.

Süreç:

FMEA süreci aşağıda gösterilmiştir:

- Çalışmanın kapsamı ve amaçları tanımlanır,
- Takım üyeleri çalışma için bir araya gelir,
- FMECA'e tabi olan sistem\sürec kavranmaya çalışılır,
- Sistemin bileşenlerinde ya da aşamalarında meydana gelebilecek hatalar tanımlanır,
- Her bileşenin ve aşamanın işlevi tanımlanır,
- Listelenen her bileşen ve aşama için tanımlama yapılır,
- Hatayı gidermek için, tasarımdaki doğal koşullar tanımlanır,
- Şu sorular takım üyeleri tarafından tartışılır;
  - Her bir bölümün hata yapma ihtimali mümkün müdür?
  - Hangi mekanizmalar arızanın bu modlarını üretebilir?
  - Eğer hata meydana gelir ise, hangi etkiler ortaya çıkabilir?
  - Hata zararlı mıdır, zararsız mıdır?
  - Hata nasıl ortaya çıkarılır?

FMECA için, çalışma grubu, tanımlanan hata modlarının her birini, kritikliklerine göre sınıflandırmaya devam eder. Bunun yapılabilmesi için bir takım yöntemler bulunmaktadır. Genel yöntemler aşağıda sunulmaktadır:

- Mod kritiklik endeksi,
- Risk seviyesi,
- Risk öncelik sayısı.

Model kritikliği, dikkate alınan modun sistemin bir bütün olarak arızalanması sonucunu doğuracağı ihtimaline karşı bir önlemdir:

Hata etkisi ihtimali * Mod arıza oranı* Sistemin işleyiş süresi

Bu, bahsedilen ifadelerin nicel olarak tanımladığı durumlarda ekipman hatalarına sık olarak uygulanır ve bütün hata modları aynı sonuca sahiptir.

Risk seviyesi, hata ihtimali ile meydana gelen bir hata modunun sonuçlarının birleştirilmesi ile elde edilir. Değişik hata modlarının farklılaştığı ve ekipman sistemlerine ya da süreçlerine uygulandığı zaman kullanılır. Risk seviyesi kantitatif olarak, yarı kantitatif olarak ya da kalitatif olarak ifade edilir.

Risk öncelik sayısı (RÖS), problemi ortaya çıkarma yetisi, hat ihtimali ya da hatanın sonucuna yönelik değerlendirme ölçeğine ait (genellikle 1 ve 10 arasında) sayıları çarparak elde edilen kritikliğe karşı yarı kantitatif bir önlemdir (eğer bir hatanın algılanması zor ise, daha fazla öncelik tanınır).

RÖS değeri P, S ve D değerlerinin çarpımıyla elde edilir.

RÖS = P(olasılık) x S(şiddet) x D(fark edilebilirlik)

P: Her bir zarar modunun oluşma olasılık değeri;

S: Zararın ne kadar önemli olduğunun değeri, şiddet, ciddiyet

D: Zarar meydana getirecek durumun keşfedilmesinin zorluk derecelendirilmesi,

RÖS: Risk öncelik sayısı

Hata modları ve mekanizmaları bir kez tanımlanır, düzeltici faaliyetler tanımlanabilir ve daha büyük hata modları için gerçekleştirilebilir.

FMEA analizi yardımıyla olası zarar meydana getirecek durumlar önceden sezilerek önlemler geliştirilir ve böylece olası zararların artış olasılığı giderilir.

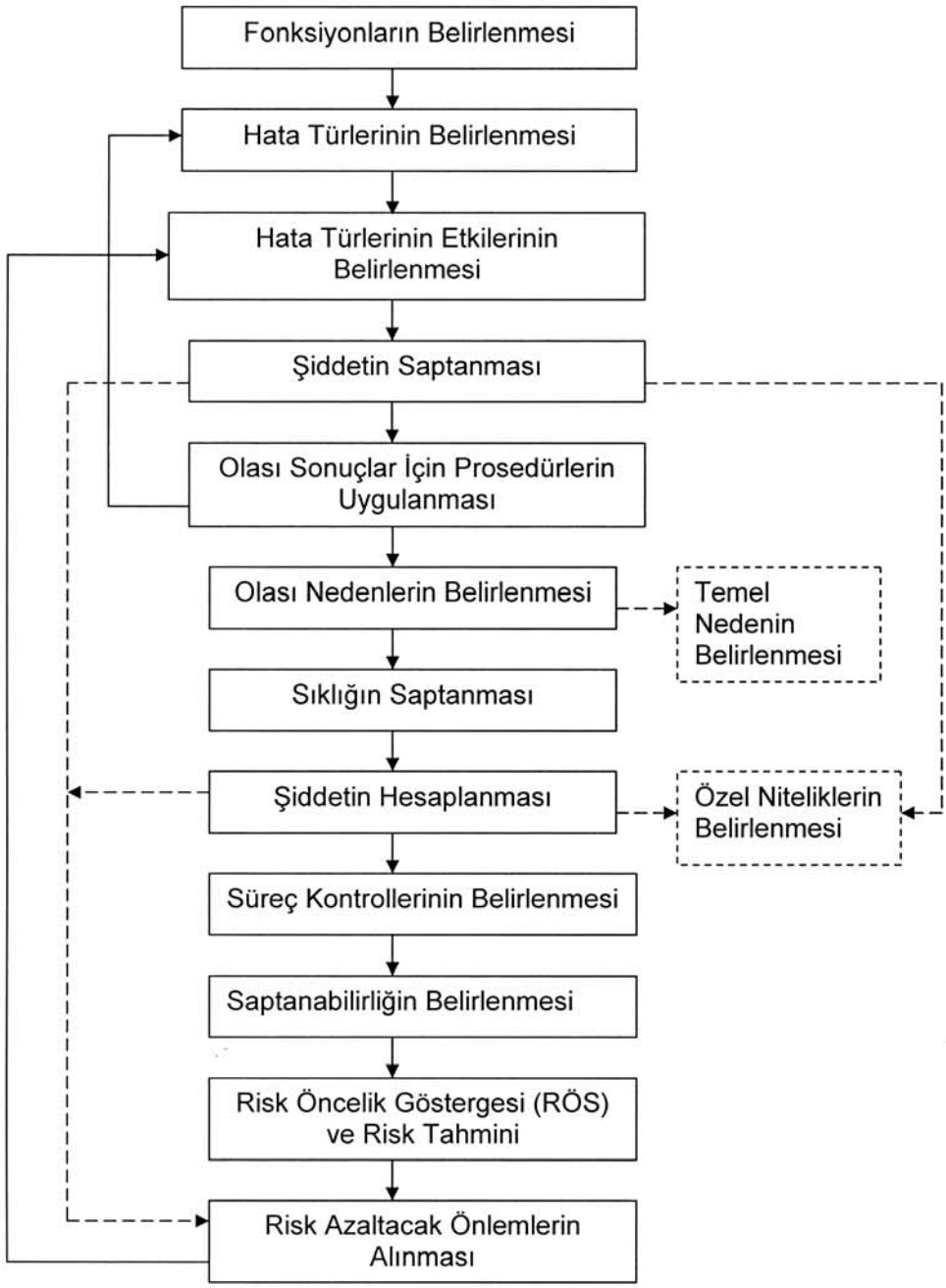
Bu metodda yukarıdaki tablodan da görüleceği üzere risk tablosuna "Olasılık" ve "Şiddet" kolonları yanında bir de “Farkedilebilirlik veya Keşfedilebilirlik” kolonu eklenmiştir. Bu bileşen özellikle başarısızlığın ne kadar tehlike yarattığının yanında, bir tehlikenin gizli kalmasının da ne kadar tehlike derecesini artıracağının da belirlenmesini sağlar.

Belgelendirme:

FMEA aşağıdakileri içeren bir raporda belgelendirilir:

- Analiz edilen sisteme ilişkin ayrıntılar,

Şekil 35: FMEA Prosesi



Tablo 42: Zararın Şiddeti (Ciddiyet)

Sistem OFMEA Şiddet Etki Sınıflaması		
Etki	**Şiddetin Etkisi**	**Derece**
Uyarısız Gelen Tehlike	Felakete yol açabilecek etkiye sahip ve uyarısız gelen potansiyel hata	**10**
Uyarısız Gelen Tehlike	Yüksek hasara ve toplu ölümlere yol açabilecek etkiye sahip ve uyarısız gelen potansiyel hata	**9**
Çok Yüksek	Sistemin tamamen hasar görmesini sağlayan yıkıcı etkiye sahip ağır yaralanmalara, 3. derece yanık, akut ölüm vb. etkiye sahip hata türü	**8**
Yüksek	Ekipmanın tamamen hasar görmesine sebeb olan ve ölüme, zehirlenme, 3. derece yanık, akut ölümcül hastalık vb. etkiye sahip hata	**7**
Orta	Sistemin performansını etkileyen, uzuv ve organ kaybı, ağır yaralanma, kanser vb. yol açan hata	**6**
Düşük	Kırık, kalıcı küçük iş göremezlik, 2. derece yanık, beyin sarsıntısı vb. etkiye sahip hata	**5**
Çok Düşük	İncinme, küçük kesik ve sıyrıklar, ezilmeler vb. hafif yaralanmalar ile kısa süreli rahatsızlıklara neden olan hata	**4**
Küçük	Sistemin çalışmasında yavaşlatan hata	**3**
Çok Küçük	Sistemin çalışmasında kargaşaya yol açan hata	**2**
Yok	Etki Yok	**1**

Tablo 43: Zararın Oluşma Olasılığı

Hata Olasılığı	Hatanın İhtimali	Derece
Çok Yüksek: Kaçınılmaz Hata	>1 / 2	**10**
	1 / 3	**9**
Yüksek: Tekrar Tekrar Hata	1/ 8	**8**
	1 / 20	**7**
Orta: Ara Sıra Olan Hata	1 / 80	**6**
	1 / 400	**5**
	1 / 2,000	**4**
Düşük: Nispeten Az Olan Hata	1 / 15,000	**3**
	1 / 150,000	**2**
Pek Az:Olası Olmayan Hata	<1 / 1,000,000	**1**

Tablo 44: Fark Edilebilirlik

Farkedilebilirlik	Farkedilebilirlik Olasılığı	Derece
Fark Edilemez	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği mümkün değil	**10**
Çok Az	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği çok uzak	**9**
Az	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği uzak	**8**
Çok Düşük	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği düşük	**7**
Düşük	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği çok düşük	**6**
Orta	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği orta	**5**
Yüksek Ortalama	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği yüksek ortalama	**4**
Yüksek	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği yüksek	**3**
Çok Yüksek	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği çok yüksek	**2**
Hemen hemen Kesin	Potansiyel hatanın nedeninin ve takip eden hatanın keşfedebilirliği hemen hemen kesin	**1**

- Uygulamanın nasıl gerçekleştirildiği,
- Analizde yapılan varsayımlar,
- Veri kaynakları,
- Tamamlanmış analiz cetvelini içeren sonuçlar,
- Tanımlama için kullanılan yöntem bilimi ve kritiklik (eğer tamamlanmışsa),
- Test planları, vb. bünyesinde bulunan daha fazla analiz, tasarım değişikliği ya da özelliklerine yönelik herhangi bir tavsiye.

Sistem, faaliyetler tamamlandıktan sonra, başka bir FMEA takımı tarafından yeniden değerlendirilebilir.

Sonuçlar:

FMEA'in başlıca sonucu, sürecin ya da sistemin her bir aşamasına veya bileşenine yönelik hata modlarının, hata mekanizmalarının ve etkilerinin bir lis-

tesidir (hata ihtimalindeki bilgileri de içerir).

Bilgiler, ayrıca, başarısızlık nedenleri ve bütünüyle sisteme getirdiği sonuçlar şeklinde de verilir. FMECA'den gelen sonuç, sistemin başarısız olacağı ihtimaline, hata modundan ya da risk seviyesinin kombinasyonundan doğan risk seviyesine ve hata modunun algılanabilirliğine dayalı bilgi sınıflandırmasını içerir. Eğer veri bankası olarak kalitatif sonuçlar kullanılmış ise, FMECA ancak kalitatif sonuç verebilir.

Güçlü Yönler ve Sınırlılıklar:

FMEA/FMECA'nın güçlü yönleri aşağıda gösterilmiştir:

- İnsan, ekipman ve sistem hata modları ile yazılım, donanım ve prosedürlere büyük ölçüde uygulanabilir,
- Bileşen hata modlarını, nedenlerini ve sisteme olan etkilerini tanımlar ve bunları kolayca okunabilir bir formatta sunar,
- Tasarım sürecindeki problemleri erken tanımlayarak kullanılır durumda olan maliyetli ekipman değişikliği ihtiyacından kaçınılmasını sağlar,
- Güvenlik sistemine yönelik gereklilikleri ve tek nokta hata modlarını tanımlar,
- Gözlemlenen kilit özellikleri belirginleştirerek gelişim kontrol programlarına yönelik girdi sağlar,

Sınırlılıklar aşağıdakileri içermektedir:

- Hata modlarının kombinasyonlarını tanımlamak için değil, sadece tek tek hata modlarını tanımlamak için kullanılabilir,
- Karışık çok iç içe geçmiş sistemler için uygulaması zor ve meşakkatli olabilir.

Bu ölçülere göre analizler yapılır ve sonuçlar risk tablosuna kaydedilir. Sonuçta kritiklik önceliği ortaya çıkarılır ve kritiklik önceliğine gore aksiyon planları geliştirilmeye çalışılır. RÖS katsayısının en büyük değerinden başlanarak önlemlerin alınmasına çalışılır, çünkü en büyük zararlar RÖS'nın en büyük değerlerine isabet etmektedir. FMEA metodu ile gerçekleştirilen bir çalışma çok yararlıdır, çünkü sistemin içindeki aksaklıkların neler olduğu ve sistemin çalışması hakkında bilgi sağlanır. Analist, sistematik yaklaşımdan dolayı sistemin nasıl çalıştığını daha iyi anlama hususunda daha iyi bilgi sahibi olur.

Tablo 45: Örnek FMEA Analizi

Tarih :	01.11.2013	Hata Modu ve Etkileri Analizi (FMEA)	FMEA Tipi:	Risk Değerlendirme
Proses/Sistem :	Fırın		FMEA No:	5
Alt Sistem :	Propan Tankı		Düzenleyen:	İG Uzmanı
Bileşen:			FMEA Tarihi:	01.11.2013
Dizayn Rehberi:			Revizyon Tarihi:	
FMEA Takımı:	Fabrika Müdürü, İş Güvenliği Uzmanı, Bakım Amiri, İşletme Müh., Elektrik Müh.		Sayfa:	1

Sistem /Parça	Potansiyel Hata Türleri	Hatanın Sonuçları	S	Hataların Nedenleri	P	Kontrol Önlemleri	D	RÖS	Tavsiye Edilen İyileştirmeler/ Eylemler	Sorumlu & Tamamlama Tarihi	Hareket Sonucu				
											Hareket Tarihi	Yeni (S)	Yeni (P)	Yeni (D)	Yeni RÖS
Valf 1 (propan enjeksiyonu esnasında sıcaklık kontrolü)	Valf bloke, açılmıyor	Patlama	8	Bakım prosedürü oluşturulmamış	4	Sıcaklık alarmı ve basınç alarmı kontrolü	3	96		Bakım Amiri, 1.11.2013	13.11.2013	8	2	1	16
	Valf bloke, açılmıyor	Fırında basınç ve sıcaklık artışı	7	Bakım prosedürü oluşturulmamış	4	Sıcaklık alarmı ve basınç alarmı kontrolü	2	56	Bakım prosedürünün gözden geçirilmesi, opetratör eğitimi	Bakım Amiri, 1.11.2013	13.11.2013	7	2	1	14
	Valf bloke, kapanmıyor	Fırında sıcaklık düşüşü, ekonomik kayıp	3	Bakım prosedürü yetersiz	4	Sıcaklık alarmı ve basınç alarmı kontrolü	1	12	Bakım prosedürünün gözden geçirilmesi, opetratör eğitimi	Bakım Amiri, 1.11.2013	01.12.2013	3	2	1	6
Propan Tankı	Propan sızıntısı	Patlama riski	10	Tanka veya ekipmanına çarpma	4	Tankın etrafını çevirilmesi ve tanka yakın araç park ettirilmemesi	3	120	Tankın etrafının tel örgü ile çevrilmesi kapısına kilit takılması, park mesafesi bırakılması	İSG Mühendisi 1.11.2013	13.11.2013	10	2	2	40
	Propan sızıntısı	Yangın riski	7	propan alarmı veya tankın basınç alarm sisteminin olmaması	5	Propan seviyesinin kontrolü ve sızıntının tespiti	2	70	Propan dedektörü ve tank basınç alarmı kurulması	İSG Mühendisi 1.11.2013	20.12.2013	7	2	1	14
ONAY: İMZA:															

11.18. Olay Ağacı Analizi (Event Tree Analysis - ETA) :

Olay ağacı analizi, hata sonuçları önemli olan ve bu sonuçların hafifletilmesi istenilen çeşitli sistemlerin işleyişi/ işlemeyişine göre hazırlanan, basit olasılık hesaplamalarına yönelik grafiksel bir tekniktir. Bu analiz için birçok yöntem problemlerin ve hataların tanımlanması ve bunların nasıl düzeltileceğinin etrafında şekillenir.

Bu yaklaşımda sistemin güvenlik özellikleri direkt olarak incelenir ve değerlendirilir. Bunun birtakım potansiyel faydaları olur. Örneğin:

- Güvenlik fonksiyonları (hem teknik hem organizasyonel) başlangıçtan itibaren uygun olarak tasarlanmamış olabilir,
- Sistemin güvenlik karakteristiğine ilişkin kapsamlı bir tanımlama gerekli olabilir,(örneğin; özellikle kritik sistemler için, yangın söndürme sistemleri, güç sistemleri vb.),
- Destek, tasarım spesifikasyonlarına ve sistemler ve sorumluluklar arasındaki bağlantıların netleştirilmesi gerekebilir,
- Güvenlik fonksiyonların verimli ve kapsamlı olup olmaması değerlendirilir. (Sistem yeterince güvenli midir?)

Olay Ağacı analizi, başlangıçta seçilmiş olan olayın meydana gelmesinden sonra ortaya çıkabilecek sonuçların akışını diyagram ile gösterir. Tetikleyici bir olayı takip eden olaylar silsilesinin yayılarak, tetiklemeli olay sonrasında sistem bileşenlerinin ve işlevlerinin nasıl etkilediğini, ağırlaştırıcı ya da hafifletici olayları gösterir. ETA, hem kalitatif hem de kantitatif olarak uygulanabilir.

Olay Ağacı analizi nükleer endüstride daha çok uygulama görmüştür ve nükleer enerji santrallerinde işletilebilme analizi olarak yoğun kullanım alanına sahip olmuştur. Büyük Endüstriyel Kazaların Önlenmesi ve Etkilerinin Azaltılması Hakkında Yönetmelik (Seveso-COMAH Direktifi) kapsamında olan kimya fabrikalarında da mevcut proses bileşenlerinin ve güvenlik sistemlerinin hata olasılıklarının belirlenmesinde ve ortaya çıkacak sonuçların vehametinin tespitinde de sıklıkla kullanılmaktadır. Hata ağacı analizinden farklı olarak bu metodoloji tümevarımlı mantığı kullanır. Kaza öncesi ve kaza sonrası durumları gösterdiğinden sonuç analizinde kullanılan başlıca tekniktir. Diyagramın sol tarafı başlangıç olay ile bağlanır, sağ taraf fabrikadaki/işletmedeki hasar durumu ile bağlanır, diyagramın en üst kısmı ise sistemi tanımlar. Eğer sistem başarılı ise yol yukarı, başarısız ise aşağı doğru gider.

Olay Ağacı Analizinde kullanılan mantık, hata ağacı analizinde kullanılan mantığın tersinedir. Bu metod; sürekli çalışan sistemlerde veya "standby" modunda olan sistemlerde kullanılabilir.

Sisteme meydan okumaya karşı sistemin cevebının keşfi ve sistemin başarı/hata olasılık değerlendirmesi yapılır.

Örnek "Meydan Okuma/Tetikleyici Olay";

- Tankın boru hattında patlama,
- Depolanmış yanıcı malzemenin tutuşması,
- Sistem hatası,
- Teknoloji ihtiyacı,
- Normal sistem işletme komutları,
- Yükseltilmiş ticari rekabet,
- İstenmeyen zincirleme olayların meydana gelmesi.

ETA, sisteme meydan okumayı/tetiklemeli olayı takip eden farklı kaza senaryolarını biçimlendirme, hesaplama ve sıralama için kullanılabilir. ETA, bir durum ya da sürecin kullanım süresindeki herhangi bir aşamasında rahatlıkla kullanılabilir. ETA, tetiklemeli bir olayı takip eden olaylar silsilesi ve potansiyel senaryolar hakkında beyin fırtınası yapmaya yardım etmesi için kalitatif olarak kullanılabilir.

ETA, kayıp getirebilecek sisteme meydan okumayı/tetikleme olaylarını modellemek için de kullanılabilir. Ayrıca, Seveso Direktifinin istediği üzere kaza sonuçlarının, çeşitli uygulamalar ile engeller ya da istenmeyen sonuçları hafifletme eğiliminde olan kontrollerin nasıl etkilendiği hakkında fikir sahibi olunması için de kantitatif olarak kullanılabilir. Kantitatif analiz, kontrollerin (bariyerler) kabul edilebilirliğinin belirlenmesine yardımcı olur. Birçok kontrolün (bariyer) bulunduğu yerlerdeki hataları modellemek için de sıklıkla kullanılır.

Ancak, kök nedenlerin belirlenmesine yönelik koşulların araştırıldığı durumlarda, sıklıkla hata ağacı (FTA) kullanılarak modellenir.

Girdi:

Girdiler aşağıdakileri içermektedir:

- Uygun sisteme meydan okuma/tetikleme olayların bir listesi,
- Uygulama, engeller ve kontrollere yönelik bilgi ve bunların hata olasılıkları (kantitatif analizler için);

- Bir arızanın tırmanması ile süreçlerin kavranması.

Güçlü Yönler ve Sınırlılıklar:

ETA'nın güçlü yönleri aşağıda gösterilmiştir:

- ETA, analiz edilen bir tetiklemeyici vakayı takip eden potansiyel senaryoları ve hafifletici sistem ya da işlevlerin hatasının ya da başarısının etkisini, anlaşılır ve şematik olarak gösterir,
- Hata ağaçlarında modelleme yapmaya elverişsiz olan domino etkileri, bağlılık ve zamanlamaya yönelik açıklama getirir,
- Hata ağaçları kullanıldığında, gösterilmesi mümkün olmayan olaylar silsilesi grafiksel olarak gösterilebilir.

Sınırlılıklar aşağıdakileri içermektedir:

- ETA'yı kapsamlı değerlendirmenin bir parçası olarak kullanmak amacı ile bütün potansiyel tetikleme olayların tanımlanması gerekmektedir. Bu ancak başka bir analiz yöntemi kullanılarak yapılabilir (örn. HAZOP, PHA), ancak noksan olan bazı tetikleyici olaylar için her zaman bir potansiyel vardır,
- Olay ağaçları ile bir sistemin yalnızca başarı ve hata durumları üzerinde durulur, gecikmeli başarı/hata ya da sistemi kurtarma (ya da geriye getirme) sonrası başarı/hata olaylarını dahil etmek zordur,
- Bu yöntem, yol boyunca sapma noktasında meydana gelen olaylara bağlıdır. Ancak, genel bileşenler, hizmet sistemleri ve operatörler gibi bazı bağlılıklar, eğer dikkatli bir şekilde ele alınmaz ise, göz ardı edilebilir ve riskin iyimser tahminlerine neden olabilir.

Olay Ağacı Analizi aşamaları:

Olay ağacı analizi süreci aşağıda gösterilmiştir;

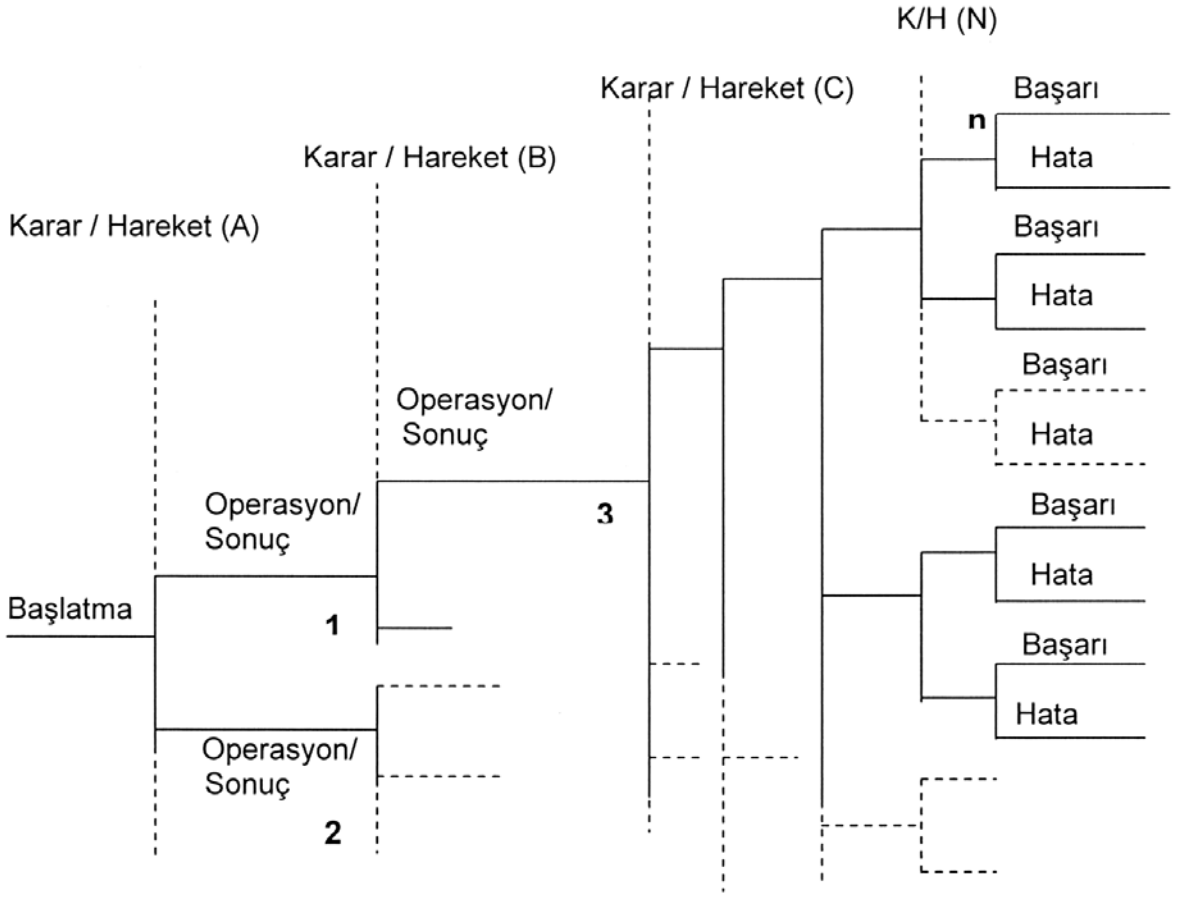
- Bir olay ağacı, herhangi bir tetikleme olayının (meydan okuma) seçilmesi ile başlar,
- Bu, bir toz patlaması gibi bir özel durum ya da doğal bir olay sonucu güç kesintisi olabilir,
- Sonuçları hafifletmek için mevcut olan sistemler ya da işlevler, daha sonra sırası ile listelenir,

- Her bir işlev ya da sistemin başarısını ya da arızasını göstermek için bir çizgi çizilir,
- Hatanın/Arızanın özel bir olasılığı, örneğin geçmiş bakım verisi ya da bir hata ağacı analizi tarafından tahmin edilen koşullu olasılığı ile her bir çizgiye olasılık verillir,
- Sistem içindeki tüm güvenilir operasyonal değişimler tanımlanır. Her bir yol takip edildiğinde nihai başarı veya hataya götürür,
- Bu şekilde, ön olaydan gelen farklı yollar koşullu olasılıklardır, örneğin; yangın söndürücünün işleyiş olasılığı, normal şartlar altında yapılan testlerden elde edilen olasılık değil, patlamanın sebep olduğu yangın şartları altındaki işleyiş olasılığıdır,
- Ağacın bütünündeki her bir yol, bu yoldaki bütün olayların meydana gelme olasılığını gösterir,
- Bu nedenle her bir sonucun olasılığı, bağımsız ve şarta bağlı olasılıkların bir ürünü şeklinde temsil edilir.

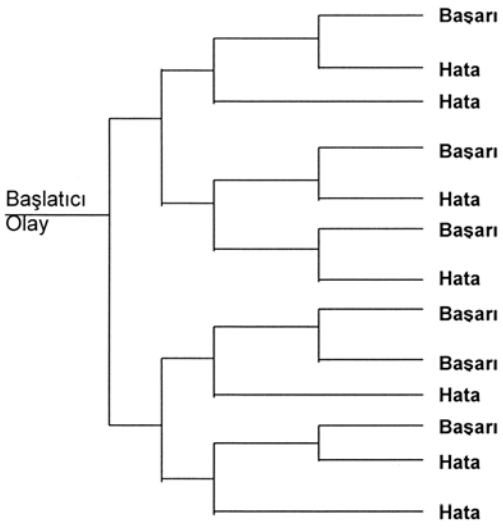
Olay Ağacı Analizi (Bernoulli Modeli);

Sistem, davranışını temsil eden basit ağaca indirgenir. İkili dal kullanılır. Final çıktıları geri döndürülemez hatalar ve hiç yenilgisiz başarılara direk olarak götürür. Bir hata ağacı veya diğer analizler, başlangıç olayın veya koşulun olasılığını belirler.

Şekil 36: Olay Ağacı Genel Durum

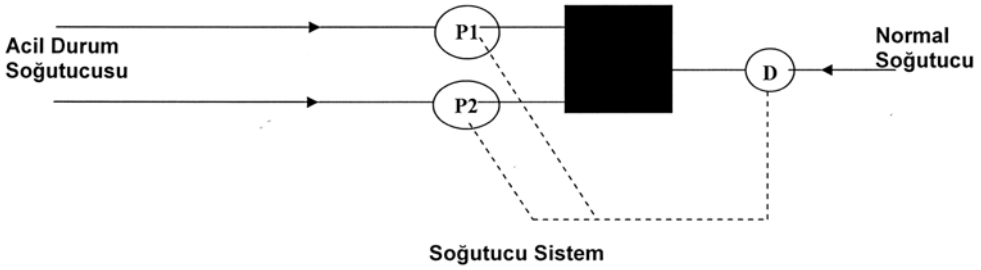


Şekil 37: Bernoulli Modeli

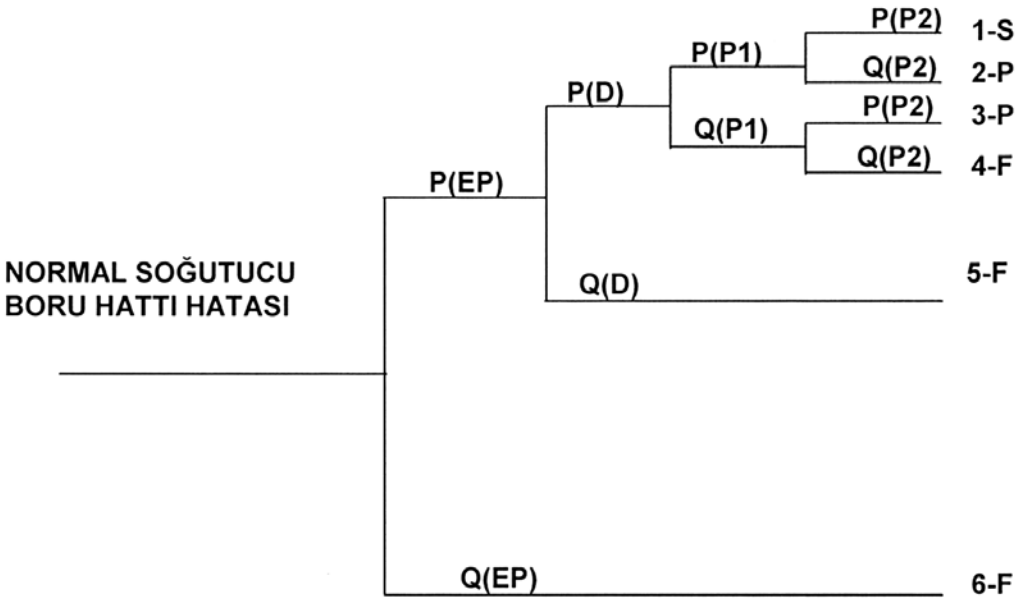


Olay Ağacı Analizini daha iyi kavrayabilmek maksadıyla aşağıdaki örnekler verilmiştir.

Örnek1- Soğutucu Sistem (standby çalışan sistem)



- P1 ve P2 elektrikli yürütücü pompa, D akış dedektörü ve EP (şekilde gözükmüyor) de elektrik gücüdür.
- Başlatıcı olay, normal soğutucu boru hattındaki kırılmadır
- Tüm sistemin başarısı (S) iki pompanın her ikisinin de işlemesini gerektirir
- Kısmi başarı (P) içinde, bir pompanın çalışma sonucu
- Sistem Hataları içinde (F), İki pompa kusuru veya elektrik güç kaynağı hatası (EP) sonuçları değerlendirilir ve Olay Ağacı oluşturulur.



P(.) – Parçanın Başarı Olasılığı

Q(.) – Parçanın Hata Olasılığı

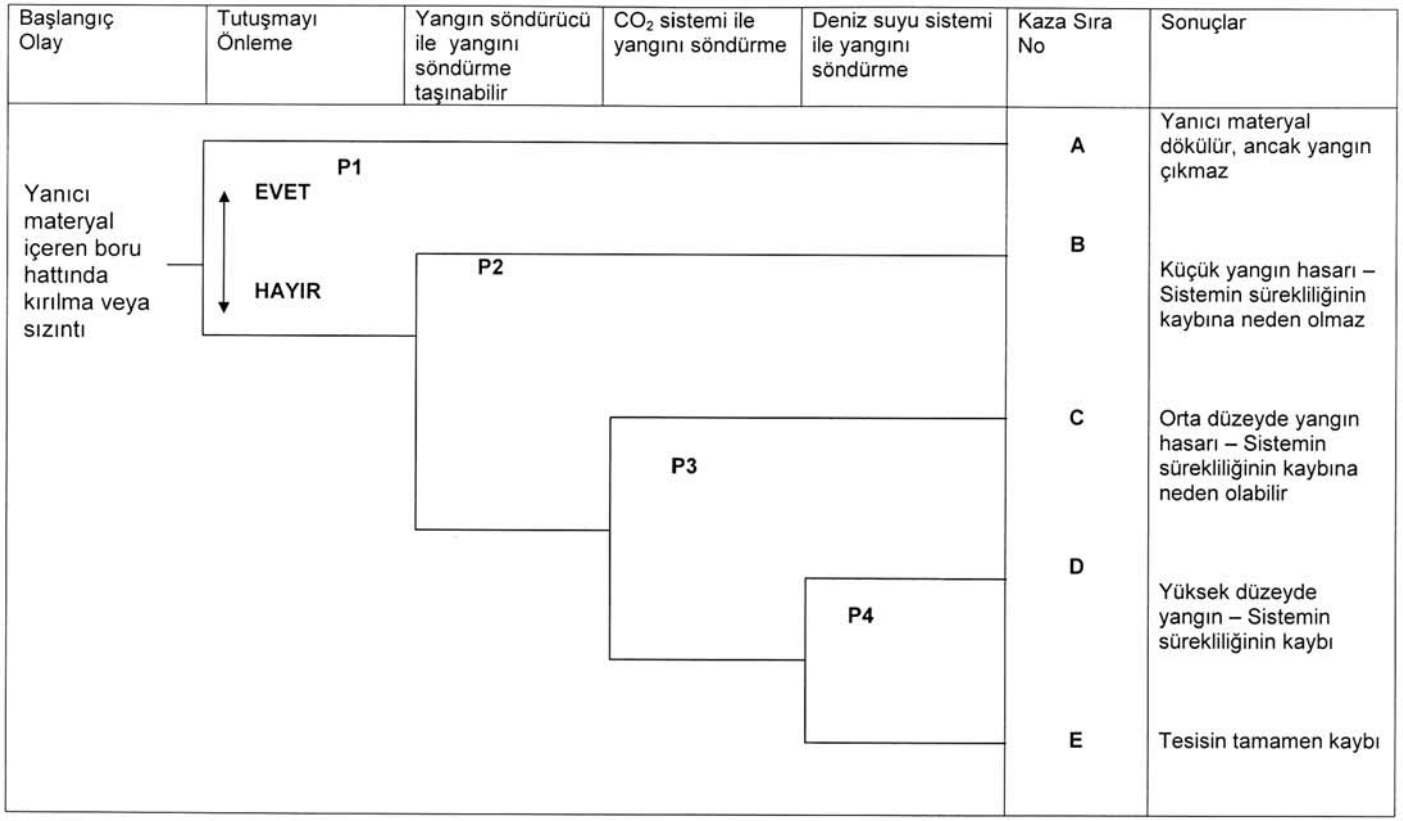
S – Tüm Sistemin Başarısı

P– Sistemin Ksmi Başarısı

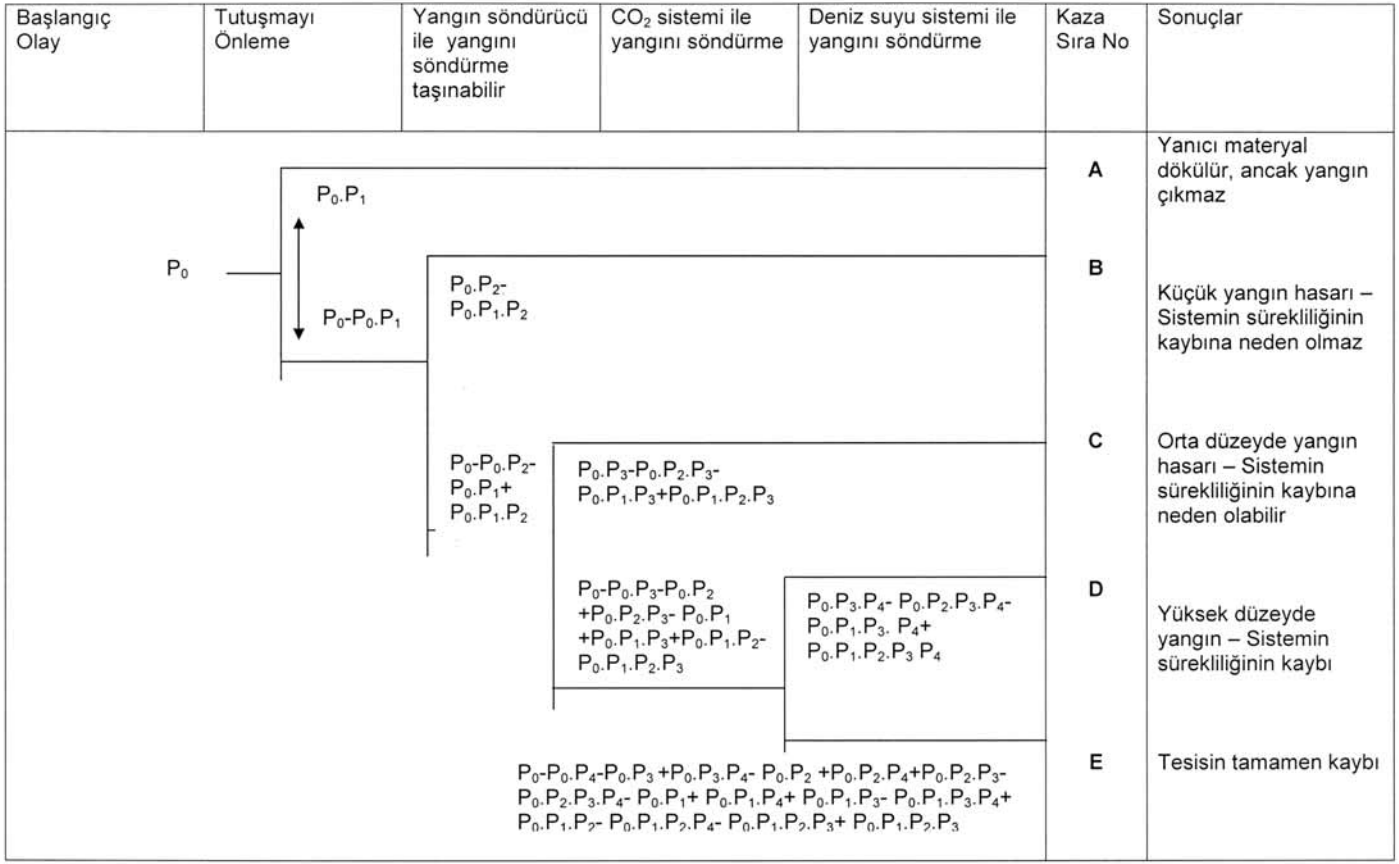
F– Sistem Hatası

Örnek 2- Aşağıdaki örnekte verilen Olay Ağacı, bir akaryakıt tankının boru hattındaki kırılma veya sızıntıdan sonra meydana gelebilecek çeşitli sonuçları gösterir. İlk dal iki potansiyel yolu, hava koşullarına bağlı veya bağlı olmamak üzere ateş kaynağıyla temas ile yangının başlamasını gösterir. Eğer kazara dökülen yanıcı malzeme tutuşursa, yangını söndürmek üzere üç sistem mevcuttur; bunlar: taşınabilir yangın söndürücüler, CO_2 sistemi ve deniz suyu sistemi. Ard arda dal noktaları, her bir sistemin başarısını veya başarısızlığını tarif eder. Dikkat edilecek nokta ise; üst dal herbir durum için doğrudan sonuça uzanır, çünkü yangının sönmesi halinde diğer sistemlerin işletilmesine gerek kalmaz.

Şekil 38: Yanıcı Materyalin Sızması veya Boru Hattının Kırılması Olay Ağacı Analizi



Şekil 39: Yanıcı Materyalin Sızması veya Boru Hattının Kırılması Olay Ağacı Olasılık Analizi



11.18.1. Olay Ağacından Hata Ağacına Transformasyon

Sisteme meydan okuyan bir olaya karşı sistemin cevabının ve başarı/hata değerlendirmesinin yapıldığı Olay Ağacı diyagramından hata ağacı diyagramına kolaylıkla transformasyon yapılabilir. Böylelikle final çıktılarından elde edilmiş olan geridönülemez hataların esas olaylarının değerlendirmesi ve eşit hata ağacının belirlenmesi sağlanır.

Sonuçlar:

ETA'dan gelen sonuçlar aşağıdakileri içermektedir:

- Potansiyel problemlerin, tetikleme olay sonucunda ortaya çıkarabileceği çeşitli sonuçlar veya sonuç silsileleri, üretilen olayların kombinasyonları olarak kalitatif bir şekilde tarif edilmesi,
- Yardımcı sistemlerin çeşitli hata silsilelerine ilişkin bağıl öneminin ve olay sıklıklarının ya da olasılıklarının tahminleri,
- Riskleri azaltmaya yönelik önerilerin listeleri,
- Sistem parçalarının verimliliğinin kantitatif değerlendirmeleri.

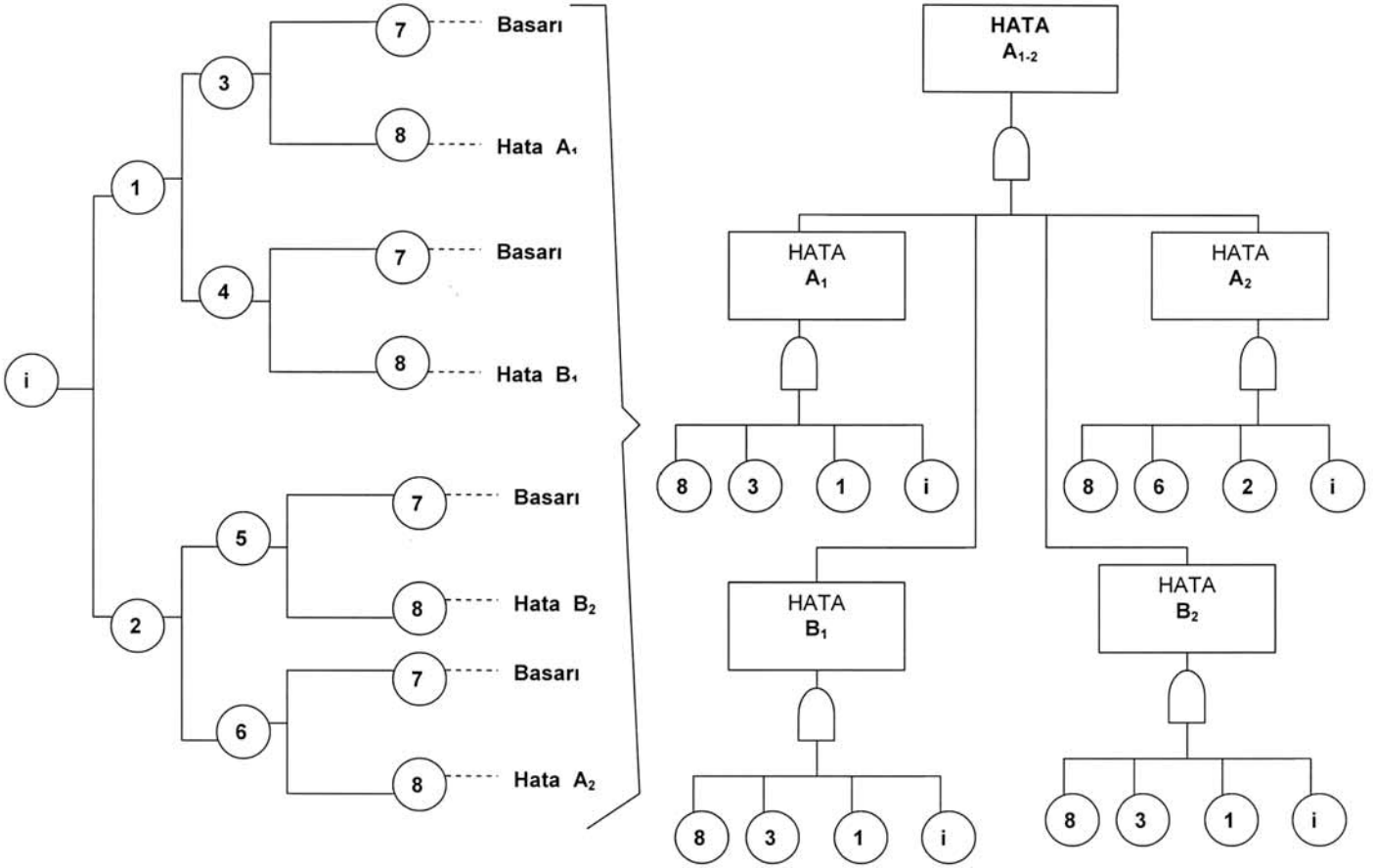
11.19. Neden – Sonuç Analizi (Cause-Consequence Analysis)

Neden sonuç analizi, hata ağacı ve olay ağacı analizinin bir birleşimidir. Tetikleyici olayın (meydan okuma) sonuçlarını hafifletmek amacı ile tasarlanan sistemlerin hatalarını ya da oluşabilecek koşulları gösteren EVET/HAYIR mantık geçitleri aracılığıyla yapılan bir analizden ibarettir. Koşulların ve hataların nedenleri, hata ağaçları aracılığıyla analiz edilir.

Bu teknik nükleer enerji santrallerinin risk analizinde kullanılmak üzere Danimarka RISO labaratuvarlarında yaratılmıştır. Ancak, diğer endüstrilerin sistemlerinin güvenlik düzeyinin belirlenmesi için de adapte edilebilir. Bu metodoloji, neden analizi ile sonuç analizini birleştirir ve bu nedenle de hem tümdengelimli hemde tümevarımlı bir analiz yöntemi kullanır. Neden - Sonuç analizinin amacı, olaylar arasındaki zinciri tanımlarken istenilmeyen sonuçların nelerden meydana geldiğini belirlemektir. Neden - Sonuç diyagramındaki çeşitli olayların olasılığı ile, çeşitli sonuçların olasılıkları hesaplanabilir. Böylece sistemin risk düzeyi belirlenmiş olur. Tipik bir Neden - Sonuç analizi diyagramı Şekil 39'da gösterilmiştir.

Neden - sonuç analizi, sistem hatalarının daha kapsamlı bir şekilde kavranmasını sağlamak amacıyla, başlangıçta, kritik güvenlik sistemleri için güvenilir bir araç olarak geliştirilmiştir. Hata ağacı analizleri gibi, bir kritik olaya sebebiyet veren hata mantığını göstermek için kullanılır. Yöntem, diğer ağaç diyagramlarında inceleme imkanı bulunmayan gecikmeli olayların ya da başarısızlıkların da

Şekil 40: Olay Ağacından Hata Ağacına Transmisyon

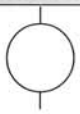


ağaç yapıları ile incelenmesini mümkün kılar ve sonuç analizlerine dahil olmasına olanak sağlar.

Yöntem, kritik bir olayı takiben ve belirli alt sistemlere (acil durum müdahalesi sistemleri gibi) bağlı olarak, bir sistemin geçebileceği çeşitli yolları analiz etmek için kullanılır. Kritik bir olayı takip eden farklı muhtemel sonuçların olasılık tahminini de verir.

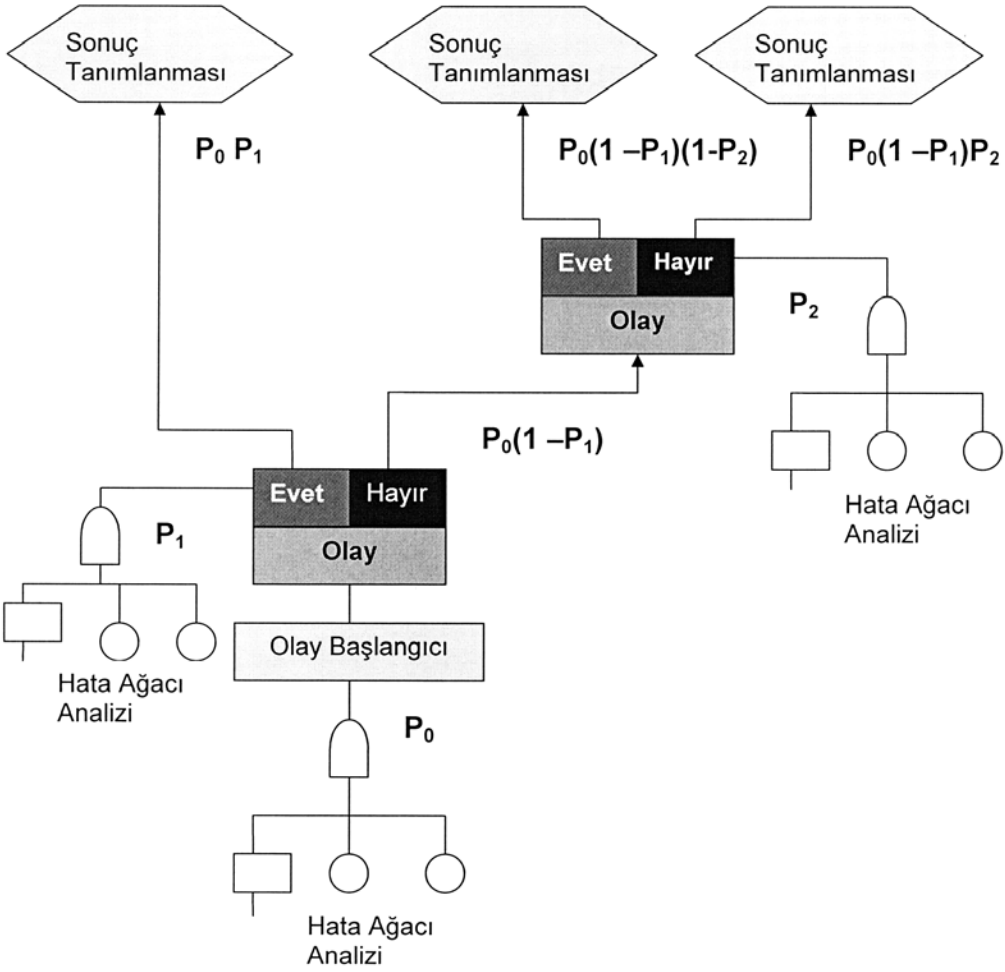
Neden-sonuç grafiğindeki her bir sıra alt hata ağaçlarının bir birleşimi olduğu için, neden-sonuç analizi büyük hata ağaçlarını geliştirmek için bir araç olarak kullanılabilir.

SEMBOLLER:

OLAYLAR	ANLAMI
 DAİRE	Esas olay (Yaprak, başlatan olay). Bu sembol birincil durumdaki problem için kullanılır. Daha ileri bir gelişimi gerektirmeyen, işleme gerek duyulmayan temel bir olaydır.
 VE KAPISI	Sadece sembol altındaki tüm girdi olayların gerçekleşmesi durumunda yukarıda yer alan olayın ortaya çıkması gerçekleşir.
 VEYA KAPISI	Sembol altındaki bir veya birden fazla girdi olaydan en az herhangi birinin gerçekleşmesi durumunda yukarıda yer alan olayın ortaya çıkması gerçekleşir.
 SONUÇ TANIMLAYICI	Hata seviyesini belirten son olay veya koşul

 DALLANDIRMA OPERATÖRÜ	Eğer koşullar uygusa çıktı "EVET" 'dir, eğer koşullar uygun değilse çıktı "HAYIR" 'dır. Dallandırma operatörüne kusur ve başarı ifadelerinden her ikisi de yazılabilir. $P_Y + P_N = 1$

Şekil 41: Tipik Bir Neden – Sonuç Temelli Risk Metedolojisi Akış Diyagramı



Başlatıcı Olayın Olasılığı;

$\mathbf{P_0} = (P_0.P_1) + P_0(1-P_1)(1-P_2) + P_0(1-P_1)P_2$

Girdi:

Sistemin hata modlarının ve hata senaryolarının kavranması gereklidir.

Süreç:

Prosedür aşağıda gösterilmiştir;

- Kritik (ya da tetiklemeli) olay tanımlanır (bir hata ağacının üst olayına ve bir olay ağacının tetiklemeli olayına eşdeğer olan),
- Hata ağacı analizinda tarif edildiği gibi, tetiklemeli olayın nedenleri için hata ağacı geliştirilir ve onaylanır. Geleneksel hata ağacı analizinde kullanılan sembollerin aynıları kullanılır,
- Şartların dikkate alınma sırası belirlenir. Bu, olayların oluşum sıralamasını takip edecek mantıksal bir sıra izlemelidir,
- Farklı koşullara bağlı olarak, sonuçlar için yollar inşa edilir. Yollar olay ağacına benzer şekilde çizilir, ancak, olay ağacındaki bölünme, ilgili özel durum ile etiketlenen bir kutu halinde gösterilir,
- Her bir durum kutusuna yönelik hatalar bağımsız ise, her sonuç olasılığı hesaplanabilir. Bu, ilk önce olasılıkları durum kutusunun tüm çıkışlarına vererek gerçekleştirilir (ilgili hata ağaçlarını uygun bir şekilde kullanarak). Özel bir sonuca sebebiyet veren herhangi bir sıranın olasılığı, bu özel sonuçta sona eren durumların her sıra olasılıklarının çarpımı sonucu elde edilir. Eğer birden çok sıra, aynı sonuç ile sona erer ise, her sıradan gelen olasılıklar eklenir. Eğer bir sıradaki durumların hataları arasında bağımlılıklar var ise (örneğin, bir güç arızasının, birçok koşulun gerçekleşmemesine neden olması), o zaman bağımlılıklar, hesaplamadan önce ele alınmalıdır.

Neden – Sonuç Analizinin Avantajları:

- Neden-sonuç analizinin avantajları, birleştirilen hata ağaçları ve olay ağaçları ile aynıdır. Ayrıca, zamanla gelişen olayları analiz edebilmesiyle, bu tekniklerin bazı sınırlamalarının üstesinden gelir,
- Neden-sonuç analizi sisteme kapsamlı bir bakış getirir,
- Neden – Sonuç analizi " en kötü durum" sonucuna göre hataların belirlenmesi ile sınırlandırılmamıştır, daha az tutucudur ve imkân dâhilinde daha gerçekçidir,
- Son olayın tahmin edilmesine ihtiyaç yoktur,
- Çoklu yanlışların ve hataların var olduğu sistemlerin değerlendirilmesine olanak sağlar,
- Olayların zaman sıralaması dikkatle gözden geçirilir,
- Uygun sistem işlemlerinin sonuçlarının olasılığı belirlenebilir, kayıpların derecelendirmesi yapılabilir. O nedenle, kısmi başarıların veya hataların dereceleri belirlenebilir,
- Sistemin maruz kaldığı, potansiyel tek-nokta hatalar veya başarılar değerlendirilebilir.

Limitleri:

- Analistlerin sistemde meydana gelebilecek değişikleri önceden tahmin etmesini geretirir,
- Operasyonun aşamalarının analistler tarafından önceden analiz edilmesi gerekir,
- Sonucun şiddetinin belirlenmesi subjektif olabilir ve analist için savunması zor olabilir,
- Başlatıcı meydan okuma/tetikleyici olay neden sonuç analizi ile belirlenemeyebilir, bu nedenle farklı risk değerlendirme teknikleri ile kullanım gerektirebilir (Örn; Proses FMEA, HAZOP, What If?, PHA vb..)
- Hem diyagramı oluşturma, hem de olasılık belirleme açısından hata ağacı ve olay ağacı analizinden daha karmaşıktır.

Sonuç:

Neden-sonuç analizi, bir sistemin hata nedenleri ile bu hataların sonuçlarını gösteren aynı zamanda da sistemin nasıl başarısız olduğunun grafiksel bir tasvirini yapan bir analiz türüdür. Kritik olayı takip eden özel durumların meydana gelme olasılığına dayalı her potansiyel sonucun meydana gelme olasılığının tahminidir.

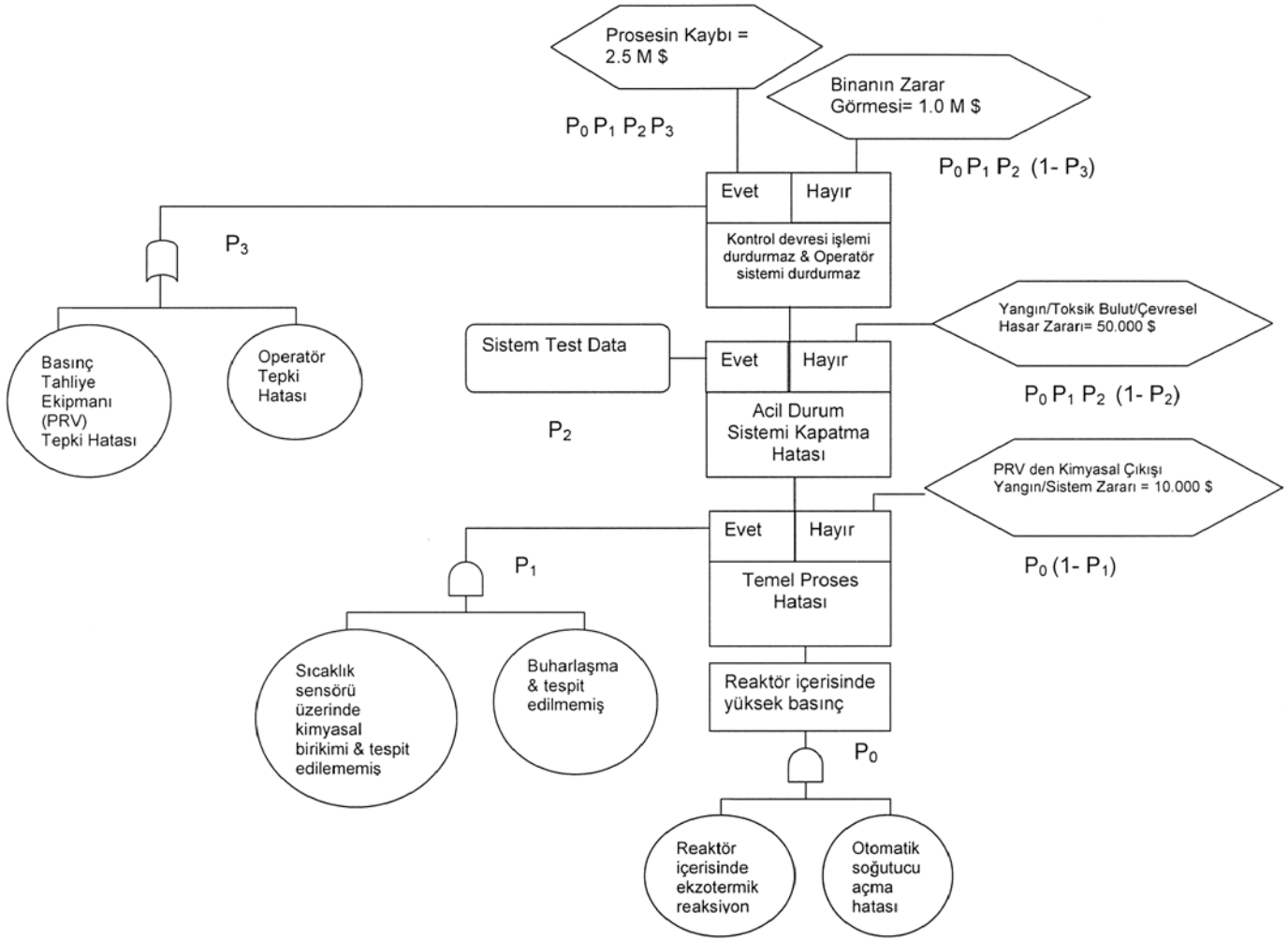
Örnek Problem:

Bir reaktörde, iki kimyasal 10 saatlik bir süre boyunca 180oC sıcaklıkta reaksiyona tabii tutulmaktadır. Reaksiyon tamamlandığında, reaksiyon ürünü kimyasal açılan bir valf ile depolama tankına doldurulmaktadır. İki kimyasal bileşen iki ayrı tanktan pompalanmaktadır. Pompalanan hacimler iki seviye kontrolünden okunmaktadır. Reaktörün içerisinden sıcaklık ve basınç kontrolü yapılmaktadır ve operatörün takip etmesi gerekmektedir. Ekzotermik reaksiyonda sıcaklık 200oC'ye geldiğinde soğutma suyu açılmakta, sıcaklık 250oC'ye ulaşıldığında ise otomatik acil durum kapatma sistemi (ESD) devreye girmektedir. Ayrıva reaktörde basınç tahliye vanası da mevcuttur. Sıcaklık sensöründen gelen sinyal düzenleyiciye bağlanmış ve sıcaklık kontrol devresinin bir parçasını oluşturmuştur. Eğer sıcaklık gerekenden daha düşük ise, düzenleyici ısıtıcıyı açar. Eğer sıcaklık çok yüksek ise, ısıtıcı kapatılır. Algılayıcıya gelen sinyal aynı zamanda sıcaklık 250°C'yi geçtiğinde devreye giren bir alarma bağlıdır. Alarm çaldığında operatörün gücü elle keseceği ve acil durum soğutma suyunu açacağı varsayılmaktadır.

Reaktör İçerisinde Yüksek Basınç Olasılığı;

$$\mathbf{P_0} = P_0.P_1.P_2.P_3 + P_0.P_1.P_2(1\text{-}P_3) + P_0.P1(1 - P_2) + P_0(1 - P_1)$$

Şekil 42: Örnek Neden Sonuç Analizi



11.20. Neden ve Etki Analizi (Cause and Effect Analysis)

Risk değerlendirmesinin genel amacı, sistemin olduğu gibi kabul edilebilir olup olmadığının, değişiklik gerekip gerekmediğinin tespiti için temel oluşturmaktır. İlave bir amaçta önemli ve daha önemsiz riskler arasında ayrım yapmaktır. İlave bir amaçta önemli ve daha önemsiz riskler arasında ayrım yapabilmektir. Daha detaylı amaçlar aşağıda verilmiştir. Bunlar birbirlerini kapsam dışı bırakmaz ve genellikle risk analizinin genel hedeflerine göre belirlenirler.

- Riskin "boyutu" ile ilgili tahmin yapmak,
- Risk seviyelerini kriterlere göre karşılaştırarak sistemi onaylamak,
- Güvenliği arttırmak için sistemde iyileştirme yapılmasına gerek olup olmadığına karar vermek,
- Uyarılar için temel oluşturmak, örneğin; güvenlik sisteminin güvenilirliğini belirleyerek bu güvenilirlik derecesinin yeterli olup olmadığı ile ilgili uzmanlara bilgi sağlamak.

Bazı kimyasal fabrikalarında, açık deniz platformlarında ve nükleer güç santrallerinde daha ayrıntılı ve kantitatif olarak uygulanabilecek risk değerlendirmesi yapılmasını zorunlu kılan yasal düzenlemeler mevcuttur. Bu tip kuruluşlar genelde yetkili kurumlarca ayrıntılı olarak kontrol edilirler ve kapsamlı güvenlik analizleri hazırlamaları istenir.(Örneğin, Seveso Direktifine göre). İşte bu aşamada Neden-Sonuç analizi bir grup uzman tarafından oluşturulan bütün muhtemel senaryolar ve nedenlerin göz önünde bulundurulmasını sağlamak için kullanılır ve deneysel olarak ya da mevcut verinin değerlendirilmesi ile test edilebilen en muhtemel nedenlere ilişkin fikir birliği oluşturulmasına olanak sağlar. Analizin ilk safhalarında, muhtemel sebepler hakkında fikir yürütmeyi genişletmek ve sonrasında da daha resmi bir şekilde ele alınacak olan muhtemel hipotezleri oluşturmak en faydalı yoldur.

Neden-Etki analizi, istenmeyen bir olay ya da problemin muhtemel nedenlerini tanımlayan yapılandırılmış bir yöntemdir. Neden-Etki analizi, kök neden analizi gerçekleştirmede bir yöntem olarak kullanılır. Muhtemel yardımcı faktörleri geniş kategorilere ayırır, böylece bütün muhtemel hipotezler göz önünde bulundurulabilir. Ancak, asıl nedenleri kendisi göstermez, çünkü asıl nedenler, sadece gerçek kanıt ve hipotezlerin deneylere dayalı olarak test edilmesi ile belirlenebilir. Bilgiler bir ağaç grafiğine yerleştirilebilir. Neden-Etki analizi, belirli bir etkinin nedenlerine ilişkin bir listenin, yapılandırılmış resimli anlatımını içerir. Etki, içeriğe bağlı olarak pozitif (bir amaç) ya da negatif (bir problem) olabilir.

Aşağıdaki işlemlere ihtiyaç duyulduğunda, Neden-Etki analizi oluşturma süreci başlatılabilir:

- Belirli bir etki, problem ya da koşula yönelik, muhtemel kök nedenleri ve temel sebepleri tanımlamak,
- Belirli bir süreci etkileyen faktörler arasındaki etkileşimlerin bazılarını sınıflandırmak ve bunlar arasında bağlantı kurmak,
- Mevcutproblemleri analiz etmek, böylelikle doğrulayıcı müdahaleleri gerçekleştirebilmek.

Neden-Etki analizi oluşturmanın faydaları şunlardır:

- Risk değerlendirme takım üyelerinin dikkatini belirli bir problem üzerinde toplar,
- Yapısal bir yaklaşım kullanarak bir problemin kök nedenlerini belirlemeye yardımcı olur,
- Grup katılımına teşvik eder ve ürün ya da süreç için grup bilgisinden faydalanır,
- Neden-Etki ilişkilerini şema ile göstermek için düzenli ve kolay okunabilir bir format kullanır,
- Bir süreçteki sapmaların muhtemel nedenlerini belirtir.

Girdi:

Bir neden-etki analizinin girdisi, uzmanlık ve deneyimden gelen verileri ya da geçmişte kullanılmış önceden geliştirilmiş bir risk değerlendirme yönteminden gelen verileri girdi olarak kullanır.

Süreç:

Neden-Etki analizi, çözümleme gerektiren problem ile ilgili bilgi sahibi olan bir uzman grubu tarafından gerçekleştirilebilir.

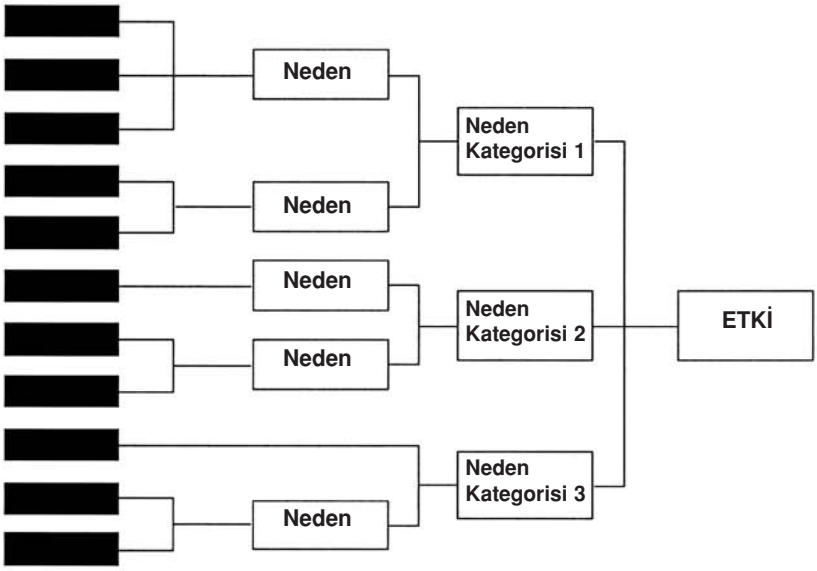
Bir neden-etki analizinin temel aşamaları aşağıda gösterilmiştir;

- Analiz edilecek etki tanımlanır ve bir kutuya yerleştirilir. Etki, koşullara bağlı olarak bir problem ya da istenmeyen bir olay olabilir,
- Kutular tarafından gösterilen nedenlerin ana kategorileri belirlenir. Genellikle, bir sistem problemine yönelik kategoriler, insan, ekipman, çevre, süreç, vb. şeklinde olabilir. Ancak bunlar, belirlenmiş içeriğe uygun olarak seçilir,

- Her bir baş kategoriye yönelik muhtemel sebepleri ve bunlar arasındaki ilişkiyi tarif etmek amacıyla, grafik dallar ve alt dallar ile doldurulur,
- Nedenleri saptamak için "neden?" ya da "buna ne sebep oldu?" soruları sorulmaya devam edilir,
- Tutarlılığı ve eksiksiz neden analizi yapıldığını doğrulamak ve nedenlerin ana etkiyi ilgilendirdiğini çek etmek amacıyla bütün dallar gözden geçirilir,
- Mevcut delile ve takımın görüşüne bağlı olarak en muhtemel nedenler tanımlanır.

Sonuçlar, genellikle, yatay ağaç diyagramı şeklinde gösterilir. Ağaç gösterimi, genelde sayfanın alt kısmına doğru değil, soldan sağa doğru gelişen ağaç ile gösterilmesine rağmen görünüşte bir hata ağacına benzer.

Şekil 43: Neden-Etki Analizinin Ağaç Formunda Örneği



Neden-Etki diyagramları genellikle kalitatif olarak kullanılır, ancak Seveso direktifi gibi kantitatif risk değerlendirmesi gerekli olduğu durumlarda kantitatif olarak da rahatlıkla kullanılabilir. Ancak bu durumda etki kısmından sonrası için de ayrıca bir risk değerlendirme tekniği daha kullanılması gerekir.

Sonuç:

Neden-Etki analizinin sonucunda, olası ve muhtemel nedenleri gösteren bir ağaç diyagramı elde edilir. Söz konusu diyagram daha sonra doğrulanır ve öneriler yapılmadan önce deneysel olarak test edilmesi gerekebilir.

Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler aşağıda gösterilmiştir:

- Hata ağacı analizinde olduğu gibi temel nedenlere odaklanır ancak kullanımı daha kolaydır,
- Bütün muhtemel hipotezleri göz önünde bulundurmayı sağlar,
- Sonuçların kolay okunabilen grafiksel çizimini verir,
- Daha fazla veriye ihtiyaç duyulması durumunda diğer kök neden analizi tekniklerine veri sağlar,
- İstenmeyen etkiler kadar beklenen etkilere yönelik de yardımcı faktörleri tanımlamak için de kullanılabilir,
- Bir konu üzerine olumlu bir şekilde odaklanmayı, daha büyük uzman katılımını ve olay nedenlerinin sahiplenilmesini teşvik eder.

Sınırlamalar aşağıda gösterilmiştir:

- Takım gereken uzmanlığa sahip olmayabilir,
- Kendi içinde tam bir süreç değildir ve öneriler üretmesi için kök neden analizinin bir parçası olmasına ihtiyaç duyar,
- Bağımsız bir analiz tekniğinden çok, beyin fırtınasına yönelik bir eleme tekniğidir.

11.21. Senaryo Analizi (Scenario Analysis)

Senaryo analizi, gelecekte meydana gelebilecek potansiyel olayların nasıl gelişebileceği konusunda açıklayıcı modellerin geliştirilmesine verilen isimdir. Gelecekte olası gelişmeleri dikkate alarak, onların etkilerini keşfederek riskleri tanımlamak ve her bir senaryo için potansiyel sonuçlar ile olasılıklarını analiz etmek amacı ile kullanılır.

Senaryo analizi, bir kuruluş, sistem veya proses ile ilgili politika kararlarını vermede ve mevcut faaliyetleri dikkate alarak gelecek stratejilerin planlanmasını değerlendirmek için de kullanılabilir. Senaryo analizleri özellikle büyük endüstri-

yel kazalara sebebiyet verebilecek kimya tesislerinde meydana gelebilecek en iyi durumu, en kötü durumu ve beklenen durumu yansıtan senaryoların, belirli koşullar altında oluşabileceğini belirlemek ve potansiyel sonuçları ve her bir senaryo için olasılıkları analiz etmek için kullanılır. Olasılık analizi, gelişecek tehditlerin ve fırsatların nasıl olduğunu tahmin etmek için yapılır ve hem kısa hem de uzun vadeli zaman dilimleri ile bütün risk türlerine yönelik olarak düşünülür. Kısa zaman dilimleri ve uygun veriler ile muhtemel senaryolar günümüzden tahmin edilerek yürütülebilir. Daha uzun zaman dilimleri veya güçlü veri ile senaryo analizi daha yaratıcı olur ve gelecek analizi olarak ifade edilebilir.

Girdi:

Bir senaryo analizi yapmak için ön koşul, aralarında mutlaka proses ile ilgili değişiklikleri tahmin edebilecek tecrübe ve bilgiye sahip kişilerden oluşturulmuş bir risk değerlendirme takımıdır. Ayrıca zaten var olan değişikliklere yönelik literatür ve verilere erişim de yararlıdır.

Süreç:

Bir ekip ve ilgili iletişim kanalları kurulduktan ve problemin içeriği tanımlandıktan ve sorunlar düşünüldükten sonra, bir sonraki adım oluşabilecek değişikliklerin türünü tanımlamaktır. Temel eğilimler ve eğilimlerdeki muhtemel değişikliklerin zamanlamasının yanı sıra, gelecek hakkında yaratıcı düşünmeye yönelik araştırma da gerekecektir.

Analiz aşamasında şu hususlar değerlendirilir;

- Harici değişiklikler (örneğin teknolojik değişiklikler gibi),
- Makro çevredeki değişiklikler (kanun yapıcı, toplumsal, vb.)
- Yakın gelecekte proseste yapılacak değişiklikler, sonuçları açısından değerlendirilmeye ihtiyaç duyulan kararlar,
- İhtiyaçları ve onların nasıl değişebileceği.

Bazen bir değişiklik başka bir risk sonucuna neden olabilir. Analiz için en önemli ve en belirsiz olan faktörler dikkate alınır. Anahtar faktörler veya eğilimler, senaryoların geliştirilebileceği alanları göstermektedir ve her biri için ayrı ayrı bir senaryolar oluşturulabilir.

Senaryo analizleri öncesinde proses veya sistemde mutlaka başka bir risk değerlendirme yöntemi ile proses tehlikeleri değerlendirilmiş olmalıdır (Proses FMEA, HAZOP, What If? vb.). Bu analiz sonrasında ise; örneğin, en iyi durum,

en kötü durum ve beklenen durum senaryolarının kullanıldığı yerlerde, elde edilen her bir senaryonun sonucunun olasılığı bize o sistemin veya prosesin ne kadar daha koruyucu önleme ihtiyaç duyulduğunu göstermesi açısından önemlidir.

Çıktılar:

Elde edilen senaryo ile; bir proseste veya sistemde eğer işler ters giderse ne gibi sonuçlar ortaya çıkabileceğini görmüş oluruz. Ayrıca bu senaryolar hikayeleştirilebilir ve bu senaryolara göre acil durum planları, felaket senaryoları ile müdahele plan ve tatbikatları da hazırlanabilir. Yine senaryo sonuçlarının olasılık değerlerinin yüksek çıkması da bize proses veya sistem için yeterli koruyucu bariyere sahip olmadığımızı da göstermektedir.

Güçlü Yönler ve Sınırlılıklar:

Senaryo analizi, gelecek olayların geçmiş eğilimleri muhtemelen takip etmeye devam edeceği varsayılarak, tarihsel verilerin kullanımı yoluyla, yüksek-orta-düşük tahminlere dayanarak proses veya sistemleri analiz etmeye yardımcı olmaktadır.

Senaryo analizinin kullanımındaki temel zorluklar; örneğin, Seveso Direktifi gibi yasal gereklilikler nedeni ile gerçekçi senaryoları geliştirmekle yükümlü karar mercileri ve analistlerin olası sonuçları araştırmak için uygun verilere sahip olmaları veya bu tür analizleri yapabilmeleri için gerekli eğitime ve kabiliyete sahip olmaları gerekmektedir.

11.22. Koruma Katmanları Analizi (Layers of Protection Analysis - LOPA)

Risk temelli yaklaşımlara bir tamamlayıcı unsur olarak risk değerlendirmesinin bir kategorisi sistemin güvenliğinin doğrulanması ile ilgilenmektedir. Bu bağlamda amaç, sistemdeki güvenlik fonksiyonlarının ve bariyerlerinin yeterliliğini değerlendirmektir. Bazı risk değerlendirmesi yöntemleri bu yaklaşımı temel alır.

Özellikle kimya sanayi, nükleer sanayi veya petrol platformları gibi bazı tesisler için özellikle yetkili otoriteler tarafından yayımlanan mevzuatlarda kaza risklerinin analizine dair zorunluluklar bulunmaktadır, Örneğin; Seveso Direktifi gibi.. Bununla birlikte kalitatif risk değerlendirme yöntemleri, genel karakterde olup tüm tehlike tiplerini değerlendirmek için kullanılamazlar. Bazı durumlarada, belli tipteki ekipmanlar için riskin kabul edilebilir olup olmadığına dair oldukça sağlam bilgilere ihtiyaç bulunmaktadır.

Büyük endüstriyel kazaların kontrolü ile ilgili yaklaşımda (Seveso Direktifi) "yaralanmalara karşı yeterli koruma sağlanmalıdır" ya da "sözkonusu risk olabildiğince azaltılmalıdır" tipinde formülasyonlar bulunmaktadır. Alınan kontrol tedbilerinden neyin "yeterli" neyin "yeterli olmadığı"na ya da risklerden özellikle "mümkün olabildiğince" hangisinin azaltılmasına gerek olduğuna olduğu karar verilmesi istenilmektedir. İşte bu aşamada hem büyük endüstriyel kazalara sebebiyet verebilecek tesislerde risk değerlendirme yapacak uzmanlar için, hem de bu tesisler ile ilgili karar verme yetkisine sahip olan merciler için bir güçlük bulunmaktadır; bir proseste veya sistemde alınabilecek güvenlik sistemleri nereye kadar kabul edilebilir bir seviyededir.

Bu aşamada yapılacak olan rik analizlerinin birçok uygulamasında kantitatif değerlendirmeler kullanılmaktadır. Belli bir kazanın meydana gelme olasılığı ve sonuçlarının büyüklüğü hesaplanır veya tahmin edilir. Bundan sonra riskin kantitatif değeri tehlikenin kabul edilip edilmeyeceği noktasında verilecek kararda kullanılır, işte bu analizlerden en önemlisi ise Koruma Katmanları Analizi (LOPA)'dır.

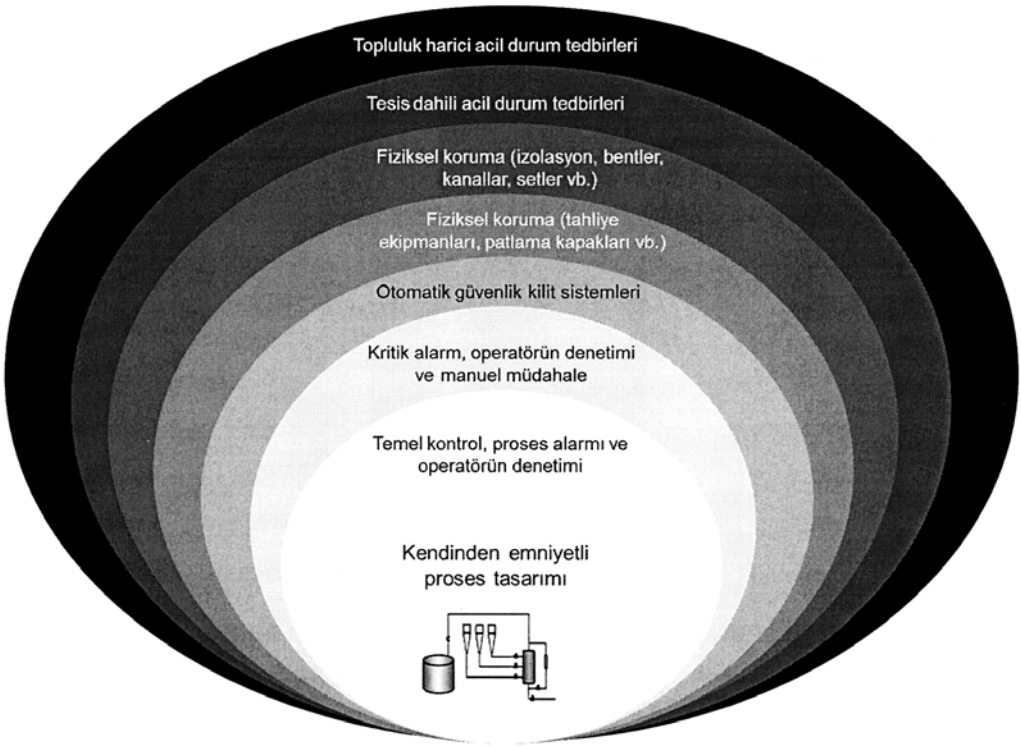
Kimya sanayii sistematik güvenlik çalışmalarında uzun bir geleneğe sahiptir. Güvenlik prensiplerinin kapsamlı bir özeti "Kimya Endüstrisinde Güvenli Otomasyon Rehberleri" (CCPS,1993) isimli yayında verilmiştir. Anılan yayın hem genel boyutları hem de otomatik ve proses kontrol sistemlerindeki güvenlik konusunda açıklamalar yapmıştır.

Kullanılan temel terim, açık şekilde tanımlanmamakla birlikte "koruyucu tabaka"dır. Bu "tipik olarak özel proses tasarımlarını, ekipmanını, idari prosedürleri, temel proses kontrol sistemini ve/veya ani olumsuz proses durumlarına karşı planlanmış önlemleri kapsamaktadır. Sözkonusu önlemler otomatik veya insan hareketine bağlı olabilir. "Koruyucu tabaka" olarak adlandırılan **Şekil 44**'de sekiz seviyeden oluşmaktadır.

Bunlar, muhtemel kazalara karşı nasıl aktive edildiklerine göre aşağıdaki gibi düzenlenmiştir:

1. Kendinden emniyetli proses tasarımı,
2. Temel kontrol, proses alarmı ve operatörün denetimi,
3. Kritik alarm, operatörün denetimi ve manuel müdahale,
4. Otomatik güvenlik kilit sistemleri,
5. Fiziksel koruma (tahliye ekipmanları, PRV, patlama kapakları vb.)

Şekil 44: LOPA katmanları



6. Fiziksel koruma (izolasyon, bentler, kanallar,setler vb.),
7. Tesis dahili acil durum tedbirleri,
8. Topluluk harici acil durum tedbirleri.

LOPA, istenmeyen olay ya da senaryolarla ilgili riskleri tahmin etmeye yönelik yarı kantitatif bir yöntemdir. Riski kontrol etmek ya da hafifletmeye yönelik yeterli önlem bulunup bulunmadığını analiz eder. Koruma Katmanları Analizi, özellikle kimya sanayiinde proses tehlike analizi yapılırken koruma seviyesinin yeterli olup olmadığının değerlendirilmesi ve hangi koruma katmanının ya da bariyerinin eksik olduğunun değerlendirilmesi için kullanılır. Özellikle Seveso Direktifi çerçecesinde proses tehlikelerine karşı ne derecede koruyucu önlemlere ihtiyaç duyulduğunu ve bu koruyucu katmanların güvenilirlik ve hata olasılıklarını analiz etmek amacı ile en çok kullanılan yöntemdir.

Referans standartlar:

- *IEC 61508, Elektrik/elektronik/ programlanabilir elektronik güvenlik ile ilgili sistemlerin işlevsel güvenliği. (Functional safety of electrical/electronic/programmable electronic safety-related systems)*
- *IEC 61511, İşlevsel emniyet - Proses endüstrisi sektörü için emniyetli enstrümante sistemleri (Functional safety – Safety instrumented systems for the process industry sector)*

Bu analizde bir neden-sonuç çifti seçilir ve istenmeyen sonuca yol açan nedeni engelleyen koruma katmanları tanımlanır. Olasılık hesaplaması ise; riski kabul edilir bir seviyeye indirmek için koruyucu bariyerlerin yeterli olup olmadığı belirlemek için gerçekleştirilir.

LOPA, bir risk ya da rastlantısal olay ile bir sonuç arasındaki koruma katmanlarını incelemek için kolay bir şekilde kalitatif olarak da kullanılabilir. Genellikle, örneğin HAZOP ya da PHA'yı takip eden proses tehlike analiz sürecinde ihtiyaç duyulan koruyucu katmanların ne kadarına ihtiyaç duyulduğunu analiz etmek amacıyla, yarı kantitatif bir yaklaşım olarak kullanılır.

Bu analiz çoğu zaman olasılıksal güvenlik analizi veya olasılıksal risk analizi olarak adlandırılır. Bu tür uygulamalarda risk değerlendirmesi iki ana bileşene sahiptir:

- Risk tahmini (olasılıkların ve sonuçlarla ilgili tahmin yapma)
- Risk değerlendirmesi (riskle ilgili genel değerlendirme yapma, örneğin, kabul edilebilirliği ve nasıl görüldüğü ile ilgili)

Risk değerlendirmesi (belli bir risk için) birtakım kriterler ve kabul edilme limitleri gerektirir. Bir tehlike için meydana gelme sıklığı ile sonuçlarının derecesi ve kabul edilme limitleri arasındaki ilişki ise ALARP veya ALARA ile değerlendirilir.

LOPA, IEC 61508 serisinde tarif edildiği gibi, güvenlik enstrümanlarına yönelik güvenlik bütünlüğü seviyelerinin (Safety Integrity Level - SIL) saptamasında ve enstrümanlı sistemlerin bağımsız koruma katmanlarının (Independent Protection Layer - IPL) belirlenmesi için bir zemin hazırlar. LOPA, her bir koruma katmanı tarafından üretilen risk azaltımını analiz ederek, risk azaltım kaynaklarını etkili bir şekilde dağıtmaya yardımcı olması için kullanılır.

Girdi:

LOPA'ya yönelik girdiler şunlardır:

- PHA, HAZOP, Proses FMEA, What If vb. analizler ile proses tehlikeleri, nedenleri ve sonuçlarını içeren risklerle ilgili temel bilgiler,
- Mevcut olan ya da önerilen kontroller ile ilgili bilgiler,
- Rastlantısal olay sıklıkları, koruma katmanı arıza olasılıkları, sonuç ölçümleri,
- Tetikleyici olay sıklıkları, koruma katmanı arıza olasılıkları, sonuç ölçümleri ve kabul edilir risk tanımı.

Süreç:

LOPA, aşağıdaki prosedürü uygulayan uzman bir risk değerlendirme ekibi tarafından gerçekleştirilir:

- İstenmeyen bir sonuca yönelik tetikleyici nedenleri tanımlayınız ve sıklıkları ile sonuçları hakkındaki verileri araştırınız,
- Tek bir sebep-sonuç çifti seçiniz,
- İstenmeyen sonuca doğru ilerleyen sebebi engelleyecek koruma katmanlarını tanımlayınız ve etkililikleri yönünden analiz ediniz,
- Bağımsız koruma katmanlarını (IPL) tanımlayınız (bütün koruma katmanları IPL değildir),
- Her IPL'nin hata olasılığı hakkında tahmin yürütünüz,
- Kök neden ve istenmeyen sonucun meydana gelme sıklığını belirlemek amacıyla, her IPL'nin hata olasılıkları, herhangi bir koşullu değişken (bir koşullu değişken, örneğin, etki edilecek kişinin mevcut olup olmadığıdır) olasılıkları ile birleştirilir. Önem sıraları, sıklıklar ve olasılıklar için kullanılır,
- Riskin hesaplanan seviyesi, daha fazla korumaya gereksinim olup olmadığını belirlemek için, risk tolerans seviyeleri ile karşılaştırılır.

Bir IPL, istenmeyen sonuca doğru giden bir senaryoyu engelleme yetisine sahip olan, rastlantısal olaydan ya da senaryo ile ilgili diğer koruma katmanlarından bağımsız bir enstrüman, sistem ya da faaliyettir.

IPL aşağıdakileri içerir:

- Tasarım özellikleri,

- Fiziksel koruma aygıtları, enstrümanları,
- Kilitleme ve kapama sistemleri,
- Kritik alarmlar ve el ile müdahale,
- Olay sonrası fiziksel koruma,
- Acil durum yanıt sistemleri (prosedürler ve denetimler IPL değildir).

Çıktılar:

Daha fazla kontrol gerekip gerekmediği (yani koruyucu bariyer) ve bu kontrollerin etkinliği için öneriler risk azaltma faktörleri çıktı olarak verilir.

LOPA güvenlikle ilgili / enstrümante sistemlerinin yeterliliği ile uğraşırken aynı zamanda SIL değerlendirmesi için kullanılan tekniklerden de birisidir.

Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler şunlardır:

- Tamamen kantitatif risk değerlendirmesinden daha az zaman ve kaynak gerektirmektedir,
- Bir prosesin ihtiyacı olan en kritik koruma katmanları üzerindeki eksiklikleri tespit etmemize ve onlara odaklanılmasına yardımcı olur,
- Yeterli emniyet tedbirlerinin olmadığı işlemleri, sistemleri ve süreçleri tanımlar,
- En ciddi sonuçlara odaklanılmasını sağlar,

Sınırlılıklar ise şu şekildedir:

- LOPA, bir defada bir neden-sonuç çifti ve bir senaryo üzerinde durmaktadır. Karmaşık etkileşimler var ise risklerin tespiti mümkün olamayabilir,
- Ortak mod hataları tespit edilemeyebilir,
- LOPA, birçok sebep-sonuç çiftlerinin veya farklı paydaşları etkileyen sonuçların var olduğu karmaşık senaryoları analiz edemez.

11.23. Karar Ağacı Analizi (Decision Tree Analysis)

Bir karar ağacı, belirsiz sonuçları dikkate alan ve sonuçları peş peşe gelecek şekilde sıralayarak bu sonuçlar için karar alternatiflerini geliştirmek için kullanılan bir analiz türüdür. Olay ağacına benzemektedir, çünkü tetikleme bir olay tarafından veya bir ön karar veya farklı bir yol nedeni ile meydana gelebilecek olayların sonuçları ile alınabilecek farklı kararları içeren bir analizdir.

Bir karar ağacı, sistem, süreç, ekipman, proses veya proje risklerini yönetmenin belirsizlik içerdiği yerlerde eylemin en iyi gidişatının seçimine yardımcı olmak için kullanılmaktadır. Grafik çizimi de en iyi yolun seçimi ve bu yol için karar alınması için yardımcı olur. Bu, analizi ve planlamayı kolaylaştırır. Tesisten veya bir ekipmandan kaynaklabilecek tehlikelerin hızlı bir biçimde gözden geçirilmesi için ideal bir yöntemdir. Bu yöntemin adımları aşağıda verimiştir:

- Sistem farklı bileşenlere ayrılarak sistemin basitleştirilmiş bir modeli elde edilir. Bu adıma "yapılandırma" denir.
- Sistemin her bileşeni için riskler (tehlikeler) ve kaza riskleri ile ilgli diğer faktörler tanımlanır.

Girdi:

Karar noktaları ile bir proje veya süreç planı,

Kararların olası sonuçları ve kararları etkileyebilecek tesadüfi olaya ilişkin bilgiler.

Süreç:

Bir karar ağacı ön karar ile başlar. Örneğin; Proje A'dan Proje B'ye devam etmesi. İki varsayımsal proje devam ederken, farklı olaylar meydana gelir ve farklı öngörülebilir kararların alınması gerekecektir. Bunlar, olay ağacına benzer bir ağaç biçiminde temsil edilmektedir.

Olayların olasılığı, izlenen yolun nihai sonucunun kullanımı ve maliyeti ile birlikte tahmin edilebilir.

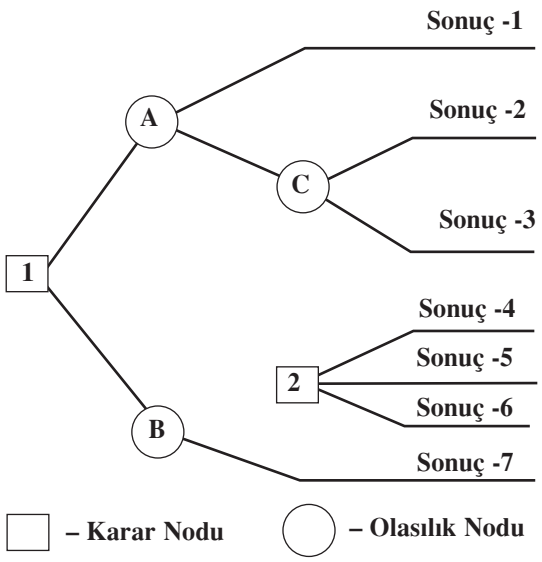
En iyi karar yoluyla alakalı bilgiler, mantıken yöntem ve sonuç değeri boyunca bütün koşullu olasılıkların bir ürünü olarak hesaplanan en yüksek beklenen değeri üreten unsurlardır.

Çıktılar:

Çıktılar aşağıdaki gibidir;

- Benimsenebilecek farklı seçeneklerin görüntülenmesi yoluyla riskin mantıksal bir analizi,
- Her bir olası yöntem veya yol için beklenen olasılık değerinin hesaplanması.

Şekil 45: Karar ve Olasılık Nodları



Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler şunlardır;

- En iyi yöntem ile ilgili karar verilmesi gereken bir problemin ayrıntılarının net bir grafiksel gösterimini sağlamaktadır,
- Bir durum ile ilgili en iyi yöntemin seçilmesini ve olasılığının hesaplanmasını sağlamaktadır.

Sınırlılıklar ise şöyledir:

- Büyük karar ağaçları özellikle analize katılmamış olan diğer kişilerin anlaması bakımından karmaşık olabilir,
- Bir ağaç diyagram olarak temsil edildiğinde, durumun basitleştirilmesi eğilimi söz konusu olabilir.

11.24. İnsan Güvenilirlik Değerlendirmesi (Human Reliability Assessment - HRA)

19. yüzyılın sonundan itibaren günümüze kadar, çoğu kişi insanların hareketleri düşünürken ve yaparken neden hata yaptıklarını araştırmışlardır. Hatalar ve ihlaller arasında kesin bir çizgi çizmek zordur ve muhtemelen gerekli de değildir.

Bazı durumlarda, bilinçli sapmalardan olan uygulamalar da sapma olarak kabul edilir. Çoğu koşulda bu risk almadır. Elbetteki hatalar direk olarak bir parça malzeme ile çalışan ve planlamaya ve tasarıma katılmış insanlar tarafından işlenir. İnsan hatası ve riskli davranış, önemli derecede teknik tasarım ve organizasyonel yapı ve aynı zamanda işyerindeki sosyal yapıdan etkilenir. İnsanların kuralların dışına çıkması durumu için bir çok neden vardır, birkaç örnek verecek olursak;

- Kişi, hareketin ihlal olduğunu bilmemektedir. Kurallardan haberi yoktur, veya hareketin bir ihlali ifade ettiğinin bilincinde değildir.
- Kişi kurallardan haberdardır, fakat unutmuştur, örneğin ender olarak uygulanıyorsa.
- Kural kişi veya çevresi tarafından önemsiz olarak algılanmıştır.
- Diğer hedefler ve kurallar arasında bir çelişki vardır.
- Sebepli veya sebepsiz, kuralın yetersiz veya yanlış olduğu düşünülmektedir.

Bireysel düzeyde, kazalar tehlikeli ve aynı zamanda yasak olduğu bilinen hareketlerin yapılması örneğinde olduğu gibi risk alma ile ilişkilendirilebilir. Aynı zamanda risk almanın bir bedeli vardır. Tehlikeli çalışma şekilleri daha hızlı ve daha özensiz olabilir ve bu sebeple yüksek verimliliğe yol açabilir. İnsan hatası ve riskli davranış, önemli derecede teknik tasarım ve organizasyonel yapı ve aynı zamanda işyerindeki sosyal yapıdan etkilenir. Bireylerin daha güvenli davranmalarını sağlamış az veya çok derecede başarılı çok sayıda yöntem mevcuttur. Güvenliğin geliştirilmesi için yapılan bilgi etkinlikleri çok güncel bir konudur, fakat kısa süreli ve marjinal etkiye sahiptirler.

İnsan hatalarının olasılıksal boyutları ile ilgili özel bir çalışma alanı da" İnsan Güvenilirlik Değerlendirmesi" (HRA) olarak adlandırılmaktadır. İnsan güvenilirlik değerlendirmesi (HRA) sistem performansı üzerindeki insan etkisi ile ilgilenir ve sistemde insan hatası etkilerini değerlendirmek için kullanılır. Birçok süreç, özellikle operatörün karar alması için var olan zaman kısa olduğunda insan hatası potansiyeli içerir. Sorunların ciddi bir hal alması halinde, operatörün yeterince ihtimalleri tahmin etmesi ve buna göre eylem geliştirmesi olasılığı az olabilir. Ancak bazen, insan eylemi kaza yolunda ilerleyen ilk başarısızlığı (hatayı) önlemek için sadece savunma (bariyer) da olabilir. HRA'nın önemi, özellikle yaşanan bir dizi endüstriyel kazada olaya katkıda bulunan kritik insan hatalarının varlığının fark edilmesi ile anlaşılmıştır. Bu tür kazalar, endüstriyel tesislerdeki yazılım

ve donanımların hata olasılılarına, insan hata katkısı olasılığının göz ardı edilmemesi gerektiğini göstermektedir.

Daha çok sayısallaştırma üzerinde durulur ve sonuçlar olasılıksal güvenlik tahminlerinde kullanılır. HRA'nın amacı, bir aktivitenin başarı (veya başarısızlık) ile sonuçlanma ihtimalinin ortaya çıkarılmasıdır. HRA prosesini sekiz temel parçayla açıklayabiliriz;

1. Problem tanımı,
2. Görev analizi,
3. İnsan hata analizi,
4. Bu bilgilerin, hatanın sistem üzerindeki etkisini gösteren sayısal değerlendirmeye imkan sağlayan bir form olarak gösterilmesi,
5. İnsan hatalarını sayısallaştırma,
6. Etki değerlendirmesi, toplam sistem risk düzeyinin hesaplanması,
7. Hata azaltma analizi,
8. Dokümantasyon ve kalite güvencesi.

Bununla birlikte, farklı prosedürlere sahip çok sayıda insan güvenilirlik yöntemi bulunmaktadır, insan hatalarını tanımlamayı amaçlayan birbirine benzer bir çok yöntem vardır. (Örneğin; THERP, CREAM vb.) Bu yöntemler iyi tanımlanmış prosedürlerin bulunduğu kuruluşlara uygulanabilir, örneğin; inşaat, otomasyon veya proses endüstrileri gibi. Eğer iyi kurgulanmış rutinler bulunmuyorsa analizin üzerinde gerçekleştirileceği bir temel bulmak zorlaşır. Genelde, amaç insan hatasına maruz adımların belirlenmesi ve bu tür hataların sonuçlarının değerlendirilmesidir.

Kullanım:

HRA, kalitatif ya da kantitatif olarak kullanılabilir. Kalitatif olarak, insan hatası ve bu hatanın nedenleri için potansiyel durumları belirlemek için kullanılır, böylelikle hata olasılığı azaltılabilir. Kantitatif olarak HRA ise, FTA veya diğer teknikler içerisindeki insan hatalarına veri sağlamak için kullanılır.

Girdi:

HRA girdileri şunlardır:

- İnsanların gerçekleştirmesi gereken görevlerin tanımlanmasına yönelik bilgiler,

- Hata potansiyelinde ve pratikte meydana gelen hata türlerinin deneyimi,
- İnsan hatası ve ölçümü ile ilgili uzmanlık.

Süreç:

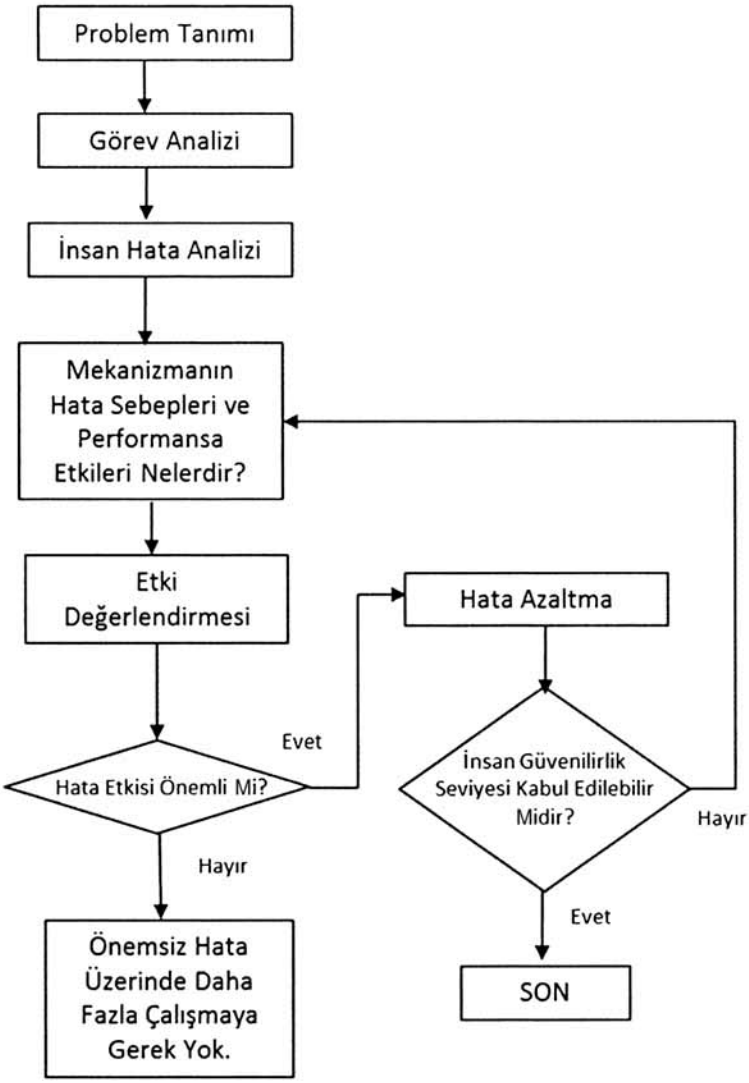
HRA süreçleri aşağıdaki gibidir:

- **Problem tanımı;** ne tür insan bağımlılıkları bulunuyor? araştırılmalı/ değerlendirilmelidir,
- **Görev analizi;**
  - Nasıl görev yapılmaktadır?
  - Hangi tür yardımlar insan performansını desteklemek için gerekli olacaktır?
- **İnsan hata analizi;**
  - Görev performansı nasıl başarısız olabilir?
  - Söz konusu hatalar veya görev performans başarısızlıkları nelerdir?
  - Hangi hatalar oluşabilir ve bunlar nasıl telafi edilebilir?
  - Bu hatalar diğer donanım, yazılım ve çevre olayları için ne gibi hatalar oluşturabilir?
- **Olasılık belirleme;**
  - Yapılan görev ile ilgili insan hataları ve bu hatalara bağımlı diğer sistem arızalarına ilişkin olasılıklar nelerdir?
- **Etki değerlendirmesi;**
  - Hatalar veya görevlerden en önemlisi hangisidir?
  - Yani hangisi güvenilirlik veya risk için en büyük katkıya sahiptir?
  - Kritik sistemler veya ekipmanlar için önem arz eden herhangi bir hata veya görev var mıdır?
- **Hata azaltılması;**
  - Daha yüksek insan güvenilirliği nasıl elde edilebilir?

HRA'nın ayrıntılarının belgelenmesi gerekmektedir. Uygulamada, bazen parçalar ile birbirine paralel olarak ilerlemesine rağmen HRA işlemi adım adım başlar (örneğin; görev analizleri ve hata tespiti ile).

Bu analiz özellikle proses endüstrileri içinaşağıdaki aşamaları içerecek şekilde uygulanır;

Şekil 46: İnsan Güvenilirlik Değerlendirmesi Akım Şeması



- Operasyonel prosedürdeki adımların listelenmesi. Bu liste, farklı hareketlerin kuruluş üzerindeki etkilerini ortaya koymaktadır. Bu liste "A Butonuna bas" veya "C valfini çevir" gibi unsurlar içerecek şekilde detaylandırılır.
- Hata kontrol listesi kullanılarak, herbir adım için muhtemel hataların tanımlanması yapılır,

- Hataların sonuçlarının değerlendirilmesi yapılır,
- Önemli hataların belirlenebilen nedenlerinin araştırılması yapılır,
- Proses üzerinde kontrolü sağlayacak şekilde tasarlanan muhtemel faaliyetlerin analizi yapılır.

Çıktılar:

Çıktılar şunlardır;

- Hata modları, hata türleri nedenleri ve sonuçları belirlenmiş olur,
- Hataların yarattığı riskin kalitatif veya kantitatif olarak değerlendirmesi yapılmış olur,
- Bir hatalar listesi oluşturulabilir ve bunlar, önerilen yeni yöntemler tarafından azaltılabilir,
- Tercihen sistemin yeniden tasarlanması yapılabilir,

Güçlü Yönler ve Sınırlılıklar:

HRA 'nın güçlü yönleri şunlardır:

- HRA, insanların önemli bir rol oynadığı sistemler ile bağlantılı olarak, risklerin göz önünde tutulması suretiyle insan hatasını kapsamaya yönelik formal bir mekanizma sağlar,
- İnsan hata modları ve mekanizmalarının şekilsel değerlendirmesi hata olasılığını aynen FTA analizinde olduğu gibi hesaplama şansı yaratır.

Sınırlamalar şunlardır:

- İnsan davranışlarının değişkenliği, karmaşık hata modları ve olasılıklarını belirlemeyi zorlaştırır,
- HRA, yetersiz karar verme sonucu ortaya çıkabilecek kısmi hataları belirlemekte zorluk çekmektedir.

11.25. Papyon Analizi (Bow - Tie Analysis)

Papyon analizi sebeplerden sonuçlara risk yollarını tanımlama ve analiz etmeye yönelik basit bir şematik analizdir. Özellikle Seveso Direktifi gibi büyük endüstriyel kazların felakete sebebiyet verecek sonuçlarının değerlendirilmesinde sıklıkla kullanılır.

Avrupada, önemli kazaya neden olabilecek kimyasal tesisler ile ilgili direktif olan Seveso direktifi kantitatif değerlendirme ve kabul edilebilirlik kriterleri üze-

rinde durmaktadır. Kantitatif değerlendirmeler, özellikle risklerin sonuçlarının ağır olduğu birçok kişinin ölümüne neden olabilecek kazaların olma ihtimalinin değerlendirilmesinde kullanılmaktadır. Bu alanda oldukça geniş literatür bilgisi ve uluslararası standartlar bulunmaktadır. Ancak papyon yaklaşımı, daha az tehlikeli sistemlere ve normal kazalara da uygulanabilir.

Zaman içerisinde proses endüstrilerinde güvenlik fonksiyonlarını tanımlamak için kullanılan terminoloji oldukça değişim göstermiştir, Bow-Tie modelleme gibi modelleme teknikleri işte bu aşamada özellikle proseslerin güvenlik fonksiyonlarını değerlendirmek maksadı ile kulanılmış ve kullanılmaktadır. Analizde incelene fonkasiyonlar;

- Bariyer fonksiyonu; kaza/olay evrimini engelleyerek zincirdeki diğer olayın gerçekleşmesini önler,
- Savunma hatları,
- Fonksiyonel güvenlik, örneğin; güvenlikle ilgili sistemin kontrol altındaki ekipmanın güvenli durumda olması için gerekli faaliyetleri yapabilmesi (IEC 61508),
- Koruma katmanları (CCPS,1993),

Güvenlik fonksiyonu, daha ziyade genel bir terimdir ve literatürde açık bir tanımına rastlanmamıştır. Hatta " Fonksiyonel Güvenlik Standard"ında (IEC 61508) terim birçok yerde kullanılmasına rağmen tanımlanmamıştır. Bu yüzden çeşitli uygulamalarda değişik anlamlarda kullanılmaktadır. Güvenlik fonksiyonunu tanımlayacak olursak; sistemdeki kazaları ve istenmeyen olayların olasılığını ve/veya sonuçlarını azaltacak teknik, organizasyonel veya bunların bileşke fonksiyonu olarak tanımlanabilir.

11.25.1. Kantitatif Risk Tahmini

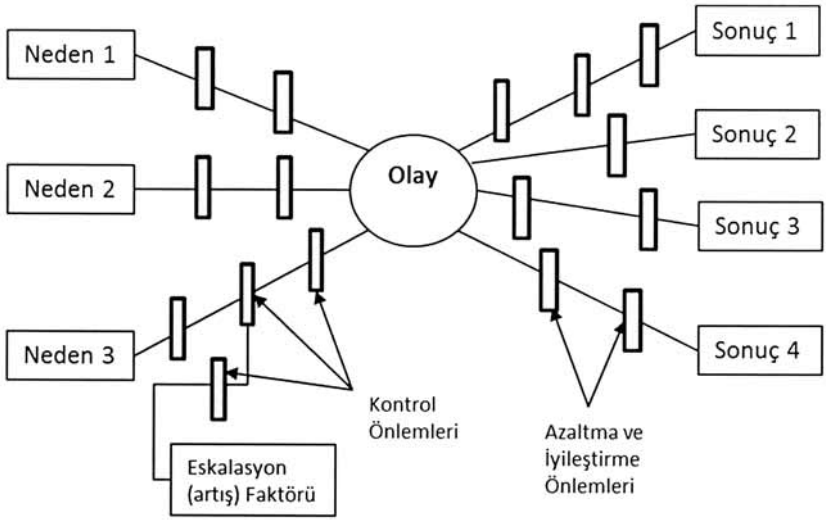
Kantitatif risk tahminleri birçok yolla yapılır ve birtakım parçaları kapsar. Papyon analizi istenmeyen her olayın meydana gelme olasılığı ile ilgili tahmin yürütür. Üç genel yaklaşım gerek bireysel olarak gerek bunların kombinasyonu olarak uygulanabilir.

- İlgili tarihi bilgilerin kullanımı,
- Analitik tekniklerin kullanılması, örneğin; Hata ağacı veya Olay Ağacı, LOPA vb.
- Uzman görüşlerinin kullanılması.

Papyon analizi istenmeyen olayın meydana gelmesi durumunda oluşacak muhtemel etkiyi de tahmin eder. Örneğin kimya sektöründe, yangın ve patlamalar durumunda gaz emisyonlarının hesaplanması için birçok yöntem bulunmaktadır. Bu tipte bir tahminin detaylı tanımını yapmak için papyon analizin devamında farklı sonuç – etki analizlerinin yapılması gerekmektedir. Bu kapsamda daha özel literatüre yönlenilmesi önerilir.

Hata ağacı analizi herhangi bir olayın nedenini (papyonun düğümünün sol tarafı) ve olay ağacı analizi de bu olayın ortaya çıkması sonrasındaki sonuçlar kısmını (papyonun düğümünün sağ tarafı) analiz eder. Papyonun odağında bulunan incelenen ana olayın hemen sağında ve solunda kök nedenler ile sonuçlar arasındaki bariyerler bulunmaktadır. Papyon şemaları hata ve olay ağaçlarının bir bileşimidir, analistler bir beyin fırtınası oturumunda hata ve olay ağaçlarının herhangi birinden başlayarak analizi yapılandırılabilir.

Şekil 47: Papyon Şema Örneği



Papyon analizi, meydana gelmesi istenmeyen olası bir olayı meydana getiren kök nedenlerin ve olay meydana geldikten sonra ortaya çıkabilecek sonuçları grafiksel olarak görüntülemek için kullanılır. Analiz tam olarak hata ağacının karmaşıklığını içermez, papyon analizinin anlaşılması, karmaşık hata ve olay ağaçlarından daha kolaydır. Her bir hata yoluna yönelik bir bariyerin veya denetimin var olduğunu ve bu bariyerlerin yeterli olup olmadığını değerlendirmek maksadı ile kullanılır.

11.25.2. Güvenlik Fonksiyonlarının Karakteristikleri

Bir güvenlik fonkisyonunun toplam güvenliğe olan katkısını açıklamak ve bunun değerlendirilmesine temel oluşturmak amacıyla birtakım karakteristiklerle tanımlanmıştır. İlgili karakterizasyonlara örnekler aşağıda verilmiştir:

- Güvenlik fonksiyonunun hatası durumundaki sonuçlar, GF'nin ne kadar önemli olduğunu, ayrıca hatanın direk kazaya veya istenmeyen olaya neden olup olmayacağını açıklar,
- Güvenlik fonksiyonunun sapmalara ve prosedürlerin bozulmasına karşı dayanıklılığı (veya tam tersi- zayıflığı ki bunu halletmek daha kolaydır.),
- Güvenlik fonksiyonunun sonuçlarının beklenen çıktılarla doğrulanabilme imkanı,
- "Verimlilik" güvenlik fonksiyonunun amacını nasıl gerçekleştirdiği. Daha genel bir tanım henüz yapılmamış olup yapılsa bile tüm güvenlik fonksiyonu tiplerini kapsayan bir tanım aldatıcı olabilir.

Benzer terimler IEC tarafından yayımlanan standartlarda da (IEC 61508) bulunabilir.

- Fonksiyonel güvenlik, güvenlikle ilgili sistemin kontrol altındaki ekipmanın güvenli durumda olması için gerekli faaliyetleri yapabilmesidir
- Entegre güvenlik güvenlikle ilgili sistemin belirlenen durumda ve belirlenen zaman periyodunda gerekli güvenlik fonksiyonlarını tatminkar şekilde yerine getirebilme ihtimalidir.

Güvenlik fonksiyonunun amacı, güvenlik tartışmaları ve sistem analizi için oldukça basit bir temel elde etmektir. Sözkonusu sisteme göre uygun bir karakteristik grubu tanımlanabilir. Sistem iyi biliniyor ise farklı güvenlik fonksiyonları arasındaki ilişkiler modellenir ve karakteristiklerin olasılıksal tahminleri yapılabilir. Diğer karakteristik grupları da seçilebilir. Tehditler ve farklı faktörler güvenliği azaltabilir. Örneğin aktif hatalar, istenmeyen durumlar ve lokal olaylar kapsama alınabilir. Bu tip boyutlar, "Bow-Tie Modelleme" içerisinde ele alınabilir.

Girdi:

Bir bir riskin, engelin ve engellenebilen, azaltılabilen veya uyarabilen kontrollerin sebep ve sonuçları üzerine çeşitli bilgilere ihtiyaç duyar.

Süreç:

Papyon şeması aşağıdaki gibi çizilir:

- Belirli bir risk, bir papyon merkez düğümü olarak temsil ve analiz edilmek üzere tanımlanır.
- Olayın sebepleri risk kaynağı gibi (veya güvenlik bağlamındaki tehlikeler şeklinde) düşünülerek listelenir. Risk kaynağı kritik olaya öncülük eden mekanizma tanımlanır.
- Çizgiler papyonun sol kenarını şekillendiren her bir kök neden ve sebep arasında çizilir. Artmaya öncülük edebilecek faktörler (Eskalasyon faktörleri) şemada belirlenebilir ve dahil edilir.
- İstenmeyen sonuçlara öncülük eden her bir nedeni önlemesi gereken bariyerler, çizgi boyunca dikey çubuklar olarak gösterilir. Artışa neden olabilecek faktörlerin (Eskalasyon faktörleri) olduğu yerde, artışa yönelik engeller de temsil edilir ve çizilir.
- Papyonun sağ tarafında, riskin farklı potansiyel sonuçları tanımlanır ve çizgiler olaydan her bir potansiyel sonuca merkezi bir noktadan yayılmak suretiyle çizilir.
- Sonuçlara yönelik engeller, radyal çizgiler boyunca dikey çubuklar (bariyerler) olarak gösterilir.
- Bariyerleri destekleyen yönetim işlevleri papyon altında gösterilebilir ve ilgili kontrol ile bağlantılı olabilir.

Bir papyon şeması eğer Büyük Endüstriyel Kazaların Önlenmesi ve Etkilerinin Azaltılması Hakkında Yönetmelik yani Seveso Direktifi gibi kantitatif değerlendirme gerektirmiyor ise bu durumda yanlızca şematik olarak söz konusu olayı meydana getiren nedenler ve olayın meydana gelmesi durumunda ortya çıkabilecek sonuçları engellemek veya kontrol altına almak için mevcut bariyerlerin yeterliliğini incelemek maksadı ile kullanılır. Ancak kantitatif olarak kullanılmak isteniyor ise papyon modellemesi ile birlikte uygun farklı risk değerlendirme veya tehlike analizi tekniklerini birlikte kullanmak gerekir, tek başına papyon diyagramı kantitatif analizi gerçekleştiremez. Birçok durumda, yollar ve bariyerler bağımsız değildir ve kontroller prosedür ile ilgili olabilir ve dolayısıyla etkililiği belirsiz bir nitelik taşıyabilir. Nicelleştirme genellikle daha uygun bir şekilde FTA ve ETA kullanılarak gerçekleştirilir. Örneğin; HAZOP, LOPA, İşlevsel Güvenlik Analizi, RCM vb. teknikleri de kullanarak papyon analizine kantitatif veri sağlanması gerekir.

Çıktılar:

Çıktı, ana olayı, istenmeyen sonuçları azaltma veya kontrol altında tutmak üzere mevcut bariyerleri ve istenilmeyen sonuçları gösteren basit bir şemadır.

Güçlü Yönler ve Sınırlılıklar:

Papyon analizinin güçlü yönleri şunlardır:

- Problemin açık bir grafiksel temsilini verir ve kolaylıkla anlaşılabilir,
- Sol ve sağ tarafta bulunan önleme ve azaltma kontrolleri ile bunların etkinliğini çek etmeye ve eksik kontrollere odaklanılmasını sağlar,
- İstenilmeyen sonuçların belirlenmesini sağlar,

Sınırlamalar ise şunlardır:

- Sonuçlara sebep olan eş zamanlı çoklu nedenlerin meydana geldiği yerlerde tek başına yeterli olamayabilir,
- Özellikle kantitatif analiz gerektiren durumlarda karmaşık durumları fazlaca basitleştirebilir.

11.26. Güvenilirlik Merkezli Bakım (Reliability Centred Maintenance - RCM)

Bir işletmedeki güvenliğin sağlanabilmesi için sistemle ilgili bilgilerin toplanması bir temel oluşturur. Sistemin ve içinde yer alan aktivitelerin tümü analiz kapsamına alınmalıdır. Analiz önemli parçaları gözden kaçırmayacak şekilde tasarlanmalıdır. Takip edilecek ana yol tanımlanmalı ve buna uyulmalıdır.

Tehlikelerin artmasına neden olabilecek riskler tutarlı biçimde değerlendirilmelidir. İşte bu aşamada tehlikelerin tanımlanması için sistematik olarak belirlenmiş bir risk analizi yöntemi gereklidir. Güvenlik önlemlerinin oluşturulması ve değerlendirilmesinde sistematik yaklaşım kullanılmalıdır.

Güvenilirlik alanında uluslararası bir standart olan IEC 60300-3-9 "risk analizi" ve ilgili şu tanımlamayı yapmaktadır. Bu standarta göre:

Risk analizi; mevcut bilginin tehlikelerin tanımlanması ve bireylere, topluma, mallara veya çevreye karşı risklerin tahmin edilmesi amacıyla sistematik biçimde kullanılmasıdır. Standartta risk, sıklığın veya meydana gelme olasılığının ve sözkonusu tehlikeli olayın sonucunun kombinasyonu olarak ifade edilir.

Güvenlik ancak kaza risklerinin sistematik olarak tanımlanması ve ortadan kaldırılması ile mümkündür. Tasarım sırasında yapılacak sistematik analizlerle hata ve problemlerin etkin şekilde belirlenmesi ile sonradan çıkacak daha büyük maliyetlerden kurtulmak mümkündür. Sistem veya proseslerde meydana gelebilecek arıza veya kesilmelere neden olabilecek faktörlerin sistematik olarak belirlenmesi ve yokedilmesi güvenilirlik çalışmaları ile yapılabilir. Güvenirliğin geliştirilmesi için çeşitli stratejiler uygulanabilir ve birleştirilebilir;

- **İyi tasarım:** Yüksek güvenirlik için dizayn ve iyi mühendislik temeldir.
- **Güvenilir bileşenlerin kullanımı:** Bir sitemin güvenirliği bütün olarak bileşenlerin ve alt sistemlerin güvenirliğine bağlıdır.
- **Bakım:** Güvenirlik bakımından tesisin bakımı şüphesiz önemlidir. Ancak bakım ile güvenilir bileşenlerin kullanıldığı dizaynın mevcut güvenilirliğinin devamı saplanabilir.

Ekipman ve sistemler için teknik hatalardan tamamen kurtulmak mümkün değildir. Bir tasarım felsefesi de, hata oluştuğu taktirde sürekli güvenli duruma dönecek şekilde ekipmanın yapılmasıdır. Bu, basit sistemlerde çoğunlukla makinenin durması anlamına gelir. Genel olarak, bu tip sistemlerin oluşumu belirli tasarım prensipleri ve sadece belirli şekilde bozulan kritik bileşenlerin seçimini gerektirmektedir.

Ancak bazı durumlarda ekipmanın sadece basit bir şekilde durması ya da çalışmaması çok daha büyük sorunlara, hatalara veya tehlikelere sebiyet verebilir. İşte bu durumda onarımı mümkün ekipman, makine veya sistemlerin bakım programları yapılarak arıza yapmadan bakımının planlanması ya da bu ekipman, makine veya sistemin değiştirilmesi gerekir.

Bileşenlerin ve sistem fonksiyonlarının düzenli testi güvenirliğin sağlanması için etkili bir yöntem olabilir. Ancak değişik alt sistemlerin ve önemli bileşenlerin çalışıp çalışmadığının düzenli ve sık aralıklarla test edilmesini gerektirir. Eğer hatanın mevcudiyeti direk olarak görülemiyorsa özellikle kritik ekipman ve sistemler açısından bunun büyük önemi vardır. Ekipman veya sistemdeki hatanın gizli olarak artması demek, güvenlik fonksiyonunun ihtiyaç anında çalışmaması anlamına gelmektedir. Sistem güvenliğinin sağlanması için güvenirlik teorisi ve olasılık hesaplamalarının kullanılmasını gerektirir.

Diğer anahtar kavramlar ise Arızalar Arası Ortalama Süre (MTBF) ve Arızaya Kadar Geçen Ortalama Süre (MTTF)'dir. İki kavram birbirine benzerdir ama aynı değildir. MTBF, onarım yapılan malzeme grubuna veya sisteme uygulanır. Bu, toplam operasyon süresinin gerçekleşmeme sayısına bölünmesinden türetilmiş ortalama zamandır. Bundan farklı olarak, MTTF onarılamayacak durumdaki sistemlere uygulanır.

Güvenilirlik merkezli bakım (RCM), bütün ekipman türleri için gerekli güvenlik ve kullanılabilirlik hususları ve ekipmanın işleyişini verimli ve etkili biçimde sağlamak amacıyla arızaları yönetmek için uygulanması gereken ilkeleri tanımlamaya yönelik bir yöntemdir. RCM, sanayide geniş bir yelpazede kullanılan kanıtlanmış ve kabul görmüş bir yöntemdir. RCM, tanımlanabilir hataların güvenlik, işlemsel ve ekonomik sonuçları ve bu hataların sorumlu olduğu bozulma mekanizmasına uygun olarak ekipman için uygun ve etkili önleyici bakım gereksinimlerini belirlemeye yönelik bir karar süreci sağlar. RCM analizi, ekipmanın yaşam süreci boyunca işlemsel olarak gösterdiği değişiklikler yanında diğer eylem veya bakım görevlerinin gerçekleştirilme gerekliliği ile ilgili olarak yapılan bir analiz türüdür.

Referans Standartlar:

- IEC 60300-3-11, Güvenilirlik Yönetimi – Bölüm 3-11: Uygulama Kılavuzu – Güvenilirlik Merkezli Bakım (Dependability management – Part 3-11: Application Guide – Reliability Centred Maintenance)

Analiz, elipmanın yaşam döngüsü boyunca güvenilirliğine ve üreticiden sağlanan ekipmana ait işlemsel veya ekonomik bilgilerine dayanmaktadır. Bununla birlikte, üretici tarafından düşünülen ölçütlerin ürün ve uygulamasının türüne bağlı olacağı belirtilmelidir. En büyük faydası, kritik ekipmanların hangi ciddi güvenlik hatalarına, çevresel, ekonomik veya işlemsel etkilere sahip olacağının analizini yapabilmesidir.

RCM, uygulanabilir ve etkili bakımın gerçekleştirilmesini ve genel olarak tasarım ve gelişme aşaması boyunca ve işlem ve bakım süresince ekipmanların hatasız kullanımını sağlamak için kullanılmaktadır.

Girdi:

RCM'nin başarılı uygulaması ekipman ve yapısı, operasyonel çevre ve ilişkili sistemler, alt sistemler ve olası arızalar ve bu arızaların sonuçları ile birlikte ekipman öğelerinin iyi bir şekilde kavranılmasını gerektirir.

Hata Verisi ve Hesaplamalar:

Güvenirlik tekniklerinin kullanımı, bileşenler ve sistem hata verileri ve aynı zamanda onarıma ayrılan zamanlar hakkında bilgi sahibi olmayı gerektirir. Veri bankalarından veya teknik literatürden toplanabilir. Veriye ulaşılamaması durumunda güvenilirlik ve olasılık teoremleri için geçmişe dayalı tahminler kullanılabilir. Hesaplamalar ileri matematiksel tekniklerin uygulanmasını gerektirebilir. Zaten, asıl zorluk verinin toplanmasında ve değerlendirilmesinde ortaya çıkmaktadır. Bir problem de teknolojinin hızlı oranda gelişmesidir. Bileşenlerin yeni versiyonları o kadar kısa zaman aralıklarında ortaya çıkmaktadır ki, bu ekipman veya sistemlerin güvenirlikleri hakkında yeterli bilgi elde etmek için gereken süre yetersiz kalabilmektedir.

Süreç:

Bir RCM programının ana adımları aşağıdaki gibidir:

- Başlatma ve planlama,
- İşlevsel arıza analizi,
- Görev seçimi,
- Uygulanma aşaması,
- Sürekli gelişim.

RCM, risk değerlendirmesindeki ana adımları takip ettiği için risk merkezlidir. Risk değerlendirme türü bir hata modu, etkisi, kritik olma durumu analizidir (FMECA) ancak bu bağlamda kullanıldığında, analiz için özel bir yaklaşıma ihtiyaç duyar. Risk tanımlama, bakım görevleri tarafından gerçekleştirerek sıklık ve/veya sonuçta azaltılabilen veya ortadan kaldırılabilen potansiyel hatalardaki durumlara odaklanır.

Bu analiz, ekipmanlara ait gerekli işlevler ve performans standartları dikkate alınarak bu ekipmanların işlevlerini yarıda bırakmaları veya ekipman ve bileşen arızaları tarafından işlevin tamamının gerçekleştirilememesi durumunda ortaya çıkacak sonucun etkisinin belirlenmesi şeklinde yapılır, ayrıca bu sonucu önlemek üzere ekipmana yapılması gerekli bakım programın geliştirilmesi veya ekipmanın ömür tahminini yapmak için de kullanılır. RCM risk analizi, ekipman için gerçekleştirilen bakım olmadan meydana çıkabilecek her bir arıza (hata) sıklık tahmininden oluşur, sonuçlar hata etkileri belirlenerek oluşturulur. Risk seviyeleri, arıza sıklığı ve sonuçlarını içeren bir risk düzeyidir. Risk değerleme, her bir hata modu

için uygun arıza (hata) yönetim politikası seçilerek gerçekleştirilir. Tüm RCM süreci yoğun olarak gelecek referans ve incelemesi için belgelenir, bu belgeleme arıza ve bakım ile ilgili verilerinin toplanması, gelişmelerin uygulanması ve sonuçların izlenmesini sağlar.

Çıktılar:

RCM durum izleme, planlanan restorasyon, planlanan yenileme, arıza bulma veya mevcut olmayan önleyici bakım gibi bakım görevlerinin tanımlanmasını sağlar. Diğer olası eylemler, yeniden tasarım, işletim değişiklikleri veya bakım prosedürleri ya da ek eğitim içerebilen analizden kaynaklanır. Görev aralıkları ve gerekli kaynaklar zamanı geldiğinde tespit edilir.

11.27. Gizlilik Analizi (Sneak Analysis -SA) ve Gizlilik Devre Analizi (Sneak Circuit Analysis -SCI)

Sistemlerin diğer boyutu üretim sisteminin çalışma döngüsü yaklaşımını ve oluşabilecek bütün değişik durumları içerir. Güvenlik önlemleri planlama, tasarım, üretime başlangıç, operasyon ve çalışmanın olmadığı durumlarda uygulanmalıdır. Operasyonel durum hem normal hem ve durdurulmuş üretim, bakım ve sistem değişimini içerir. Sneak analizi (SA) tasarım hatalarını tanımlayan bir yöntemdir. Bir gizlilik durumu, istenmeyen bir olayın meydana gelebileceği veya istenen bir olayı önleyebileceği ve bileşen arızasından kaynaklanmayan gizli bir donanım, yazılım veya entegre bir durumdur. Bu koşullar, en dikkatli standart sistem testleri yapılsa bile sistemin yaşam döngüsü süresince tespitten kaçmak için rastgele tür ve yetenekte gizlenmiş hatalar olarak karakterize edilmiştir. Gizlilik durumları, uygunsuz işlem, sistem geçerlilik kaybı, program gecikmeleri veya personele yönelik sakatlanma hatta ölüme sebep olabilir.

Sneak Devre Analizi (Gizlilik devre analizi), tasarımların bütünlüğünü ve işlevselliğini doğrulamak adına NASA tarafındann 1960'ların sonunda geliştirilmiştir. SCA, kasıtsız olarak elektrik devre yollarındaki gizli hataları keşfetmek için yararlı bir araç olarak hizmet etmiş ve her bir işlevdeki olası hataları bulmak ve çözüm üretmede yardımcı olmuştur. Bununla birlikte teknoloji ilerledikçe, gizlilik devre analizini gerçekleştirebilmek için araçlar geliştirilmek zorunda kalınmıştır. Gizlilik analizi, gizlilik devre analizinin kapsamını içermekte ve aşmaktadır. Her türlü teknoloji için hem donanım hem de yazılımda problemlerin yerini tespit edebilecek bir analiz türüdür. Gizlilik analiz araçları, zaman tasarrufu ve proje giderleri, tek bir analiz ile hata ağaçları, arıza modu ve etkiler analizi (FMEA), güvenilirlik tahminleri vb. gibi pek çok analizle bütünleştirilebilir.

Girdi:

Gizlilik analizi, problemin özel bir türünü bulmak amacıyla farklı araçlar, gizlilik durumlarını tanımlamak için analiste yardım etmeye yönelik ağ ağaçları ve ipuçları veya sorular kullanır. Ağ ağaçları, devre çizimleri güncel sistemin topolojik yapısını verir. Her bir şebeke ağacı, bir alt işlevi temsil eder ve alt işlev çıktısını etkileyebilecek bütün girdileri gösterir.

Süreç:

Gizlilik analizi gerçekleştirilirken uygulanacak temel adımlar şunlardan oluşmaktadır:

- Veri hazırlama,
- Ağ ağacının oluşturulması,
- Ağ yollarının değerlendirilmesi,
- Nihai öneriler ve rapor.

Çıktılar:

Bir gizlilik devresi, belirli koşullar altında, bir sistem içerisinde beklenmeyen bir yol veya mantık akışıdır, istenmeyen bir işlevi başlatabilir veya istenen bir işlevi engelleyebilir. Yol, donanım, yazılım, operatör eylemleri veya bu üç elementin kombinasyonlarını kapsayabilir. Gizlilik devreleri, donanım arızasının sonucu değildir ancak sistem içerisine dikkatsizce tasarlanmış, yazılım programı içine kodlanmış veya insan hatası tarafından tetiklenen gizli durumlardır. Gizlilik devrelerinin dört kategorisi mevcuttur:

- **Gizlilik yolları:** İstenmeyen bir yönde, akım, enerji veya mantıklı sıralama akışları boyunca beklenmeyen yollar,
- **Gizlilik zamanı:** Beklenmeyen veya çakışan bir sıralama meydana getiren olaylar,
- **Gizlilik durumları:** İstenmeyen bir eylem almaya yönelik sistem veya bir operatör davranışına sebep olacak, sistem işlem durumlarının belirsiz veya yanlış eylem durumları,
- **Gizlilik etiketleri:** Sistem işlevlerinin hatalı veya belirsiz etiketlemesi, örneğin bir operatörün sisteme hatalı bir uyarıcı girmesine sebep olabilecek sistem girdileri, kontroller, ekran araçları.

Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler şunlardır:

- Gizlilik analizi tasarım hatasının tanımlanması için uygundur,
- HAZOP ile birlikte uygulandığında en verimli şekilde çalışır,
- Toplu ve yarı kesikli tesis gibi birden fazla duruma sahip olan sistemler için uygundur.

Sınırlılıklar şunları içerebilir:

- Süreç oldukça farklıdır,
- Süreç, elektriksel devrelere, proses tesislerine, mekanik ekipman veya yazılıma uygun olunup olunmamasına bağlı olarak kısmen farklıdır, bu nedenle çok yüksek bilgi düzeyi gerektirir,
- Yöntemin başarısı, doğru bir şebeke ağacı veya hata ağacı kurulmasına bağlıdır.

11.28. Markov Analizi (Markov Analysis)

Markov analizi, yalnıza mevcut duruma bağlı bir sistemin gelecek durumlarda nasıl cevap verebileceğini analiz etmek maksadı ile kullanılır. Birden fazla durumda var olabilecek sonuçların, güvenilir bir blok diyagram analizi kullanılarak analiz edilmesini sağlar. Onarılabilir sistemlerin analizi için yaygın biçimde kullanılır. Yöntem, daha yüksek mertebede Markov süreçleri kullanılarak daha karmaşık sistemlere de uyarlanabilir.

Referans Standartlar:

- *IEC 61078, Bağımlılık için analiz teknikleri- Güvenilirlik blok diyagram ve Boole yöntemleri (Analysis Techniques for Dependability – Reliability Block Diagram and Boolean Methods)*
- IEC 61165, *Markov tekniklerinin uygulanması (Application of Markov Techniques)*
- ISO/IEC 15909 (bütün bölümler), *Yazılım ve sistem mühendisliği – Yüksek seviyeli Petri ağlar (Software and Systems Engineering – High-Level Petri Nets)*

Markov analiz süreci kantitatif bir tekniktir ve ayrık (durumlar arasında değişik olasılıklar kullanarak) veya sürekli (durumlar boyunca değişim oranları

kullanarak) durumlar için kullanılabilir. Bir Markov analizi elle yapılabilir, ancak bu teknik daha çok birçoğu piyasada var olan bilgisayar programlarının kullanımı ile gerçekleştirilir.

Markov analiz tekniği çeşitli sistem yapılarında onarım ile veya onarım olmaksızın kullanılabilir ve şunları içerir:

- Paralel bağımsız bileşenler,
- Seri bağlı bileşenler,
- Yük- Paylaşım Sistemleri,
- Destek sistemleri.

Markov analiz tekniği, onarım için yedek bileşenlerin dikkate alınması dahil sistemin veya ekipmanın kullanılabilirlik analizi için de uygun bir analiz türüdür.

Girdi:

Markov analizi için gerekli girdiler aşağıdaki gibidir:

- Sistem, alt sistem veya bileşen içerisinde olabilen çeşitli durumların bir listesi, (örneğin; tamamen işlevsel, kısmi olarak işlevsel (yani bozulmuş bir hal), başarısız durum, vb.),
- Modellenmesi gerekli olan olası geçişlerin açıkça kavranması. Örneğin, bir araba lastiği arızasında yedek lastiğin ve dolayısıyla denetleme sıklığının dikkate alınmasını gerektirir,
- Bir durumdan diğer bir duruma değişim oranı, genellikle ya ayrı olaylar için durumlar arası bir değişim olasılığı ya da arıza oranı (λ) ve/veya bilinçli olaylar için onarım oranı (μ) tarafından temsil edilir.

Süreç:

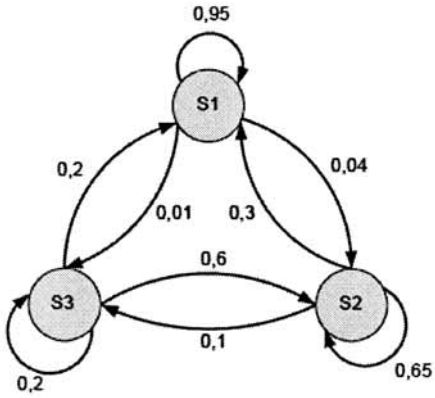
Markov analiz tekniği 'durumlar', yani 'geçerli' ve 'başarısız' konsepti etrafında merkezlidir ve bu iki durum arasında zamanla sürekli bir değişim olasılığına dayanır. Bir rastgele geçiş olasılık matrisi çeşitli çıktıların hesaplanmasına izin veren durumların her biri arasında geçiş tanımlaması için kullanılır. Markov analiz tekniğini yansıtmak için, sadece üç durumda olabilen karmaşık bir sistem düşününüz; işleyiş, bozulmuş ve başarısızlık durumları sırasıyla S1, S2, S3 olarak tanımlanır. Her gün, bu üç durumdan biri sistemde var olur. **Tablo 46** yarın olasılığını gösterir, 1, 2, veya 3'ün olabildiği yerde sistem Si durumundadır.

Tablo 46: Markov Matrisi

		Durum Bugün		
		S1	**S2**	**S3**
Durum Bugün	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

Bu olasılıklar dizisine Markov matrisi veya geçiş matrisi denir. Her durumda bütün olası çıktıların toplamı olduğundan her bir sütun toplamı 1'i verir. Sistem, aynı zamanda dairelerin durumlarını temsil eden bir Markov şeması ile gösterilir ve oklar, eşlik eden olasılık ile birlikte bir geçişleri temsil eder. Oklar genellikle bir durumdan diğer duruma geçişleri gösterir.

Şekil 48: Markov Şema Sistemi Örneği



Sonuç:

Markov analizinden elde edilen sonuç, farklı durumlarda olma olasılıkları ve böylece hata olasılıkları ve\veya kullanılabilirliğin bir tahminidir.

Güçlü Yönler ve Sınırlılıklar:

Markov analizinin güçlü yönleri aşağıda gösterildiği gibidir:

- Çok sayıda kısıtlanmış durum ve bir onarım yeteneğine sahip sistemlere yönelik olasılık hesaplaması yapılabilir.

Markov analizinin sınırlılıkları aşağıda gösterildiği gibidir:

- Durum; arıza ya da onarım değişiminin sabit olasılıklarının varsayımını gerektirir,
- Gelecekte yaşanabilecek olaylar, hemen önceki olay dışında bütün geçmiş olaylardan bağımsız olduğu için, tüm olaylar istatistiksel olarak bağımsız olarak kabul edilir,
- Tüm durum değişikliği olasılıklarına yönelik bilgi gereksinimi gerektirir,
- Matris işlemleri ile ilgili (matematiksel teoremler dahil) yüksek bilgi gerektirir,
- Sonuçları teknik departmanlar dışındaki personellere aktarmak güçtür.

11.29. Monte Carlo Simülasyonu (Monte Carlo Simulation)

Birçok sistem, analitik teknikler kullanılarak üzerinde belirsizlik etkilerinin biçimlendirilmesi konusunda oldukça karmaşıktır, ancak istenmeyen sonucun muhtemel N çıktılarını elde etmek amacıyla girdi örnekleme ile N sayısında hesaplamalar (simülasyon) gerçekleştirerek ve girdileri rastlantısal değişkenler olarak düşünerek değerlendirilebilir.

Referans Belgeleri:

- IEC 61649, Weibull Analizi (Weibull Analysis)
- IEC 62551, Güvenilirlik İçin Analiz Teknikleri - Petri Ağ Teknikleri (Analysis Techniques for Dependability – Petri Net Techniques)
- ISO /IEC Klavuzu 98-3:2008, Belirsizlik Önlemi – Bölüm 3: Önlemlerdeki (GUM:1995) Belirsizliğe Karşı Kılavuz (Uncertainty Measurement – Part 3: Guide to The of Uncertainty in Measurement (GUM:1995))

Bu yöntem, analitik yöntem ile anlaması ve çözümlemesi oldukça zor olan karmaşık durumların üzerine gidebilir. Sistemler, hesap tabloları ve diğer bilinen araçlar kullanılarak geliştirilebilir, ancak günümüzde karmaşık sistemleri analiz etmek amacı ile kullanılan daha karmaşık araçlar mevcuttur.

Monte Carlo Simülasyonu, analistlere belirsizliğin çok çeşitli durumlardaki sistemler üzerindeki etkisini değerlendirme olanağını sağlar. Genellikle, muhtemel sonuç çeşitliliğini, masraf, süre, üretilen iş, talep ve benzer ölçümler gibi bir sistemin kantitatif ölçümlerine yönelik bu çeşitlilikteki değerlerin göreceli sıklığını değerlendirmek için kullanılır. Monte Carlo simülasyonu iki farklı amaç için kullanılabilir:

- Geleneksel analitik modeller üzerindeki belirsizliklerin tahmini,
- Analitik teknikler işe yaramadığında olasılıksal hesaplamalar.

Girdi:

Monte Carlo simülasyonuna yönelik girdi, sistemin çeşitleri girdileri olabilir ve bu bilgiler, belirsizlik içerebilir. Belirsizlik içeren girdi verileri, belirsizliklerin seviyesine göre, daha fazla ya da daha az yaygın olan dağılımlar ile rastlantısal değişkenler olarak gösterilir. Tekdüze, üçgen, normal ve log normal dağılımlar, genellikle bu amaç için kullanılır.

Süreç:

Süreç aşağıdaki gibidir:

- Çalışılan sistemin tutumunu mümkün olduğunca yakın bir şekilde gösteren bir model ya da algoritma tanımlanır,
- Model, modelin sonuçlarını elde etmek için rastlantılı sayılar kullanarak birçok kez çalıştırılır (sistemin simülasyonları); uygulamanın belirsizlik etkilerini biçimlendireceği zaman, model, girdi parametreleri ve bir sonuç arasındaki ilişkiyi sağlayan bir denklem formundadır. Girdilere yönelik seçilen değerler, bu parametrelerdeki belirsizlik yapısını gösteren uygun olasılık düzenlemelerinden alınır,
- Diğer durumda, bir bilgisayar, farklı girdilerle modeli defalarca (genelde 10,000 defaya kadar) çalıştırır ve birçok çıktı üretir. Bunlar, ortalama değerler, standart sapma, güven aralıkları gibi bilgileri sağlamak için bilinen istatistikleri kullanarak işlenir.

Çıktılar:

Sonuç tek bir değer olabilir. Olasılık veya sıklık dağılımı olarak ifade edilen bir sonuç da olabilir ya da çıktı üzerinde en büyük etkiye sahip olan model içinde bulunan ana fonksiyonları tanımlayabilir. Girdiler ve çıktılar arasındaki ilişkilerin analizi iş yerindeki etkenlerin önemine büyük ölçüde ışık tutabilir.

Güçlü Yönler ve Sınırlılıklar:

Monte Carlo analizinin güçlü yönleri şunlardır:

- Prensip olarak yöntem, ilgili sistemlerin gözlemlerinden ortaya çıkan deneyime dayalı dağılımları içeren bir girdi değişkenindeki herhangi bir

dağılımı analiz edebilir,

- Model geliştirilmek için nispeten basittir ve ihtiyaç duyulduğunda analiz detaylandırılabilir,
- Koşullu bağımlılıklar gibi çözümü zor etkiler dahil olmak üzere gerçekte meydana gelebilece etkiler veya ilişkileri ortaya çıkarır,
- Girdi ve çıktılar arasındaki ilişki şeffaf olduğundan, modeller kolaylıkla anlaşılabilir,
- Monte Carlo simülasyon amaçları için çok verimli olduğunu kanıtlayan Petri Ağları (IEC 62551) gibi etkin davranış modelleri mevcuttur,
- Yazılım ile hızlı bir şekilde gerçekleştirilebilir.

Sınırlılıklar aşağıdaki gibidir:

- Çözümlerin doğruluğu, gerçekleştirilebilen simülasyonların sayısına bağlıdır (bu sınırlama artan bilgisayar hızları sayesinde giderek önemini kaybetmektedir),
- Büyük ve karmaşık modeller, modelleyicileri zorlayabilir ve tarafların süreç ile ilgilenmesini zorlaştırabilir,
- Yüksek sonuçlu veya düşük olasılıklı teknik olayları yeterince tartamayabilir.

11.30. Bayes İstatistiği ve Bayes Ağları (Bayesian Statistics and Bayes Nets)

Güvenliğin ilgilendiği temel bir açı da organizasyondur. Makinelerin nasıl tasarlandığı ve bakımının yapıldığı, iş yöntemlerinin nasıl planlandığı ve denetlendiği hakkında yol gösterir. Güvenliği değişik şekillerde etkileyen çok çeşitli durum vardır. Kazaların açıklaması geniş değişkenlik gösterir, ve düzenli, yaygın kullanımlı teori yoktur. Fakat kazaların analizinin çeşitli yöntemlerinde kazaların nasıl oluştuğuna dair açık bir model mevcuttur.

Kazayı, bir olayın ürünü ve sadece bir açıklamasının olduğunu düşünerek kazanın değerlendirilmesi "neden" için kullanılan en genel bakış açısıdır. Basit ifade ile gerçekliğin sadece bir kısmını ele alan zorluk, problemlerin etkili şekilde çözümünü engelleyebilir.

Bu nedenle, açıklama ve teoriler, genellikle kazaların neden meydana geldiği ve nasıl önlenebileceği hakkında yeterli anlayış sağlaması nedeniyle yararlıdır. Bu konuda çok sayıda değişik model ve istatistiki yöntem mevcuttur, bunlardan birisi de BAYES ağlarıdır.

Bayes istatistiği klasik istatistiklerden farklıdır, ki tüm dağılım parametrelerinin sabit olduğunu kabul etmez, ancak bu parametreler rastlantısal değişkenlerdir. Fiziksel kanıtlara dayalı olan klasik bir olayın aksine kişinin belli bir olay üzerindeki inanç derecesi olarak ele alındığında, bir Bayes olasılığı daha kolay anlaşılabilir. Bayes yaklaşımı olasılığın öznel yorumuna dayalı olduğunu için karar düşüncesine ve Bayes ağlarının (ya da Düşünce Ağları, düşünce çevreleri ya da Bayes Ağları) geliştirilmesine yönelik hazır bir taban oluşturur.

Bayes ağları bir değişkenler kümesini ve olasılıksal bağlantılarını göstermek için bir grafik modeli kullanmaktadır. Ağ, bir rastlantısal değişkeni ve bir üst düğümü alt düğüme bağlayan okları temsil eden düğümlerin oluşumudur.

Son yıllarda Bayes Teorisi ve Ağların kullanımı, yazılım hesaplama araçlarının kullanılabilirliğinden dolayı yaygın hale gelmiştir. Bayes ağları çok kapsamlı konularda kullanılmaktadır, yapısal bağlantılar ve verilerin kullanımı yoluyla bilinmeyen değişkenler hakkında bilgi bulmak için ihtiyaç duyulan her alanda değerli olabilir. Bayes ağları bir sorun alanı ile ilgili kavrayış sağlamaya ve müdahale sonuçlarını tahmin etmeye yönelik nedensel bağlantıları öğrenmek için kullanılabilir.

Girdi:

Girdiler, Monte Carlo modeline yönelik girdiler ile benzerlik göstermektedir. Bir Bayes ağı için alınması gereken örnek adımlar aşağıdakileri içermektedir:

- Sistem değişkenlerini tanımlamak,
- Değişkenler arasındaki nedensel bağlantıları tanımlamak,
- Koşullu ve önceki olasılıkları belirlemek,
- Ağ için deliller eklemek,
- Düşünce gelişimini gerçekleştirmek.

Sonuç:

Bayes yaklaşımının son zamanlarda rağbet görmesinin nedeni, sonraki dağılımları elde etmek için Bayes ağları ile ilişkili olmasıdır. Grafik sonuçları daha kolay anlaşılabilir bir model sağlamaktadır ve veriler değişkenler arasındaki ilişkiyi ve parametrelerin hassasiyetini dikkate almak için rahatlıkla değiştirilebilir.

11.30.1. Bayesgil Çıkarsama (Bayesian Inference)

Herhangi bir zaman serisi içerisinde, meydana gelebilecek bir tehlikenin olasılığını ve izleyeceği seyri ve söz konusu hasarın alacağı değerleri tahmin edebilmek risk değerlendirmesinin ana amacıdır. Ancak bir sistemde arızaya neden olucak veya tehlike yaratabilecek birçok etken vardır ve bunların kaza oluşumuna etkisini belirlemek de son derece güçtür. Özellikle algoritmalar ile karmaşık ve doğrusal olmayan ilişkiler klasik yöntemlere göre daha iyi analiz edilebilmekte, tahminleme konusunda çok başarılı sonuçlara ulaşılmaktadır.

Klasik istatistikte, bir modelin parametrelerinin sabit olduğu fakat bilinmediği varsayılır. Ancak, Bayesgil yaklaşımda, modelin parametrelerinin de rassal değişken olduğu varsayılmaktadır. X'in gözlemlenmiş verileri (örn. operasyonel riskten kaynaklanan kayıpları), θ'nın ise modelin parametrelerini ifade ettiğini varsayalım. Bayes teoremi, X verilerinin gözlemlenmesinden sonra, θ'nın X'e bağlı koşullu olasılık dağılımının bulunmasında kullanılır. Bayes teoremi kullanılarak, söz konusu dağılıma şu şekilde ulaşılabilir:

$$P(\theta \mid X) = \frac{P(\theta)\, P(X \mid \theta)}{P(X)} = \frac{P(\theta)\, P(X \mid \theta)}{\int P(\theta)\, P(X \mid \theta) \partial\, \theta}$$

Yukarıdaki denklemde p(X) bir ölçeklendirme sabiti olarak görev yaptığından, Bayes teoremi yaygın olarak şu şekilde ifade edilmektedir:

$p(\theta|X) \propto p(\theta) * p(X|\theta)$ yani;

Son dağılım $\propto$ Ön dağılım * Olabilirlik fonksiyonu

Ön olasılık dağılımı, verinin gözlemlenmesinden önce parametre değerlerine (θ) ilişkin var olan kanılar ile oluşturulan olasılık dağılımıdır. Diğer bir deyişle ön olasılık dağılımı, θ hakkındaki bilgi birikimini (ya da tahmini) yansıtır. Sübjektif veriler, ön olasılık dağılımının oluşturulmasında kullanılır. Olabilirlik fonksiyonu, parametreler veri iken örneklemin olabilirliğini ifade eder. Objektif veriler kullanılarak olabilirlik fonksiyonu oluşturulur. Son dağılım ise, ön olasılık dağılımı ve olabilirlik fonksiyonunun çarpımı ile ifade edilir. Yani ön kanıları ve örneklemden

elde edilen bilgiyi bir araya getiren bir dağılımdır. Bayes teoremi ön olasılıkların revizyonunu sağlar.

Parametre tahmininin sadece objektif verilere dayanılarak yapılması gerektiğini savunan kişilerce, sübjektif değerlendirmeleri de dikkate alan Bayesgil yöntemlere karşı çıkılmaktadır. Ancak Bayesgil çıkarsamanın, klasik çıkarsamaya göre bazı önemli üstünlükleri bulunmaktadır:

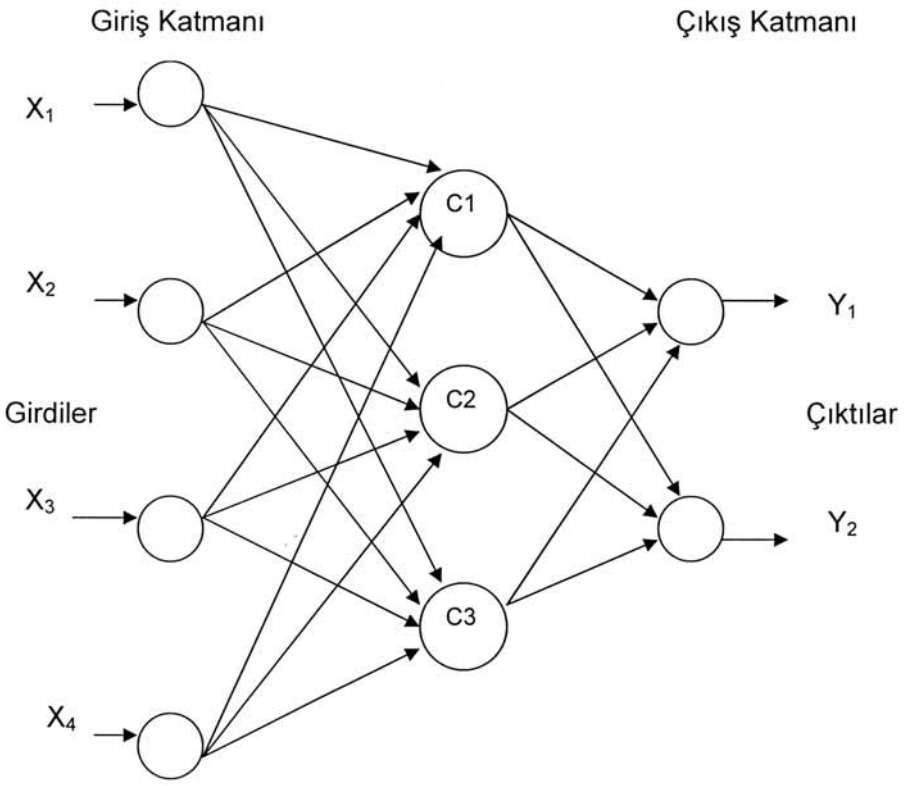
- ➢ Objektif ve sübjektif verileri -istatistiksel temellere dayandırarak- bir araya getirebilir. Bu sayede, sadece iç kayıp verileriyle sınırlı kalınmayarak, ileriye dönük bir yapı oluşturulabilir,
- ➢ Objektif ve sübjektif verilerden hangisi daha güvenilir/kesin ise, parametre tahmini sadece o veriler kullanılarak elde edilerek, sonuca daha yakın olunur,
- ➢ Bayesgil metotlarda, sübjektif veriler sürece sadece ön olasılık dağılımı aracılığı ile dahil edilebilmektedir ve bu sayede süreç kolayca denetlenebilmektedir,
- ➢ Ön olasılık dağılımlarının oluşturulabilmesi için süreçler, faaliyetler bazında operasyonel risklerin belirlenmesi ve değerlendirilmesi gerektiğinden, operasyonel risk yönetimini ve kültürünü geliştiren bir yöntemdir.

11.30.2. Bayes Ağları

Bayes ağları, bir riskin ortaya çıkmasına yol açan faktörlerin olasılık dağılımı ile riskin çok değişkenli olasılık dağılımı arasındaki ilişkiyi kuran istatistiksel bir modeldir. Bayes ağları, rassal değişkenleri temsil eden düğümler (nodlar) ve bu değişkenler arasındaki neden-sonuç ilişkisini temsil eden bağlantılardan oluşur. Şekil 46'da basit bir Bayes ağının çatısı görülmektedir.

X_1, X_2, X_3 ve X_4 giriş katmanı düğümleri, C_1, C_2 ve C_3 gizli katman düğümünü etkileyen faktörleri temsil etmektedir. Operasyonel risk yönetimi açısından bakıldığında, C_1, C_2 ve C_3 gibi risklerin gerçekleşme ihtimalinde etkisi olan ve "başlangıç düğümü" adı verilen faktörler, risk yöneticilerince belirlenmiş olan anahtar risk faktörlerini (key risk drivers) temsil edebilir.

Şekil 49: Basit Bayes Ağı



"Hedef düğüm" adı verilen C ise anahtar risk göstergelerini (key risk indicators) temsil edebilir. Ağdaki her bir değişken için sübjektif kanılara dayanılarak bir ön olasılık dağılımı belirlenir. Bayesgil analiz sürecinde, ağdaki değişkenlere ilişkin yeni bilgiler edinildikçe sübjektif tahminler iyileştirilir. Aşağıda yer alan adımları izleyerek, Bayes ağlarını oluşturmak mümkündür:

➢ Öncelikle ağ topolojisi oluşturulmalıdır. Diğer bir deyişle, uzman görüşlerinden faydalanılarak değişkenler ve bu değişkenler arasında neden-sonuç ilişkisi belirlenmeli ve bir operayonel kayıp modeli oluşturulmalıdır. Ağ topolojisi, uzmanların ilgili operasyonel riskin oluşum sürecini nasıl yorumladığını yansıtır, dolayısıyla ağ topolojisini oluşturmanın tek bir yolu yoktur.

➢ Bayes ağında yer alan "başlangıç düğümleri"nin tümü için olasılık dağılımı saptanmalıdır. Ayrıca hedef düğümlerinin başlangıç düğümlerine bağlı koşullu olasılık dağılımları saptanmalıdır. Sözkonusu olasılık dağılımları, parametreler hakkında sahip olunan ön bilgiler ışığında oluşturulur. Bu olasılık dağılımlarının oluşturulmasının ardından, bu dağılımlar kullanılarak hedef düğümlerinin olasılık dağılımları hesaplanabilir.

➢ Operasyonel risklerin daha etkin yönetilmesi için, oluşturulan bir Bayes ağı karar ve fayda düğümleri eklenerek geliştirilebilir. Bu sayede, hedef düğümünde yer alan bir operasyonel riskin azaltılması için uygulanacak kontrolün maliyetinin, sağladığı yarardan daha düşük olup olmadığı belirlenebilir.

Operasyonel risk yönetiminde, hedef düğümleri olay türü/faaliyet kolu bazında kayıp olaylarının sıklığını ve şiddetini temsil eden bir Bayes ağı oluşturulabilir. Diğer bir deyişle, oluşturulan Bayes ağı, sıklık ve şiddet dağılımlarını, anahtar risk faktörlerinin bir fonksiyonu olarak modelleyebilecektir. Ayrıca, kapsamlı bir şekilde oluşturulan sözkonusu Bayes ağında olay türü/faaliyet kolları arasındaki korelasyonlar da dikkate alınmış olacaktır.

Bayes ağları kullanılarak senaryo analizi ve nedensellik analizi yapılabilir. Aslında, Bayes ağlarının en güçlü yönlerinden biri bu analizlerin kolayca yapılabilmesine imkan tanımalarıdır:

➢ **Senaryo Analizi:** Bayes ağı kullanılarak, risk faktörlerinin olasılıklarının değiştirilmesinin riskin gerçekleşme olasılığı ve dolayısıyla kayıp tahmini üzerindeki etkisi incelebilir.

➢ **Nedensellik Analizi:** Operasyonel kayıp olaylarına ilişkin yeni veriler ışığında, anahtar risk faktörlerinin (başlangıç düğümlerinin) olasılıklarının güncellenmesidir. Meydana gelen operasyonel kayıp olaylarının nedenlerinin analiz edilmesi açısından kullanışlı bir yöntemdir.

Güçlü Yönler ve Sınırlılıklar:

Güçlü Yönler şunlardır:

- Öncekiler ile ilgili gerekli olan her şey bilgidir,
- Çıkarımsal ifadeleri anlamak kolaydır,
- Bayes kuralı gerekli olan unsurdur,
- Bir problem üzerinde öznel düşünceler kullanmak için bir mekanizma sağlar.

Sınırlılıklar:

- Karmaşık sistemler için Bayes ağlarındaki tüm etkileşimleri tanımlamak sorunludur,
- Bayes yaklaşımı genellikle uzman görüşü ile sağlanan koşullu olasılıkların çokluk bilgisine ihtiyaç duymaktadır. Yazılım araçları sadece bu varsayımlara dayalı cevaplar sağlayabilir.

11.31. F-N Eğrileri (F-N Curves)

Büyük organizasyonların, yaşanan endüstriyel kazalardan öğreneceği ana sonuçlar ve öğrenilecek özel dersler bulunmaktadır. Bu tip büyük endüstriyel kazalar, karmaşık modelde organizasyonel hatalarını ve tehlikeleri kontrol etme yollarındaki zaafiyetleri göstermiştir. Yaşanan bu büyük kazlar özellikle sistemlerin ve proselerin daha gelişmiş güvenlik özelliklerine sahip olması gerektiğini göstermiştir. Ayrıca da özellikle kimya sanayinde yaşanan kazaların teorik olasılığının sık sık bu olasılığı belirlemekle görevli uzmanlar tarafından aşırı düşük olarak belirlendiğini de göstermiştir. Bilindiği üzere özellikle Seveso Direktifi çerçevesinde uzmanların kapsam dahilinde olan bir sanayi kuruluşunda meydana gelebilecek bir büyük endüstriyel kazanın olasılığını ve şiddet derecesini belirlemesi ve kabul edilebilir seviyede olup olmadığını da değerlendirmesi gerekmektedir.

Güvenlik sistemlerinin başarısız olma ihtimali ile ilgili çeşitli araştırmalar ve bu ihtimalleri hesaplamak için de çeşitli risk değerlendirme teknikleri ile birlikte kullanılacak birçok olasılık teoremleri mevcuttur. Sistemlerin planlandığı gibi çalışmaması veya bu sistemlerin zamanla kötüleşmesi güvenlik sitemlerinin tüm olasılıklarını kapsayacak şekilde kaza meydana gelme olasılığının belirlenmesini güçleştirmektedir. İşte bu şamada özellikle İngiltere, Hollanda vb. AB ülkelerinde ALARP seviyesinin belirlenmesi aşamasında özellikle F-N eğrileri kullanılmaktadır.

F-N eğrileri, belirtilen bir grup için belirli bir seviyede zarar veren olayların olasılığının grafiksel bir gösterimidir. Çoğunlukla oluşan belirli sayıda yaralı ve ölülerin sıklığı ile ilgilidir. F-N eğrileri, N veya etkilenecek daha fazla grup üyelerindeki birikimli sıklığı (F) gösterir. N'nin yüksek bir F sıklığı ile oluşabilen yüksek değerleri, ilgilenilmesi gereken konular arasındadır çünkü sosyal ve siyasi açıdan kabul edilemez nitelikte olabilir. F-N eğrileri risk analizleri sonuçlarını gösteren bir analiz türüdür. Birçok olay, düşük etkiye sahip bir sonucun yüksek olasılığına ve yüksek etkiye sahip bir sonucun düşük olasılığına sahiptir.

F-N eğrileri, bir çift sonuç olasılığını ifade eden tek bir nokta yerine, bu oranı ifade eden tek bir çizgi olarak risk seviyesinin gösterilmesini sağlar.

F-N eğrileri riskleri karşılaştırmak için kullanılabilir, örneğin bir F-N eğrisi olarak belirlenmiş kritere karşı tahmin edilen riskleri karşılaştırmak için ya da tarihsel olaylardan elde edilen veriler ile ya da karar kriteri (ayrıca F-N eğrisi olarak ifade edilir) ile tahmin edilen riskleri karşılaştırmak için kullanılabilir. F-N eğrileri sistem veya süreç tasarımı ya da mevcut sistemlerin yönetimi için kullanılabilir.

Girdi:

Girdiler aşağıdaki gibidir:

- Belirli bir zaman dilimi boyunca olasılık sonuç çiftleri grubu,
- Belirli sayıda yaralı ve ölülere yönelik tahmini olasılıkları veren sayısal bir risk analizinden elde edilen veri sonuçları,
- Tarihsel kayıtlar ve sayısal risk analizinden elde edilen veriler.

Süreç:

N olasılıklı, yaralı ve ölü sayısı grafiği (belirli bir zarar seviyesi için, örn. ölüm) ya da koordinatı oluşturan daha fazla yaralı ve ölü sayısı grafiği üzerine mevcut veriler çizilir. Değerlerin geniş aralığından dolayı, her iki eksen normalde logaritmik nitelikli ölçeklerdedir.

F-N eğrileri, geçmiş kayıplardan elde edilen ‘’gerçek’’ sayılar kullanılarak istatistiksel şekilde oluşturulabilir veya simülasyon model tahminleri kullanılarak hesaplanabilir.. Genel olarak, teorik F-N eğrileri daha çok sistem tasarımı için kullanışlı iken; istatistiksel F-N eğrileri daha çok belirli bir mevcut sistem yönetimi için kullanışlıdır. Her iki türev yaklaşımı çok zaman alıcı olabileceği için, bu iki yaklaşımın bir arada kullanılması daha yaygındır.

Çıktılar:

Sonuç; incelenmekte olan alandaki söz konusu riskin sonucunun meydana gelmesi durumunda o alanda yaşayan nüfusun ne kadar zarar göreceğini gösterir ve bu zarar düzeyini önceden belirlenmiş olan kabul edilebilirlik kriterleri (ALARP veya ALARA) ile karşılaştırılabilir.

Güçlü Yönler ve Sınırlılıklar:

F-N eğrilerinin güçlü yönleri şunlardır:

- F-N eğrileri, risk ve güvenlik seviyeleri üzerine karar vermeye yardımcı olmak için yöneticiler ve sistem tasarımcıları tarafından sıklıkla kullanılır,

- Tesisin risk seviyesini göstermenin kullanışlı bir yoludur.
- Aynı zamanda erişebilir bir formatta sıklık ve sonuç bilgilerini de sunan kullanışlı bir yöntemdir.
- F-N eğrileri, verilerin mevcut olduğu benzer durumlardan elde edilen risklerin karşılaştırılması için uygundur.

Sınırlılıklar:

- Bu eğriler farklı tür riskler ile veri miktarının ve kalitesinin değiştiği koşullardaki değişen özellikleri karşılaştırmak için kullanılmamalıdır,
- F-N eğrilerinin bir sınırlılığı da zarar gören insan sayısı dışında gelişen olayların etkilerinin veya sonuçlarının istatistiksel dağılımı hakkında herhangi bir şey söylememesidir,
- Ayrıca hasar seviyesinin oluşmuş olabileceği farklı yönleri tanımlama yolu yoktur. Bu eğriler genellikle insanlara zarar veren türde belirli bir sonucu saptamaktadır,
- F-N eğrileri bir risk değerlendirme yöntemi değildir ancak risk değerlendirme sonuçlarını ifade eden bir yoldur,
- Risk değerlendirme sonuçlarını sunmak için iyi hazırlanmış bir yöntemdir. Ancak yetenekli analistler tarafından hazırlık gerektirmektedir ve uzman olmayan kişiler için yorumlanması ve değerlendirilmesi genellikle zordur.

11.32. Maliyet/Fayda Analizi (Cost/Benefit Analysis- CBA)

Maliyet/fayda analizi, en iyi ya da en karlı seçeneğin benimsenmesi için beklenen toplam maliyetin beklenen toplam kazanca karşı değerlendirildiği risk değerleme sürecinde kullanılabilir. Bununla birlikte, risk değerlendirmesi yaparken, erken aşamalarda maliyet faktörüne ağırlık vermek doğru değildir.

Maliyet/fayda analizi, birçok risk değerleme sisteminin dolaylı bir parçasıdır. Kalitatif veya kantitatif özellikler barındırmanın yanı sıra, bu iki elementin bir kombinasyonunu da içerebilir. Kalitatif CBA, kapsama dahil olan tüm durumları ilgilendiren maliyet ve kazançların maddi değerini hesaplar ve maliyet ile kazançların tahakkuk ettiği farklı dönemler üzerinde çeşitli düzeltmeler yapar.

Elde edilen mevcut net değer (Net Present Value- NPV), risk hakkında verilecek kararlara ilişkin bir girdi niteliği kazanır. Herhangi bir faaliyete yönelik olumlu bir NPV, normal şartlarda faaliyetin gerçekleştirilmesi gerektiğine işaret eder. Ancak, özellikle insan hayatı ya da çevreye zararlı bazı olumsuz riskler için ALARP prensibi uygulanmalıdır. Söz konusu prensip ile riskler, üç bölüme ayrılır:

- Olumsuz risklerin üzerinde bir düzey tahammül edilemez niteliktedir ve olağanüstü durumlar haricinde benimsenmemelidir,
- Risklerin altında yer alan bir düzeyde riskler önemsizdir ve yalnızca düşük seviyelerini koruduklarından emin olunması için gözlemlenmeleri gerekmektedir,
- Bir de risklerin mümkün olduğunca düşük (ALARP) nitelik taşıdığı orta bir düzey mevcuttur.

Söz konusu bölgelerin alt kısmında yer alan düşük riskler için katı bir maliyet fayda analizi uygulanabilir ancak riskler tahammül edilememe düzeyine yakın ise; ALARP prensibinin beklentisi, müdahalenin maliyeti elde edilen kazancı bariz derecede orantısız hale getirmiyorsa müdahale etmek olacaktır.

Maliyet fayda analizi, risk içeren seçenekler konusunda karar alırken kullanılabilir.

Örneğin;

- Riske müdahale edilip edilmeyeceği konusunda bir karar girdisi olarak,
- Risk müdahale yöntemleri arasındaki farkları gözetmek ve en iyi yönteme karar vermek,
- Farklı faaliyet türleri arasında karar vermek.

Girdi:

Girdiler, ilgili paydaşlara yönelik maliyet ve fayda bilgileri ile söz konusu maliyet ve faydaların belirsizlikleri hakkında bilgiler içerir. Soyut ve somut maliyet ve faydalar göz önünde bulundurulmalıdır. Maliyetler; kullanılmış kaynaklar ve olumuz sonuçları kapsarken, faydalar; olumlu sonuçları, kaçınılan olumsuz sonuçları ve muhafaza edilen kaynakları içerir.

Süreç:

Maliyet oluşturan veya fayda sağlayan durumlar tanımlanır. Kapsamlı bir maliyet fayda analizinde tüm durumlar analiz edilir. İlgili tüm paydaşlara yönelik üzerinde durulan seçeneklerin doğrudan ve dolaylı maliyet ve faydaları tanımlanır. Riske müdahale edilip edilmeyeceği konusunda maliyet fayda analizi yapılırken, risk müdahalesi ve risk alma kapsamındaki maliyet ve faydalar mutlaka göz önünde bulundurulmalıdır.

Kalitatif maliyet fayda analizinde tüm somut ve soyut durumlara faydalar tanımlanır, tüm faydalara maddi bir değer atanır (soyut drurumlar ve olaylar ile

faydalar da dahil). Maliyet kısa bir süre için belirlenir (örn; bir yıl). Normal şartlarda faydaların, geçerli bir kıyaslama yapılabilmesi için "günümüzün parası" bazında hesaplanması gerekmektedir. Tüm maliyet ve faydalar, bugünkü değer şeklinde ifade edilir. Tüm paydaşların bütün maliyet ve faydalarına ilişkin bugünkü değerler, mevcut net değer (NPV) elde etmek için bir araya getirilebilir. Olumlu bir NPV, gerçekleştirilen faaliyetin faydalı olduğunu gösterir. Fayda maliyet oranları da kullanılmaktadır. Maliyet veya faydaların düzeyine ilişkin bir belirsizlik söz konusu olursa, ya her iki durum ya da iki durumdan birisi, olasılıkları doğrultusunda baskın gelebilir.

Kalitatif maliyet fayda analizinde, soyut maliyet ve faydalara ilişkin maddi bir değer bulma eğilimi söz konusu değildir. Maliyet ve faydaları özetleyen tek bir değerden ziyade, farklı maliyet ve faydalar arasındaki ilişkiler ve dengeleri kalitattif olarak değerlendirilir. Bunlarla bağlantılı bir diğer teknik ise maliyet etkinliği analizidir.

Çıktılar:

Maliyet/fayda analizinin çıktısı, farkı seçenek ve faaliyetlere ait ilgili maliyet ve fayda bilgileridir. Söz konusu bilgiler, kantitatif olarak mevcut net değer (NPV) ve yıllık iç verim oranı (Internal Rate of Return - IRR) ya da mevcut fayda değerinin mevcut maliyet değerine oranı şeklinde ifade edilebilir. Kalitatif özellikler taşıyan çıktı ise genellikle maliyet ve faydaları karşılaştıran bir tablodur.

Güçlü Yönler ve Sınırlılıklar:

Maliyet fayda analizinin güçlü yönleri şunlardır:

- Tek bir ölçek (para birimi) kullanılarak maliyet ve faydaların karşılaştırılmasına olanak tanır,
- Karar verme şeffaflığı sağlar,
- Kararın tüm hususlarına ilişkin ayrıntılı bilgilerin toplanmasını sağlar.

Sınırlılıklar ise şu şekildedir:

- Kantitatif CBA, ekonomik değerlerin ekonomik olmayan faydalara oranını saptamak için kullanılan yöntemlere bağlı olarak çarpıcı şekilde farklı sayılar verebilir,
- Bazı uygulamalarda geleceğe yönelik maliyet ve faydalar için geçerli bir maliyet miktarı belirlemek zordur,
- Söz konusu yöntem, indirim oranlarını göz ardı eder ve uzun vadeli yatırımlar için gelecekte elde edilebilecek indirim oranlarını yok farz eder.

11.33. Çok Kriterli Karar Analizi (Multi - Criteria Decision Analysis - MCDA)

Burada amaç, bir dizi seçeneğin toplam değerliliğini nesnel ve şeffaf bir biçimde değerlendirmek için belirli kriterler kullanmaktır. Genel hatlarıyla hedef, mevcut seçenekler arasında yöntem tercihi yapmaktır. Analiz, her bir seçenek için toplam bir puan belirlemek adına derecelendirilen ve bir araya getirilen, seçenek ve kriterlerden oluşmuş bir matrisin geliştirilmesini içerir.

MCDA aşağıdaki durumlarda kullanılabilir:

- Tercih edilebilecek olası seçenekler arasından uygunsuz seçeneklerin belirlenmesine yönelik çoklu seçeneklerin karşılaştırılmasını içerir,
- Çok sayıda veya tutarsız kriterler söz konusu olduğunda seçeneklerin kıyaslanmasını sağlar.

Girdi:

Analiz için gereken bir dizi seçenek. Ayrıma varmak için tüm seçenekler arasında eşit şekilde kullanılabilen, hedeflere dayalı kriterler.

Süreç:

Genellikle bilgi sahibi paydaşlardan oluşan bir grup aşağıdaki süreci üstlenir:

- Hedef(ler)i belirlemek,
- Her bir hedefe yönelik nitelikleri (kriter veya performans ölçümlerini) saptamak,
- Nitelikleri hiyerarşik sıraya dizmek,
- Kriterlere karşı değerlendirilecek seçenekleri geliştirmek,
- Kriterlerin önemini belirlemek ve öneme karşılık gelen ağırlıkları kararlaştırmak,
- Kriterler doğrultusunda alternatifleri değerlendirmek. Söz konusu değerlendirme sayı matrisi şeklinde gösterilebilir.
- Çoklu tek-nitelikli sayılar ile tek bir çok -nitelikli sayı kümesini birleştirmek,
- Sonuçları değerlendirmek.

Her bir kriter için ağırlıklandırma işleminin yapıldığı ve her bir seçeneğe ilişkin kriter puanlarının tek bir çoklu-nitelik puanında toplandığı farklı yöntemler mevcuttur. Örneğin; puanlar, ağırlıklı toplam ya da analitik hiyerarşi süreci kullanılarak, ikili karşılaştırmalara dayalı ağırlık ve puanların çıkarılması tekniği

yoluyla kümelenebilir. Tüm bu yöntemler, herhangi bir kriter seçiminin diğer kriter değerlerine dayanmadığı varsayımında bulunur.

Çıktılar:

Seçeneklere ilişkin derecelendirme sırasının gösterimi, en çok tercih edilenden en az tercih edilene doğru bir sıra izler. Söz konusu süreçte matris eksenler kriter ağırlıklı olursa ve her bir seçenek için kriter puanı içerirse, yüksek ağırlıklı ortalamayı geçemeyen seçenekler kapsam dışı bırakılabilir.

Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler şunlardır:

- Etkili biçimde karar alma ve varsayımlar ile sonuçların gösterimi konusunda basit bir yapı sağlar,
- Maliyet/fayda analizine uygun olmayan karmaşık karar problemlerini üstesinden gelinebilir bir hale getirebilir,
- Değişimlerin yapılmasını öngören problemleri mantık çerçevesinde düşünmeye yardımcı olabilir,
- Paydaşların farklı hedeflere ve dolayısıyla farklı kriterlere sahip olduğu zamanlarda uzlaşma sağlanmasına yardımcı olabilir.

Sınırlılıklar aşağıdaki gibidir:

- Önyargı ve karar verme kriterlerinin sağlıksız şekilde seçilmesinden etkilenebilir,
- Çoğu MCDA problemleri, kesin veya tek bir çözüm gerektirmeyebilir,
- Belirtilen tercihler üzerinden veya farklı görüşleri bir araya getirme yoluyla kriter ağırlıklarını hesaplayan yığılma algoritmaları, karara ilişkin doğru dayanağı anlaşılmaz bir hale getirebilir.

11.34. Risk Endeksleri (Risk Indices)

Risk endeksi, sıralamalı ölçekler kullanılarak elde edilen bir puanlama yaklaşımı kullanılarak türetilen bir tahmini riskin yarı sayısal ölçüsüdür. Risk endeksleri benzer kriterler kullanılarak bir dizi riskleri derecelendirmek için kullanılabilir ve böylece bu riskler karşılaştırılabilir. Puanlar her risk bileşenine uygulanır, örneğin; kirletici özellikler (kaynaklar), olası maruziyet yolları, toksikolojik etki, yangın patlama etkisi vb.

Risk endeksleri, risklerin sıralanması ve karşılaştırılması için öncelikli olarak kalitatif bir yaklaşımdır. Endeksler, sistem iyice anlaşıldıktan sonra faaliyet ile bağlantılı farklı risklerin sınıflandırılmasında kullanılabilir. Risk düzeyi üzerinde

etkili olan bir takım faktörlerin, risk düzeyi doğrultusunda tek bir sayısal puana dahil edilmesine olanak tanır.

Endeksler, genellikle risk düzeyi doğrultusunda risklerin sınıflandırılmasında bir kapsam belirleme aracı olarak birçok farklı risk türünde kullanılabilir. Burada amaç, hangi risklerin derinlemesine ve büyük olasılıkla kantitatif bir değerlendirmeye ihtiyaç duyduğunu saptamaktır.

Girdi:

Girdiler, sistem analizinden veya bağlamın genel hatlarıyla tanımlanmasından elde edilir. Bu da tüm risk kaynaklarının, olası yöntemlerin ve hangi unsurların etkilenebileceğinin yeterli şekilde anlaşılmasını gerektirir. Endekslerin geliştirilmesini desteklemek adına hata ağacı analizi, olay ağacı analizi ve karar analizi gibi araçlar kullanılabilir. Sıralamalı ölçeklerlerin seçimi bir bakıma yapay olduğundan, endeksin geçerliliğini doğrulamak için yeterli verilerin elde edilmesi gerekmektedir.

Süreç:

Atılacak ilk adım sistemi anlamak ve tanımlamaktır. Sistem tanımlaması yapıldığında, bileşik endeksin sağlanması için her bir bileşen için kombine edilebilecek şekilde puanlar geliştirilir. Puanlar, risk bileşenlerine (örn; olasılık, maruziyet, sonuç) verilebileceği gibi, riski arttıran faktörlere de verilebilmektedir.

Çıktılar:

Elde edilecek çıktı, belirli bir kaynağa bağlı olan, aynı sistem içerisindeki diğer kaynaklar için geliştirilen endekslerle kıyaslanabilen veya aynı şekilde modellenebilen sayı serileridir (bileşik endeksler).

Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler şunlardır:

- Endeksler, farklı risklerin derecelendirilmesi için etkili bir araçtır,
- Risk düzeyi için tek bir sayısal puana dahil edilecek olan risk düzeyini etkileyebilecek çoklu faktörlere olanak tanır.

Sınırlılıklar aşağıdaki gibidir:

- Süreç (model) ve çıktısının geçerliliği yeterli şekilde doğrulanmaz ise elde edilen sonuçlar anlamsız olabilir. Çıktının riske ilişkin olarak sayısal bir değere sahip olması, örneğin sonraki maliyet/fayda analizinde yanlış yorumlanabilir veya yanlış kullanılabilir,
- Endekslerin kullanıldığı birçok durumda, risk faktörlerine ilişkin bağımsız

puanların doğrusal, logaritmik veya herhangi başka bir formda olduğuna dair temel bir tanımlama modeli mevcut değildir. Faktörlerin nasıl bir araya getirilmesi gerektiğine değinen bir model de bulunmamaktadır. Bu gibi durumlarda yapılan derecelendirme doğal olarak güvenilmez bir nitelik taşıyabilir ve gerçek veriler ışığında geçerliliklerinin doğrulanması oldukça önemlidir.

11.35. Toksikolojik Risk Değerlendirme- Kimyasal Mauziyet Risk Değerlendirme (Toxicity Risk Assessment- Chemical Exposure Risk Assessment)

Kimyasal maruziyet risk değerlendirmesi, bir dizi kimyasal tehlikelere maruz kalınması sonucu bitkilere, hayvanlara ve insanlara yönelik risklerin değerlendirmesinde baz alınan süreci ele almak için kullanılır. Risk yönetimi ise risk değerlendirmesi ve risk müdahalesi de dahil olmak üzere karar verme aşamalarını ifade eder.

Yöntem; tehlikeye, zarar kaynağına veya bunların hedef nüfusu nasıl etkilediğine yönelik analiz çalışmaları ile tehlikenin savunmasız hedef kişlere erişebileceği yolları içerir. Dolayısıyla söz konusu bilgiler, tehlikenin düzeyi ve doğası hakkında bir tahmin ortaya koymak için bir arada ele alınır.

Analiz kimyasallar, mikroorganizmalar veya diğer türler gibi tehlikelere maruz kalınması sonucu meydana gelen bitki, hayvan ve insana yönelik risklerin değerlendirilmesi için kullanılır. Herhangi bir hedefin risk kaynağına maruz kalmış olabileceği farklı sebepleri açıklayan bir analiz türüdür ve insan sağlığı ve çevre dışında birçok farklı risk alanında kullanılabilir. Riskin azaltılması için uygulanabilecek müdahalelerin saptanması açısından da oldukça faydalıdır.

Girdi:

Yöntem; tehlikelerin doğası ve özellikleri, hedef nüfusun (veya nüfusların) savunmasızlığı ve bu ikisinin etkileşim türü hakkında etkili verilerin edinilmesini gerektirmektedir. Söz konusu veriler genellikle laboratuar veya epidemiyolojik tabanlı araştırmalara dayalıdır.

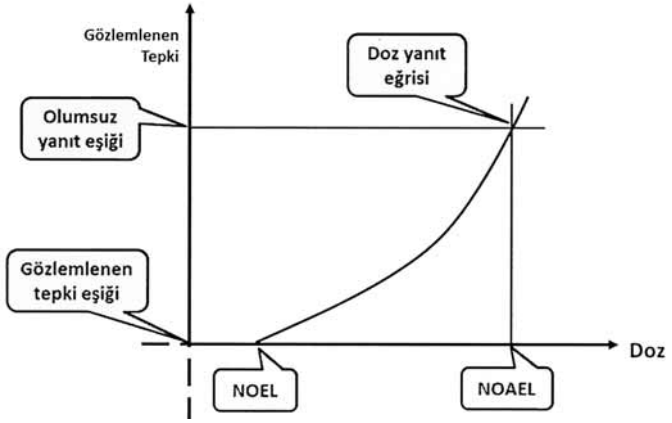
Süreç:

Prosedür aşağıda anlatıldığı gibidir:

- **Problemi tanımla:** Hedef kişileri ve tehlike türü ilişkileri dizisini belirleyerek değerlendirme kapsamını oluşturmayı içerir,
- **Tehlike saptanma:** Çalışma kapsamı çerçevesinde hedef kişilere tehlike arz eden tüm olası kaynakların belirlenmesini içerir. Tehlike saptaması, normal şartlarda uzman bilgisine ve literatür taramasına dayanmaktadır,

- **Tehlike analizi:** Tehlikenin doğasını ve hedef ile nasıl etkileşime geçtiğini anlamayı içerir. Örneğin; bir kişinin kimyasal etkilere maruz kaldığını düşünürsek, olası tehlikeler arasında akut ve kronik zehirlenme, olası DNA hasarları ve kansere sebebiyet ihtimali ile doğum kusurları arasındaki ilişki incelenir. Her bir tehlikeli etkiye yönelik olarak, etkinin büyüklüğü (tepki), hedefin maruz kaldığı tehlike miktarı (doz) ile karşılaştırılır ve mümkünse etkinin kaynağı olan mekanizma belirlenir. Gözlemlenebilir Etkinin Mevcut Olmadığı (No Observable Effect- NOEL) ve Gözlemlenebilir Yan Etkilerin Görülmediği (No Observable Adverse Effect-NOAEL) düzeyler dikkate alınır. Söz konusu veriler zaman zaman riskin kabul edilebilirlik kriterleri şeklinde kullanılır.

Şekil 50: Doz-Tepki Eğrisi



Kimyasala maruz kalmaya ilişkin test sonuçları, **Şekil 50**'de gösterilen doz-tepki eğrilerinin elde edilebilmesi için kullanılabilir. Söz konusu sonuçlar genellikle hayvanlar üzerinde yürütülen testlerden veya doku veya hücreler gibi deneysel sistemlerden elde edilir. Mikroorganizmalar veya değişik türler üzerindeki tehlikelerin etkileri, alan verileri ve epidemiyolojik çalışmalar üzerinden belirlenebilir. Hedef ile ortaya çıkabilecek etkileşiminin doğası saptanır ve belirli bir tehlikeye maruz kalınması sonucu belirli zarar düzeyi olasılığı hesaplanır.

- **Maruziyet analizi:** Bu aşama, tehlikeli maddenin veya kalıntılarının, savunmasız durumdaki hedef kişiye nasıl ve hangi miktarda ulaştığını incelemekle birlikte genellikle, tehlikenin başvurduğu farklı yöntemleri, hedefe ulaşmasını sağlayan faktörleri ve maruz kalma düzeyini etkileyen

hususları saptamak için yol analizinden faydalanır. Örneğin; kimyasalın sprey şeklinde püskürtülmesinin teşkil ettiği riski düşünürsek; maruz kalma analizi ne kadar spreyin ne şekilde ve hangi koşullar altında püskürtüldüğü, insana doğrudan nüfuz edip etmediği, ne kadar süre kalıntı bırakacağı, bünyede birikip birikmeyeceği gibi hususlar üzerinde durulur.

- **Risk nitelendirmesi:** Bu aşamada, tehlike analizi ve maruz kalma analizinden elde edilen veriler birleştirildiğinde ortaya çıkacak olan belirli sonuç olasılıklarını hesaplamak için bir araya getirilir. Çok sayıda tehlike ya da yol mevcut ise başlangıç niteliğinde bir inceleme yapılabilir ve daha kapsamlı bir risk senaryosu üzerinden ayrıntılı bir tehlike ve maruz kalma analizi ile risk nitelendirmesi gerçekleştirilebilir.

Çıktılar:

Normal şartlarda çıktı, belirli bir hedefin belirli bir tehlikeye maruz kaldığında meydana gelen risk düzeyinin göstergesidir. Söz konusu risk kantitatif, yarı kantitatif veya kalitatif olmak üzere üç şekilde ifade edilebilmektedir. Örneğin; kanser riski genellikle kantitatif olarak, belirli bir zararlı maddeye belirli bir süre maruz kalınması sonucu yaşanabilecek ihtimal şeklinde ifade edilir. Yarı kantitatif analiz, belirli bir zararlı madde için bir risk indeksi oluşturmak için kullanılabilir. Kalitatif çıktı ise herhangi bir risk düzeyi (örn; yüksek, orta, düşük) ya da olası etkilere yönelik uygulanabilir veriler içeren bir tanım olarak verilir.

Güçlü Yönler ve Sınırlılıklar:

Güçlü yönler şunlardır:

- Bu analizin güçlü yönü, sorunun doğası ve riski arttıran faktörler hakkında oldukça kapsamlı bir açıklama sağlamasıdır.
- Genellikle tüm risk alanları için faydalı bir araçtır ve kontrollerin nasıl ve hangi noktada geliştirilebileceğinin ya da yenilerinin eklenebileceğinin saptanmasına olanak tanır.

Sınırlılıklar aşağıdaki gibidir:

- Ancak, etkili veriler gerektirir ve söz konusu bilgiler genellikle ya elde edilebilir nitelikte değildir ya da yüksek düzeyde bir belirsizlik içerir. Örneğin; hayvanların yüksek düzeyde tehlikeli maddeye maruz bırakılması sonucu elde edilen doz tepki eğrilerinin, insanlarda zararlı maddenin yol açtığı etkilerin hesaplanması için dış değerleme yoluyla belirlenmesi gerekmektedir ve bunu gerçekleştirmek oldukça zor ve zahmetlidir.

12. BÖLÜM: PATLAYICI ORTAMLAR- ATEX DİREKTİFLERİ

Patlayıcı ortamların sınıflandırılması ve bu alanlarla ilgili elektriksel ekipmanların seçimi ve risklerin değerlendirilmesi ülkemiz için yeni bir konudur. Özellikle AB direktiflerinin mevzuatımıza uyarlanmış olması sebebiyle de patlayıcı ortam sınıflaması konusu büyük önem kazanmıştır.

Kitabın bu bölümün amacı özellikle birçok kimyasalın bir arada kullanıldığı sanayimizdeki tesislerin patlayıcı ortam sınıflama ve risk değerlendirmesi konularındaki bazı yanlış anlaşılmaları ortadan kaldırmak ve dünyada uygulanmakta olan standart, yöntem ve metotları karşılaştırarak patlayıcı ortam sınıflaması yapacak olan uzman ve mühendislere geniş bir bakış açısı sağlamaktır.

12.1. Patlayıcı Ortam Sınıflaması İle İlgili Standartlar ve Hukuki Düzenlemeler

Patlayıcı ortamların sınıflandırılması ve risklerin değerlendirilmesi için dünyada iki görüş hakimdir. Bu görüşlerden birincisi ve uzun zamandır da ülkemiz mevzuatı gereğince uygulanmakta olan "Kuzey Amerikan" görüşü ve ikincisi ise AB ATEX direktif ve standartları sonucu uygulanmakta olan "Batı Avrupa Görüşü" dür. Özellikle de AB direktiflerinin mevzuatımıza uyarlanmış olması sebebiyle patlayıcı ortam sınıflaması konusu büyük önem kazanmıştır.

Patlayıcı ortamlarla ilgili 22.10.1984 tarih ve 18553 sayılı resmi gazetede yayınlanarak yürürlüğe girmiş olan "Maden ve Taş Ocakları İle Açık İşletmelerde Alınacak İşçi Sağlığı ve İş Güvenliği Tedbirleri Hakkında Tüzük" ile 24.12.1973 tarih ve 14752 nolu resmi gazetede yayınlanarak yürürlüğe girmiş olan "Parlayıcı, Patlayıcı, Tehlikeli ve Zararlı Maddelerle Çalışan İş Yerlerinde ve İşlerde Alınacak Tedbirler Hakkında Tüzük, 1950'li yılların felsefesine uygun olarak, daha ziyade Amerikan standart ve hukuki düzenlemeleri temel alınarak hazırlanmıştır. Söz konusu tüzüklerde patlayıcı ortamlarda exproof olarak tarif edilen alev sızdırmaz elektrikli ekipman ile etanj tabir edilen nemli ortamlarda kullanılabilen kapalı tip elektrikli ekipmandan bahsedilmektedir. Etanj tabiri IP54 standartı veya yukarısı koruma anlamına gelmektedir ve o aletin nemli yerlerde kullanılabileceğini ifade etmektedir ve aslında bu ekipmanlar patlayıcı ortamlarda kullanılamazlar.

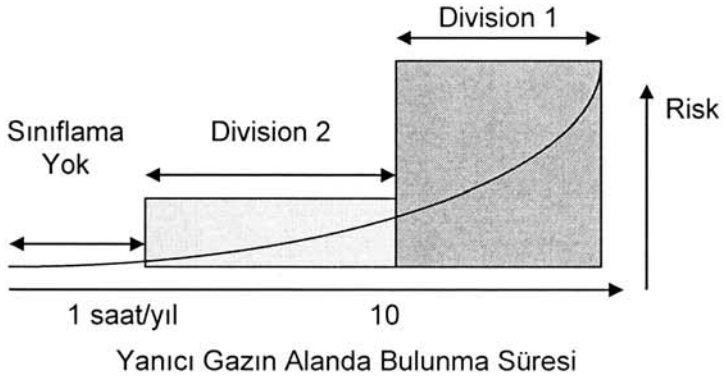
Kuzey Amerikan görüşünün uygulamakta olduğu Amerika ve Kanada da, patlayıcı ortam sınıflaması ile ilgili olarak Ulusal Yangınla Mücadele Kuruluşunun (NFPA) talimatları ve OSHA'nın çalışanların güvenliği ile ilgili yasaları dikkate alınmaktadır. Patlayıcı ortam sınıflaması DIVISION'lar ise ANSI/NFPA 70 ve National Electrical Code Article 500 standartlarında belirlen-

mektedir. Kuzey Amerika görüşüne göre patlayıcı ortamlar iki bölümde sınıflanmaktadır, buna göre patlayıcı ortamlar;

Bölge(Division) 1: Normal çalışma (koşullarında) esnasında patlayıcı ortam oluşan ve oluşma ihtimali yüksek olan ve uzun süren yerler.

Bölge(Division) 2: Normal çalışma esnasında patlayıcı ortam oluşma ihtimali az olan yerler. Ancak anormal hallerde (tamir bakım, arıza, kaza gibi) patlayıcı ortam oluşan ve oluşma ihtimali olan ve kısa süren yerlerdir.

Şekil 51: Kuzey Amerika Görüşüne Göre Patlayıcı Ortam Sınıfları



Başta Avrupa olmak üzere dünyanın diğer bölgelerinde bu sınıflandırma "Bölge" (Zone) sistemine göre International Electrotechnical Comission (IEC) ve European Committe for Electrotechnical Standardization (CENELEC) adlı kurumlar tarafından gerçekleştirilmiştir. CENELEC, Avrupa birliği ülkelerinin ve Batı Avrupa EFTA ülkelerinin işbirliği içinde olduğu Elektrotekniksel Standart Belirleme ile ilgili Avrupa Komitesidir. CENELEC üyeleri, Avrupa standartlarına ulusal standartlara uydukları gibi uymakla yükümlüdür.

Patlama korumalı bölgelerin tanımlanması ve burada kullanılabilecek elekrikli malzemelerin bu ortamlara uygunluğu için çalışmalar uluslararası IEC Komitesi tarafından yapılmaktadır. EN 60079 ve takip eden seri numaralı ve elektriksel patlamaya karşı koruma ile ilgilenen Avrupa standartları TC31 teknik komitesi tarafından geliştirilmiş ve Avrupa birliği ülkelerinde ulusal standartlar olarak kabul edilmişlerdir. IEC yayınları, ulusal ve bölgesel standartları yönlendirmeyi amaçlayan tavsiyelerle ilgili yasal düzenlemelere sahiptir. BÖLGE'ler IEC 60079-10-1 ila 2 standartlarında tarif edilmektedir. **Tablo 47**'de elektriksel patlamaya karşı koruma alanındaki AB ülkelerinde uygulanan standartlar verilmiştir.

Tablo 47: AB Ülkelerinde Patlayıcı Ortamlarda Kullanılan Ekipmanlarının Koruma Tiplerine Göre Uygulanan Standartlar

Koruma tipi	**Sembolü**	**İlgili IEC standardı**
Kendinden emniyetli	Ex-ia	IEC 6009-11
Kapsül, döküm reçine içene alarak koruma	Ex-ma	IEC 60079-18
EPL-b seviyesinde iki bağımsız koruma uygulaması		IEC 60070-26
Optik koruma yöntemi uygulanan alet ve data nakil sistemleri	Ex-op-is	IEC 60079-28
Alev sızmaz gövde	Ex-d	IEC 60079-1
Artırılmış emniyet	Ex-e	IEC 60069-7
Kendinden emniyetli	Ex-ib	IEC 60069-11
Kapsüllü koruma	Ex-mb	IEC 60069-18
Yağlı,sıvılı korumu	Ex-o	IEC 60069-6
Basınçlandırılmış koruma	Ex-p,Ex-px, Ex-py	IEC 60069-2
Tozlu, kuvarz tozlu koruma	Ex-q	IEC 60069-5
Fieldbus FISKO tipi kendinden emniyetli data nakil sistemi		IEC 60069-27
Optik koruma yöntemi uygulanan alet ve data nakil sistemleri	Ex-op-is Ex-op sh Ex-op-pr	IEC 60069-28
Kendinden emniyetli korunmuş alet ve devreler	Ex-ic	IEC 60069-11
Kapsüllü koruma	Ex-mc	IEC 60069-18
Ark çıkarmaz koruma , non sparking aletler	Ex-n, Ex-nA	IEC 60079-15
Sınırlı havalandırmalı	Ex-nR	IEC 60079-15
Enerjisi sınırlı alet veya devreler	Ex-nL= Ex-ic	IEC 60079-15
Ark çıkarmaz aletler	Ex-nC	IEC 60079-15
Basınçlı mahvaza	Ex-pz	IEC 60079-2
Optik koruma yöntemi uygulanan alet ve data nakil sistemleri	Ex-op-is Ex-op-sh Ex-op-pr	IEC 60069-28

Avrupa topluluğu konseyi 1976 yılında üye ülkelerin potansiyel patlayıcı atmosferlerde elektriksel teçhizat kullanımına ilişkin yasalarının uyumu üzerine ilk yönergeyi (76/11/EEC) imzalayarak Avrupa birliği içinde patlamaya karşı korumalı elektriksel teçhizatların serbest ticareti için yapılması gereken ön hazırlıkları oluşturmuştur. Bu alandaki tam uyum 1994 yılında yeni bir yönerge ile (94/9/EC) sağlanmıştır.

Avrupa parlamentosu daha sonra ATEX 137 olarak adlandırılan 16/12/1999 tarihli ve 99/92/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifini yayınlamış ve bu direktif ülkemizde ilk defa 2003 yılında "Patlayıcı Ortamların Tehlikelerinden Çalışanların Korunması Hakkında Yönetmelik" olarak yayınlanmıştır. Daha sonra aynı direktif; "Çalışanların Patlayıcı Ortamların Tehlikelerinden Korunması Hakkında Yönetmelik" olarak 30 Nisan 2013 de tekrar düzenlenerek yayınlanmıştır. ATEX 137'de, Bölge'lerin (Zone) genel tarifi yapılmakta ve bir tesisdeki tehlikeli alanların hangi bölgelere girdiğinin belirlemesi işverene bırakılmaktadır.

Patlayıcı ortamlarda kullanılabilecek ekipmanlarla ilgili detayları içeren ve ATEX 100a olarak bilinen Aralık 1999 tarihli 99/9/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi ise mevzuatımıza "Muhtemel Patlayıcı Ortamda Kullanılan Teçhizat ve Koruyucu Sistemler İle İlgili Yönetmelik" olarak aktarılmıştır. Bu yönetmeliğe göre ise korumalı aletlerin ve işyeri iş sağlığı ve güvenliği tedbirlerinin tarifi yapılmaktadır, ancak bu yönetmeliklerdeki tedbirlerin uygulanabilmesi için de önce ATEX 137'de belirtilen patlayıcı ortam sınıflamasının yapılmış olması gerekmektedir.

Ülkemizde 30.04.2013 tarih ve 28633 sayı ile Resmi Gazetede yayınlanan Çalışanların Patlayıcı Ortamların Tehlikelerinden Korunması Hakkında Yönetmelik olarak yürürlüğe girmiş olan ATEX 137 gereğince, işyerindeki patlayıcı ortam oluşturabilecek yerler aşağıda belirtilen koşullara göre sınıflandırılmak zorundadır.

TEHLİKELİ; özel önlem alınmasını gerektirecek miktarda patlayıcı karışım oluşabilecek yerler,

TEHLİKESİZ; özel önlem alınmasını gerektirecek miktarda patlayıcı karışım oluşması ihtimali bulunmayan yerler.

Tehlikeli yerlerin sınıflandırılması ise aşağıdaki şekilde yapılmalıdır;

Bölge(Zone) 0; Gaz, buhar ve sis halindeki parlayıcı maddelerin hava ile

karışımından oluşan patlayıcı ortamın sürekli olarak veya uzun süre ya da sık sık oluştuğu yerler.

Bölge(Zone) 1; Gaz, buhar ve sis halindeki parlayıcı maddelerin hava ile karışımından oluşan patlayıcı ortamın normal çalışma koşullarında ara sıra meydana gelme ihtimali olan yerler.

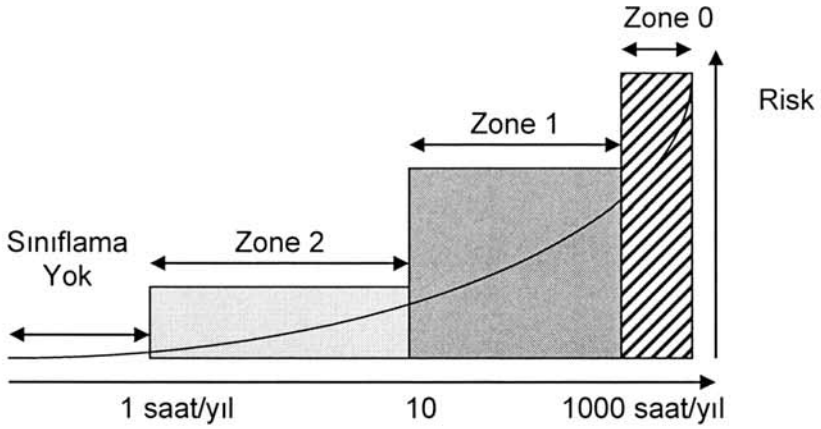
Bölge(Zone) 2; Gaz, buhar ve sis halindeki parlayıcı maddelerin hava ile karışarak normal çalışma koşullarında patlayıcı ortam oluşturma ihtimali olmayan yerler ya da böyle bir ihtimal olsa bile patlayıcı ortamın çok kısa bir süre için kalıcı olduğu yerler.

Bölge(Zone) 20; Havada bulut halinde bulunan yanıcı tozların, sürekli olarak veya uzun süreli ya da sık sık patlayıcı ortam oluşabilecek yerler.

Bölge(Zone) 21; Normal çalışma koşullarında, havada bulut halinde bulunan yanıcı tozların ara sıra patlayıcı ortam oluşturabileceği yerler.

Bölge(Zone) 22; Normal çalışma koşullarında, havada bulut halinde yanıcı tozların patlayıcı ortam oluşturma ihtimali bulunmayan ancak böyle bir ihtimal olsa bile bunun yalnızca çok kısa bir süre için geçerli olduğu yerler.

Şekil 52: Batı Avrupa Görüşüne Göre Patlayıcı Ortam Sınıfları



Patlayıcı ortam oluşabilecek tüm yerlerdeki ekipman ve koruyucu sistemler, "Muhtemel Patlayıcı Ortamda Kullanılan Teçhizat ve Koruyucu Sistemlerle İlgili Yönetmelik"te belirtilen kategorilere göre seçilmek zorundadır. Buna göre;

Bölge 0 veya Bölge 20 : Kategori 1 ekipman,

Bölge 1 veya Bölge 21 : Kategori 1 veya 2 ekipman,

Bölge 2 veya Bölge 22 : Kategori 1, 2 veya 3 ekipman.

Bu iki sistem arasındaki temel fark, risk düzeyinin Kuzey Amerika'da iki bölümde ele alınırken, Avrupa'da üç bölgede ele alınmasıdır. Amerikan DIVISION sistemi ile Avrupa ZONE sistemleri birbirinden tamamen farklı iki ayrı sistemdir. Uygulamada önemli farklılıklar vardır. Amerikalılar aletleri borularla (CONDIUT) bağlarken Avrupa ve diğer dünya ülkeleri kablo kullanmaktadır. Ayrıca ZONE'larda kullanılan aletler de birbirlerine uyum sağlamamaktadır. Avrupa normlarına uyumlu her alet division sisteminde kullanılamaz. Ancak amerikan standardına göre özel imal edilmiş olması gerekir NEC de her iki sistemin birbirine karıştırılmasına müsade etmemektedir.

12.2. Patlayıcı Ortam Sınıflandırma ve Patlayıcı Ortam Risk Değerlendirmesi

Mevzuatımıza "Patlayıcı Ortamların Tehlikelerinden Çalışanların Korunması Hakkında Yönetmelik" olarak uyarlanmış olan ATEX 137'de patlayıcı ortam; yanıcı maddelerin gaz, buhar, sis ve tozlarının atmosferik şartlar altında hava ile oluşturduğu ve herhangi bir tutuşturucu kaynakla temasında tümüyle yanabilen karışımı olarak, normal çalışma şartları ise bir tesisin tasarımlanan amaç doğrultusunda, ölçü ve değerlerde çalıştırılmaları olarak tarif edilmiştir.

Patlayıcı ortam sınıflaması ile ilgili her iki görüş için meslek kuruluşlarının yayınları ve tavsiyeleri olmasına karşın patlayıcı ortamları sınıflara ayırmakta ne Kuzey Amerikan görüşündeki DIVISION'ları ne de Batı Avrupa görüşündeki ZONE'ları belirlemekle ile ilgili olarak bir otoriteden bahsedilmemektedir.

Ülkemizde de mevzuat olarak uyarlanmış olan 16/12/1999 tarihli ve 99/92/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi, yani ATEX 137 baz alınarak bir tesisteki BÖLGE'lerin (ZONE) tespit edilmesi gerekmekte ancak bu BÖLGE'lerin tespitinin o tesisi kuran ve projelendiren mühendisler ya da tesisi işleten mal sahibinin uzman mühendisleri tarafından yapılması beklenmektedir.

Uluslararası yönetmeliklerin hemen tamamı "patlayıcı ortamlarla" ilgili BÖLGE ayrımlarına temkinli yanaşmakta ve kesin tavır koymamaktadırlar. BÖLGE'lerin genl bir tarifi yapılmakta ve buna dikkat edilerek gerekli önlemlerin alınması istenmektedir, ana düşünce tarifte saklı olduğu için sorumluluk tesisi dizayn edende kalmaktadır. Avrupa ülkelerinde bu konularla ilgili meslek kuru-

luşlarının yayınları ve tavsiyeleri vardır, özellikle de kimya mühendisleri odalarının patlayıcı ortam tehlike bölgeleri hakkında talimat ve tavsiyeleri yayınlanmaktadır.

Bu bildiride patlayıcı alan sınıflandırmasına yardımcı olan değişik görüşlerdeki proses tehlike derecelendirme ve tehlikeli alan sınıflandırma yöntem ve standartları ile patlayıcı ortam risk değerlendirme yöntemleri incelenecek ve tartışılacaktır.

12.3. NEC 50, NFPA Kodlarına Göre Alan Sınıflandırması

Kuzey Amerikan görüşünde, "Sınıf, Bölge" (Class, Division) sistemi benimsenmiştir. Riski oluşturan maddelerin yapılarındaki farklılıklar ve bunlara uygun önlemler göz önüne alınarak üç sınıf ve iki bölüm oluşturulmuştur. Buna göre, Sınıf risk oluşturan maddenin türünü belirtmekte, Bölge ise risk oluşturan maddenin ortamda bulunma sıklığını ifade etmektedir. Sınıf 1' de riski oluşturan gaz ve buhar halindeki maddeler, Sınıf 2'de parlayıcı tozlar, Sınıf3'te ise kumaş artıkları ve fiberler yer almaktadır.

Tablo 48: NEC 500'e göre patlayıcı madde sınıfları

Sınıf I:	Patlayıcı gaz ve buharlar
Sınıf II:	Patlayıcı tozlar, kömür tozu, hububat tozu (un) gibi
Sınıf III:	Uçucu tozlar, Normalde tozdan daha iri maddeler, pamuk tozu, hızar tozu, tekstil liftleri gibi

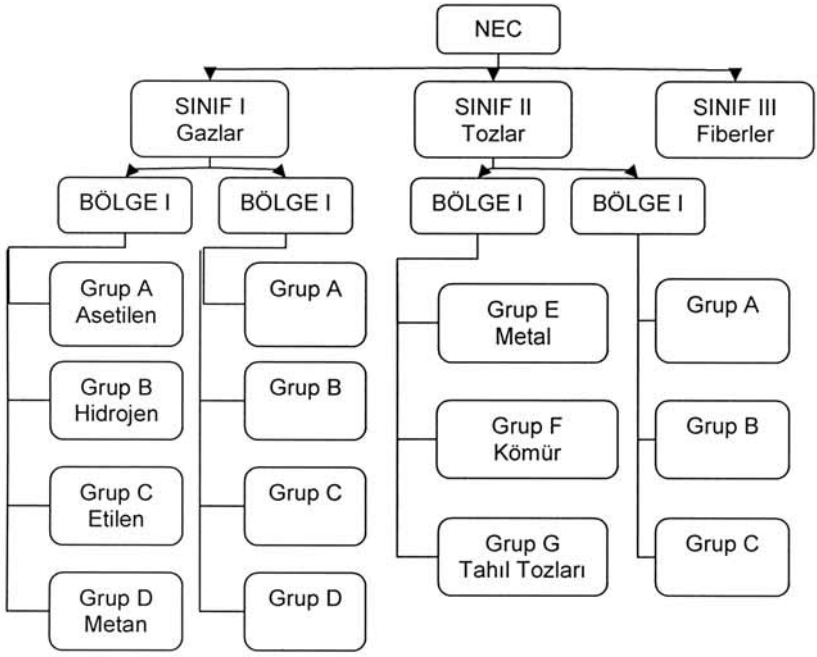
Tablo 49: NEC 500'e göre patlayıcı madde grupları

Grup A	Asetilen ve türevleri	Grup E	Metal tozları/Al-Mg
Grup B	Hidrojen ve türevleri	Grup F	Kömür tozları/kok-kömür
Grup C	Etilen ve türevleri	Grup G	Tahıl tozları/nişasta
Grup D	Metan ve türevleri		

Kuzey Amrikan görüşünde patlayıcı alanların sınıflandırılması için bir çok standart ve kod mevcuttur, bu satndart ve kodlarda SINIF ve GRUP'lara göre BÖLGE (DIVISION)'lere örnekler verilmiştir, kullanılan kod ve standartlar aşağıda verilmiştir;

- ANSI/NFPA 30 Flammable and Combustible Liquids Code
- NFPA 54 National Fuel Gas Code
- NFPA 58 Liquefied Petroleum Gas Code
- NFPA 59 Utility LP-Gas Plant Code
- ANSI/NFPA 497 Recommended Practice for the Classification of Flammable Liquids, Gases or Vapors and of Hazardous Locations for Electrical Installations in Chemical Process Areas.
- ANSI/NFPA 499 Recommended Practice for the Classification of Combustible Dusts and of Hazardous Locations for Electrical Installations in Chemical Process Areas.

Şekil 53: NEC Sistemi



12.4. EN 60079 Patlayıcı Gaz Ortamlarında Tehlikelerin Sınıflandırılması

EN 60079 standartı patlayıcı gaz ortamların oluşabileceği alanların sınıflandırılması ve BÖLGE tayini yapılması üzerine hazırlanmış bir rehber niteliğindedir. Yine standartta bölge sınıflandırmasının yanıcı malzemeler, prosesler ve tec-

hizat özellikleri hakkında bilgi sahibi olmadan yapılamayacağı, bu standardın alan sınıflandırması için bir öneri sunduğu ve alan sınıflandırmasının mutlak suretle dizayn mühendisi, emniyet, makine ve diğer mühendislik personeline de danışılarak yapılmasını tavsiye etmektedir.

Standardın ana mantığı ise patlayıcı alandaki kimyasalların yanıcılık düzeyleri, boşalma kaynakları, yayılma hızları ve bu alandaki havalandırma koşullarına göre patlayıcı alan sınıflandırmasının yapılmasıdır.

Yanabilen gaz veya buhar bulutunun boyutları ve gaz salımı durdurulduktan sonra bu bulutun ortamda kalış süresi çeşitli havalandırma yöntemleriyle kontrol altında tutulabilir. Standartta patlayıcı bir gaz atmosferinin ortamda bulunmasını kontrol altında tutabilmek için gerekli havalandırma derecesinin belirlenmesine yönelik bir metot tanımlanmıştır. Öncelikle bu metodun tanımlanan kısıtlamalara tabi olduğunu bu yüzden yaklaşık sonuçlar verdiğini belirtmek gerekmektedir. Fakat bazı güvenlik faktörlerinin kullanılmasıyla güvenlik ile ilgili sonuçlardaki hatalar azaltılabilmektedir.

Alt patlayıcılık sınırı (LEL): Belirli bir yayılma hacmi için, LEL ne kadar düşük olursa patlayıcı alanın yayılma sınırı o kadar büyük kabul edilmektedir.

Gazın veya Buharın Boşalma Hızı: Boşalma hızı ne kadar yüksek olursa patlayıcı alanın yayılma sınırının da o kadar büyük olacağı kabul edilmektedir. Boşalma hızının kendisi de boşalma kaynağının geometrik şekli, gazın yoğunluğu, yanıcı sıvının uçuculuğu ve kullanılan sıvının scaklığı parametrelerine bağlı olarak değişir.

Standartta Boşaltma Kaynakları A,B,C ve D olarak sınıflandırılmış ve bu tiplere göre de boşalma derecelendirilmesi yapılmıştır.

Gazın veya Buharın Boşaldıktan Sonraki Bağıl Yoğunluğu: Eğer gaz veya buhar havadan önemli ölçüde hafifse yukarıya doğru hareket eder. Eğer önemli ölçüde ağırsa zemin seviyesinde birikir. Patlayıcı ortamın yayılma sınırının zemin seviyesinde artan bağıl yoğunlukla artığı ve kaynağın yukarısında azalan bağıl yoğunlukla da azaldığı kabul edilmektedir.

Havalandırma: Normal olarak havalandırma arttıkça patlayıcı alanın yayılma sınırının da azaldığı kabul edilmektedir.

Standartta havalandırma tipleri doğal ve suni havalandırma olmak üzere iki sınıfa ayrılmış ve havalandırma derecesinin ve tehlikeli bölgeye etkisinin kıymetlendirilmesi gerektiği belirtilerek formülasyonlar verilmiştir;

Suni havalandırma da V_z Teorik hacmi ile tehlikeli bölge ebatları arasındaki ilişki;

$(dV / dt)_{min} = (dG/dt)_{max} / kxLEL_m . T/293$

LEL_v (%vol)'yi LELm (kg/m^3)'e çevirmek için;

$LEL_m = 0,416x10^{-3} xMxLEL_v$

Yayılma noktasındaki fiili havalandırma hızı için;

$V_k = (dV/dt)_{min} / C$

C, yani birim zamandaki hava değişimi sayısı için;

$C = (dV_0/dt)/ V_0$

Hacim hesabı;

$V_z = f x V_k = [fx(dV/dt)_{min}]/ C$

Açık havada V_z Teorik hacmi ile tehlikeli bölge ebatları arasındaki ilişki;

$V_z = [fx(dV/dt)_{min}]/ 0,03$

Kalıcılık zamanı t'nin tahmin edilmesi;

$T= -f/C \ln (LELxk)/ X_0$

Yapılan hesaplamalar sonucunda çıkan sonuçlara göre patlayıcı alan sınıflamasına yüksek, orta veya düşük seviye için BÖLGE önerilerinde bulunulmaktadır.

Diğer Faktörler: Yine patlayıcı ortamların bölge tayinini yaparken tesisin yer seçimi, tapografyası ve iklim şartlarının da dikkate alınması gerektiği belirtilmektedir.

12.5. TC31/W09 - Güvenlik Bütünlük Derecelendirme - SIL(Safety Integrity Level)

AB üyelerinde uygulanan ve patlayıcı ortamlarda kullanılan elektriksel ekipmanlar ile "Bölge" (Zone) sistemine göre patlayıcı ortam sınıflandırma konusunda standartların International Electrotechnical Comission (IEC) ve European Committe for Electrotechnical Standardization (CENELEC) adlı kurumlar tarafından hazırlandığını belirtmiştim.

CENELEC tarafından 1999 yılında SMT4-CT98-2255 anlaşma numaralı, SAFEC projesi başlatılmış ve AB ülkelerinde yaygınlıkla kullanılan EN 50 014 standartına alternatif olarak çalışma yürütülmüştür. SAFEC projesi, CELENEC'in elektriksel patlamaya karşı koruma ile ilgilenen Avrupa standartları teknik komitesi TC31'in W09 numaralı ekibi tarafından yapılmış ve çalışmalar 12 ay sürmüştür.

Birçok ülkede tesisler ve proses endüstrileri için "Güvenlik Ölçümleme Sistemi – SIS" in uygulanması kabul edilmiştir, Amerika'da OSHA 29 CFR Bölüm 1910 tarafından da kullanılması zorunlu kılınmıştır. Bir tesis ve endüstriyel prosesin güvenlik ölçümlemesi ise IEC 61508 metodolojisi ya da ANSI/ ISA S84.01 standartına göre "Güvenlik Bütünlük Derecesi –SIL" tespiti ile yapılmaktadır. SIL ise maruz kalma zamanı, olaya maruziyet sıklığı, şiddet derecesi, olayın oluşumundan kaçış ve olasılığı açısından analistin görüş açısından değerlendirilmesidir. Daha kısa bir ifade ile SIL derecesi tesisin ayakta kalma derecelendirmesi için de kullanılmaktadır.

SAFEC Projesinin esası ise ilk olarak HAZOP (Hazard and Operability Studies) metodolojisi için geliştirilmiş olan ve daha sonraları da makine risk değerlendirmesi vb. birçok alanda uygulanma şansı bulunan IEC 61508 metedolojisinin patlayıcı ortam sınıflamasında kullanılabilirliği ve alternatif standart hazırlama çalışmasıdır.

Proje sonucunda IEC 61508 metodolojisi kullanılarak alternatif hata tolerans aralıkları önerilmiş ve özellikle hata olasılığının hesaplanması için "Hata Ağacı Analizi" (FTA) yada Olası Hata Türü ve Etkileri Analizi (FMEA) kullanılması da önerilmiştir. Çalışmada alternatif hata toleransları hata ağacı analizi ve Risk Graf birlikte kullanılarak önerilmiştir.

SAFEC Projesi sonuç raporunda TC31/W09'un draft standartında **Tablo 50**'de verilen ekipman hata toleransları ve kategoriler verilmiştir.

12.6. Yangın ve Patlama İndeksleri

Tehlike derecelendirme indekslerinin ana mantığı bir bina veya bir bölümünün patlayıcı ortam tehlike sınıfının ve risk derecesinin tesisin ya da prosesin özelliklerine ve tesiste yürütülen işlem ve operasyonların niteliğine ve kullanılan kimyasalın tehlike derecesine bağlı olarak saptanması gerektiği fikrine dayanmaktadır. Bu mantık gün geçtikçe daha fazla benimsenmektedir.

Tablo 50: TC31/W09'un Draft Standartında Verilen Kategorilere Göre "Patlayıcı Alan Bölge Sınıflandırması"

TEHLİKELİ ALAN	Bölge 0 Bölge 20			Bölge 1 Bölge 21			Bölge 2 Bölge 22	
ATEX Direktiflerindeki Hata Toleransları	2			1			0	
Ekipman Hata Toleransı	2	1	0	1	0	-1	0	-1
IEC 61508 ve EN 954'e göre Sınıflandırma	-	B, 1, 2, 3 veya 4	3 veya 4	-	B, 1, 2, 3 veya 4	3 veya 4	-	B, 1, 2, 3 veya 4
ATEX Direktiflerine Göre Ekipman Kategorisi	ATEX Kategori 1 Ekipman			ATEX Kategori 2 Ekipman			ATEX Kategori 3 Ekipman	

Bir tesis ya da proses ünitesi için "Tehlike Derecelendirme ve Risk Değerlendirmesi" yapılması amacıyla kullanılan birçok indeks bulunmaktadır, bu tehlike derecelendirme ve risk değerlendirme indekslerin geliştirilmesinde ise Dow F&EI ve Mond F&ETI yöntemleri öncü olmuşlardır. Tehlike derecelendirme indekleri daha sonraları sadece iş sağlığı ve güvenliği açısından değil ayrıca çevreye verilebilecek zararlar da düşünülerek akademi ve üniversiteler tarafından geliştirilmiştir. En çok bilinen ve kullanılan bazı indeksler **Tablo 51**'de verilmiştir.

Tehlike indeksleri uygulanmadan önce, söz konusu tesis mantıksal, birbirinden bağımsız alt elementlere veya ünitelere ayrılmalıdır. Genellikle, bir ünite, mantıksal olarak içerisinde cereyan eden prosesin doğası dikkate alınarak nitelendirilmelidir, yani ünite diğer elemetlerden boşluklar veya koruyucu duvarlarla

Tablo 51: En Çok Bilinen Tehlike Derecelendirme ve Risk Değerlendirme İndeksleri

KISALTMA	METHOD İSMİ	YILI	GELİŞTİREN
Dow CEI	Dow Chemical Exposure Index	1988	Dow Chemicals
Dow F&EI	Dow Fire & Explosion Index	1994	Dow Chemicals
ISI	Inherent Safety Index	1995	Edwards ve Lawrence
HIRA-TDI HIRA-FEDI	Hazard Identification & Ranking • Toxicity Damage Index • Fire Explosion Damage Index	1998	Khan ve Abbasi
I2SI	Integrated Inherent Safety Index	1999	Heikkilä
EHS	Environment Health &Safety Index	2000	Koller, Fischer ve Hungerbühler
SREST	SREST-Layer-Assessment Index	2003	Shah
SweHI	Safety Weighted Hazard Index	2003	Khan
i-Safe Index	i-Safe Index	2002-2004	Palaniappan

ayrılmış ise bu alanları ve diğer fabrika elementlerini ayrı ayrı bölümler olarak değerlendirmek gerekmektedir.

12.6.1. Dow F&EI ve Mond F&ETI

Dow F&EI yöntemi Dow Chemical Company firmasınca geliştirilmiştir, ancak bu yöntemin daha basitleştirilmiş birçok versiyonları da mevcuttur. Bir endüstri kompleksi içindeki fabrikaya ait birbirinden ayrı elementlerin tehlike derecelendirilmesi, sınıflandırılması ve risklerinin değerlendirilmesinde kullanılmaktadır.

The Dow Chemical Company'nin bu indeksi, en çok kullanılan indekstir. Bu indeks başlangıçta daha ziyade yangın önleme yöntemlerinin belirlenmesinde kullanılan bir kılavuz olmuştur. Yangından korunma önlemlerini belirlemeye yarayan yangın ve patlama indeksinin hesaplanmasına dayanmakta, muhtemel azami temel mal hasarını hesaplamakta kullanılan hasar faktörü ile birlikte kullanılmaktadır.

Mond F&ETI indeksi ise Dow indeksinin bir uzantısıdır ve 1973 yılı versiyonundan geliştirilmiştir. Tehlikelerin, Dow F&EI'de yapılış biçimine benzer şekilde ön değerlendirmelerin yapılması esasına dayanmakla birlikte, toksisite gibi tehlikeler de dikkate alınmaktadır. Dow F&EI yöntemine kıyasla getirilen temel değişiklikler aşağıdakileri kapsamaktadır.

- Daha geniş kapsamlı prosesler ve depolama tesisleri ele alınmaktadır,
- Patlayıcı özellikleri olan kimyasal maddelerin işlenmesini kapsamaktadır,
- Hidrojen tehlikeleri geliştirilerek ele alınmaktadır,
- İlave özel proses tehlikeleri ele alınmaktadır,
- Tehlike değerlendirmesi kapsamına toksisite de ilave edilmiştir.

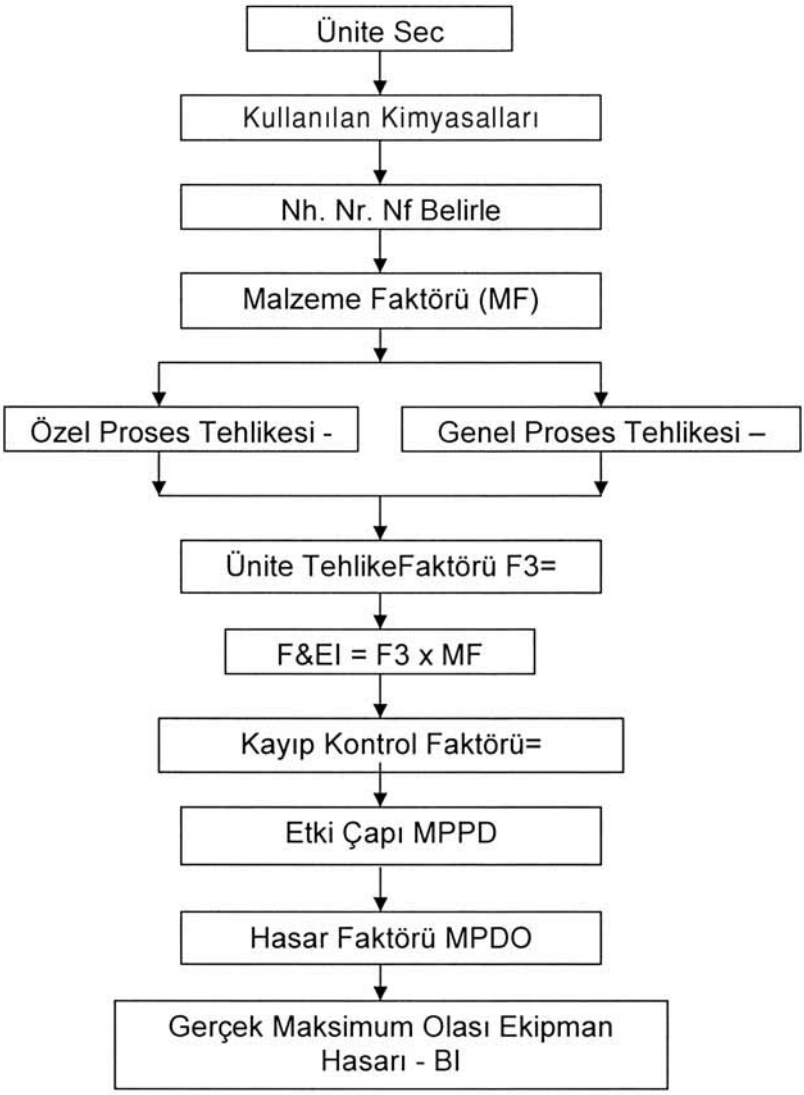
Dow indeks ve Mond indeksin her ikisinde de "Malzeme Faktörü' (MF) olarak tabir edilen bir faktör hesaplanır, bu faktör NFPA'in kodlarından elde edilir. MF, proseste yer alan en tehlikeli maddeden veya dikkate değer miktardaki maddelerin karışımından ortaya çıkan enerjinin yoğunluğunu gösteren bir sayıdır.

Olabilecek en kötü senaryo dikkate alınarak, tesis veya proses için "Ünite Tehlike Faktörü" (ÜTF) hesaplanır, ÜTF ise genel ve özel proses tehlike faktörlerinin çarpımından bulunur. Bu faktörlerin sayısal değerleri Dow Yangın ve Patlama Tehlike İndeks Sınıflama Kılavuzu'ndan elde edilir ve hem Dow F&EI hem de Mond F&ETI indeksinde kullanılır. DOW F&EI kodunun tablosuna alanda tespit edilen genel ve özel proses tehlikeleri için atama yapılarak F1 ve F2 değerleri ve F3 değerleri bulunur. Proses tehlike kontrol parametreleri C1, C2 ve C3 değerleri hesaplanır. F&EI endeksine göre alanın patlayıcı ortam sınıflaması yapılır, etki yarıçapı bölge alanının kapsadığı alanı göstermektedir. Daha sonra hasar faktörü ile maksimum olası hasar faktörü bulunur. Bu faktör alanda meydana gelebilecek patlamanın şiddetinin büyüklüğünü göstermektedir.

Tablo 52: F&EI İndeksine Göre Alan Sınıflandırması

F&EI İndeksi	**Tehlike Derecesi**
1-96	Düşük Tehlikeli Bölge
97-127	Orta Tehlikeli Bölge
128 ve üzeri	Yüksek Tehlikeli Bölge

Şekil 54: DOW F&EI Yönteminin Uygulama Şeması



Yangın ve patlama indeksi f ve toksitite indeksi t'nin belirlenmesi

Dow Chemical Company firması (A.B.D.) tarafından geliştirilen ve yangın ve patlama indeksini belirlemekte kullanılan yönteme benzer şekilde, yanıcı veya toksik maddeler ihtiva eden her bir fabrika elementi için patlama indeksi F ve toksitite indeksi T saptanabilir.

Yangın ve patlama indeksi F aşağıdaki formülden hesaplanır.

$$\mathbf{F} = MF \times (1 + GPH_{tot}) \times (1 + SPH_{tot}),$$

Burada,

MF = Malzeme Sabiti = Mevcut tehlikeli maddenin potansiyel enerjisini gösteren bir değerdir. (Milli Yangın Koruma Kurumu, (NFPA) verilerinden elde edilir)

GPH_{tot} = Genel proses tehlikeleri = Prosesin içinde bulunan tehlikeleri belirten bir değer (prosesin doğasından ve karakteristik özelliklerinden kaynaklanır.)

SPH_{tot}= Özel proses tehlikeleri = Spesifik tesislerden kaynaklanan tehlikeleri belirten bir değer. (prosesin durumu, tesisin boyutu ve doğası)

Toksitite indeksi T aşağıdaki formülden hesaplanır.

$$\mathbf{T} = \frac{T_h + T_s}{100} (1 + GPH_{tot} + SPH_{tot})$$

Burada,

Th = Toksitite faktörü (NFPA verilerinden elde edilir)

Ts = MAC değeri

GPH_{tot} ve SPH_{tot}: Yangın ve patlama indeksinin hesaplanmasında kullanılan değerlerle aynı

Bir fabrika elementinde birden fazla maddenin bulunması halinde, her madde için yangın ve patlama indeksi F ve zehirleme indeksi T'nin hesaplanması gerekir.

Fabrika elementinin tehlike sınıfının belirlenmesinde, bulunan T ve F değerlerinin en büyüğü kullanılır.

Konsantrasyonu %5'den daha az olan maddeler burada dikkate alınmazlar (sıvı ve katılar için ağırlık yüzdesi, gazlar için hacim yüzdesi).

Toksitite faktörü, NFPA'nın etiketleme sınıflama kodundan bulunur. NFPA kodunda, materyallere sağlık açısından tehlikeyi belirten 0'dan 4'e kadar değişen sayılar verilmiştir. NFPA'nın referansından alınan kimyasal madde sağlık numarası **Tablo 53** kullanılarak "Toksitite Faktörüne" dönüştürülür.

Tablo 53: NFPA Tehlike ve Toksitite Faktörü Arasındaki İlişki

NFPA İNDEKSİ	TOKSİTİTE FAKTÖRÜ (T_h)
0	0
1	50
2	125
3	250
4	325

Ilave olarak; Toksitite Faktörü tehlikeli maddelerin MAC değerleri için aşağıda **Tablo 54**'de verilen penaltıların bulunması ile düzeltilir.

Tablo 54: MAC Değerlerin Penaltı Değeri

MAC (ppm)	PENALTI (T_S)
≤ 5	125
5-10	75
> 50	50

Malzeme Katsayısı (MF)'nin Saptanması

Yangın ve patlama indeksinin hesaplanmasında başlangıç noktası malzeme katsayısıdır. Bu katsayı, mevcut en tehlikeli maddenin veya maddelerin karışımının potansiyel enerjisidir. Malzeme katsayısı 0 ila 40 arasında bir sayı ile gösterilir ve değer yükseldikçe daha büyük enerjiye işaret eder.

Malzeme katsayısı, kimyasal maddenin kararsızlık ve su reaktivitesi karakteristiklerinden kaynaklanan sadece iki özellik kullanılarak tayin edilir. – yanıcılık ve reaktivite. .

Malzeme katsayıları, fabrika elementinde bulunan tüm tehlikeli maddeler için ayrı ayrı tespit edilmelidir.

Malzeme katsayısı NFPA literatüründe belirtilen yanıcılık ve reaktivite sayısal değerleri kullanılarak elde edilebilir.

Örneğin, yanıcılık değeri 4, reaktivitesi 3 olan etilen oksitin malzeme katsayısı 29'dur. Benzer şekilde, yanıcılık değeri 2, reaktivitesi yine 2 olan butil akrilit için malzeme katsayısının 24 olduğu görülmektedir.

N_h : Sağlık Tehlike Sınıflaması

N_f : Yanıcı Tehlike Sınıflaması

N_r : Reaktiflik Tehlike Sınıflaması

Hcv ya da parlama noktası yanıcılık Nf yerine kullanılabilir. Hcv değeri, yanma ısısı, kJ/mol, ile 300K (27°C)'deki bar cinsinden buhar basıncı değerinin çarpılması ile bulunur. Kaynama noktası 300K altındaki malzemeler için, buhar basıncı için 1 alınır. Nr için, adyabatik bozunma ısısı Td kullanılır.

Örneğin, propilen oksit aşağıdaki temel özelliklere sahiptir:

- parlama noktası -20 °C'nin altındadır,
- yanma ısısı 30.703 kJ/g,
- mol. Ağırlığı 58,
- dolayısıyla yanma ısısı 30.703 x 58 = 1780.78 kJ/mol
- buhar basıncı 0.745 bar (27 °C)
- bozunma ısısı 675 °C

Parlama noktası -20 °C'nin altında ise, yanıcılık tehlike değeri 4'dür. Bu Hcv'nin hesaplanmasıyla kontrol edilebilir.

Hcv = 1780.78 x 0.745 = ca. 1326 kj. bar/mol.

Hcv değeri 1326 ise, yanılıcılık için tehlike değeri olarak 4 bulunur.

Adyabatik bozunma ısı derecesi

Td = 675 + 273 = 948 K.

Bu, reaktivite için tehlike değeri 2'yi gösterir. **Tablo 55** dikkate alındığında, propilen oksit için Malzeme Katsayısı olarak 24 okunur.

Genel proses tehlikelerinin belirlenmesi

Isıveren reaksiyonlar

Penaltı 0.20 gerektiren durumlar

Tablo 55: Malzeme Katsayısı Belirleme Matrisi

Adyabatik Bozunma	< 830	830-935	935-1010	1010-1080	>1080
			Reaktiflik		

Parlama Noktası (^{0}C)	H_{cv} Kj.bar/mol
Hiç	$< 4.10^{-5}$
>100	4.10^{-5}
40-100	2.5 - 40
-20- +40	40 - 600
< - 20	> 600

Yanıcılık

Nf / Nr	0	1	2	3	4
0	0	14	24	29	40
1	4	14	24	29	40
2	10	14	24	29	40
3	16	16	24	29	40
4	21	21	24	29	40
	Madde Katsayısı (MF)				

- Yanma = Katı, sıvı veya gaz halindeki yakıtın hava ile ocakta yanmasıdır.

Aşağıdaki reaksiyonlar 0.30 penaltı gerektirir.

a) Hidrojenleme = ikili veya üçlü bağ'ın her iki tarafına da hidrojen ilavesi; Burada tehlike yüksek basınç altında ve nispeten yüksek ısıda hidrojen kullanımıdır.

b) Hidroliz = Bir bileşiğin su ile reaksiyonudur, sülfirik veya fosforik asitlerin oksitlerden üretimi gibi.

c) Alkilleme = Muhtelif organik bileşikler elde etmek üzere, bileşiklere bir alkali grubun ilavesi

d) İzomerleştirme = Bir organik molekülde atomların yeniden düzenlenmesi, örneğin düz zincirden dallı moleküle değişim, çift bağların yer değiştirmesi vs. tehlikeler, bulunan kimyasalların dengesine ve reaktivitesine bağlı olarak değişir ve bazı durumlarda 0.50 penaltı gerektirir.

e) Sülfolama = SO3H kökünün H2SO4 ile reaksiyonu yardımıyla bir organik molekül içine yerleştirilmesi

f) Nötürleştirme = Tuz ve su oluşturmak üzere, bir baz ile asidin reaksiyonu

Aşağıdaki reaksiyonlar 0.50 penaltı gerektirir.

a) Esterifikasyon : Bir asid ve alkol veya doymamış hidrokarbon arasındaki reaksiyondur. Asidin yüksek oranda reaktif olduğu veya reaktif maddelerin dengesiz olduğu durumlar (0.75 ila 1.25 arasında penaltı) hariç orta dereceli tehlike demektir.

b) Oksidasyon : Oksijenin bir başka madde ile kombinasyonu. Reaksiyon kontrollü, ve yanma durumunda olduğu gibi, CO2 ve H2O açığa çıkmaz. Kloratlar, nitrik asit, hipoklorik asitler ve tuzlar gibi kuvvetli oksitleme araçları kullanıldığı durumlarda penaltı durumunu 1.00'e arttırınız.

c) Polimerleştirme = Moleküllerin zincir veya diğer bağlar oluşturmak üzere birbiriyle bağlanmaları; reaksiyonun kontrol altında tutulabilmesi için ısı tahliye edilmelidir.

d) Yoğunlaştırma = H2O, HCL veya diğer bileşiklerin ayrılması ile iki veya daha fazla organik molekülün birleşmesi

Aşağıdaki reaksiyonlar 1.00 penaltı gerektirir.

- Halojenleme : Florin, klorin, bromin veya iyodin benzeri halojen atomların bir organik moleküle yerleştirilmesi. Bu hem kuvvetli bir ısı yayıcı ve aşındırıcı (korozif) bir prosestir.

Aşağıdaki reaksiyonlar 1.25 penaltı gerektirir.

- Nitrolama : Bir bileşikteki hidrojen atomunun bir nitro grubuyla değiştirilmesi demektir. Çok güçlü ısı yayıcı reaksiyon, muhtemelen patlayıcı yan ürünler doğurur.

Isı kontrolü iyi yapılmalıdır; saflığın bozulmuş olması (katışıklık) daha başka oksidasyona sebep olabilir veya nitrolama ve hızlı ayrışma meydana gelebilir.

Isıalan reaksiyonlar

Isıalan reaksiyonlar 0.20 penaltı alırlar.

Isıalan reaksiyonlara aşağıdaki örnekler verilebilir:

a) Kalsinasyon : Nem veya diğer uçucu maddelerin giderilmesi amacıyla malzemenin ısıtılması;

b) Elektroliz : Elektrik akımı vasıtasıyla ionların ayrıştırılması; yanıcı veya yüksek derecede reaktif ürünlerin bulunması nedeniyle tehlikelidir.

c) Isıl bozunma veya parçalanma : Büyük moleküllerin yüksek ısı, yüksek basınç veya katalizör yardımıyla termal olarak ayrışması; başka bir yanma prosesiyle katalizörün yeniden oluşması tehlikeli olabilir.

Eğer bir yanma prosesi, kalsinasyon, ısıl bozunma veya parçalanma için enerji kaynağı olarak kullanılıyorsa penaltı iki katına (0.40) yükseltilir.

Malzemelerin Yükleme-Boşaltma ve Transferi

a) Tehlikeli maddelerin yükleme ve boşaltması, özellikle yol-tankerleri ve gemilerin transfer hatlarının birleştirilmesi veya ayrılmasından kaynaklanan tehlikelerle ilgilidir. Penaltı: 0.5

b) Tehlikeli maddelerin varil, silindir ve nakil tankları ve benzeri ortamlarda (tank depolaması hariç) atelye veya avluda depolanması,

- Proses (depolama) ısıları, atmosferik kaynama noktasının altında olan maddeler için penaltı : 0.30
- Proses (depolama) ısıları, atmosferik kaynama noktasının üzerinde olan maddeler için penaltı : 0.60

Yükleme – boşaltma esnasındaki muhtemel patlama ve potansiyel yangın tehlikesi dikkate alınarak yukarıda belirtilen penaltılar uygulanır. Malzemenin miktarı burada dikkate alınmaz (malzeme miktarları ile ilgili penaltılar diğer bölümlerde dikkate alınır).

Bina içindeki proses üniteleri

Bina içine yerleştirilmiş proses üniteleri ve içerisinde tehlikeli maddelerle ilgili süreçlerin işlendiği ve/veya içerisinde tehlikeli maddeler depolanan binalar, doğal havalandırmanın engellenmesi nedeniyle artan bir tehlike potansiyeli ifade eder.

- Parlama noktasının üzerinde, ancak atmosferik kaynama noktasının altında olan parlayıcı sıvılar için : Penaltı 0.30
- Atmosferik kaynama noktasının üzerindeki, parlayıcı sıvılar veya LPG için Penaltı 0.60

Muhtelif

Varil, torba, çuval ve kutuların tehlikeli maddelerle doldurulması ve paketlenmesi, santrifüj kullanımı, açık düzenekte işlemler, aynı düzenekte birden fazla reaksiyonun cereyan etmesi Penaltı : 0.50

Özel Proses Tehlikelerinin Belirlenmesi

Proses sıcaklığı

a) Proses veya taşıma koşulları parlama noktasının üzerinde sıcaklık gerektiriyorsa, Penaltı: 0.25

b) Proses veya taşıma koşulları atmosferik kaynama sıcaklığının üzerinde sıcaklık gerektiriyorsa, Penaltı: 0.60

c) Madde, örneğin hekzan ve karbon disülfit gibi düşük kendi kendine tutuşma sıcaklığına sahipse ve sıcak buharının tutuşması ihtimali varsa, Penaltı:0.75

Düşük Basınç

Proses atmosferik basınç yada atmosferik basınca yakın bir basınçta işliyorsa penaltı gerektirmez, sistemden hava sızıntısı olması tehlike yaratmaz. (Örneğin; glikolün vacumlu distilasyonu)

a) Sistemden hava çıkışının bir tehlike yaratma durumu varsa, (Örneğin; sıcak materyallerin taşınması, tehlikeli materyal içermesi) penaltı: 0.50

b) Hidrojenin toplanacağı bir sistem, Penaltı: 0.50

c) 0.67 bar'dan az basınç gerektiren vakumlu distilasyon, penaltı: 0.75

Yanıcılık Seviyelerinde Operasyon

a) Eğer ortama yayılan buharda gaz-hava karışımı yanıcılık seviyesine yakınsa, tankların dışında yanıcı materyalin depolanması, penaltı:0.50

b) Yanıcılık limitlerine yakın proses çalışma koşulları yada ortamda patlama limitine yakın gaz birikmesini engellemek için havalandırma gerektiren durumlar, penaltı: 0.75

c) Yanıcılık limitlerinde normal çalışma koşulu (Örnek; etilen distilasyonu ve depolanması), penaltı:1.00

Çalışma Basıncı

Atmosferik basınç üzerindeki çalışma basıncı penaltı gerektir. Penaltı yanıcı ve parlayıcı maddeler için Y aşağıdaki formülden hesaplanır, burada P tahliye vanasının ayarlandığı mutlak basınçtır ve bar cinsinden ifade edilir.

Y= 0.435 log P

a) Yüksek yoğunluktaki materyaller mesela; asfalt, katran, zift, ağır yağlar gibi, penaltı;0.7

b) Basınçlı gazlar, penaltı: 1.2

c) Basınçla sıvılaştırılmış yanıcı gazlar, penaltı: 1.3

Düşük Sıcaklık

a) 0°C ila -30°C arasında işleyen prosesler, penaltı:0.30

b) -30°C'nin altında işleyen prosesler, penaltı:0.50

Korozyon ve Erozyon Nedeniyle Malzeme Kaybı

a) Korozyon hızı 0.5 mm/yıl'dan az ise; penaltı:0.10

b) Korozyon hızı 0.5 mm/yıl'ın üzerinde, 1mm/yıl'dan düşük ise; penaltı:0.20

c) Korozyon hızı 1mm/yıl üzerinde ise; 0.50

Bağlantı Yerlerinden Sızıntı ve Paketleme

a) Pompadan ve malzeme yüzeyinden minor oranda bir sızma, penaltı:0.10

b) Pompa ve flanş bağlantı noktalarındaki problerden kaynaklanan sızıntı, penaltı:0.20

c) Prosesteki sıvılardan, aşındırıcı kirden oluşan sürekli sızma problemleri; penaltı:0.40

d) Prosesteki uzama noktaları, gözleme deliklerinden sızıntı, penaltı:1.5

Tehlike Sınıflaması

Tablo 57'de gösterilen kritere göre F ve/veya T indislerini mukayese ederek kıyaslayarak söz konusu ünite bu amaç için kurulan üç kategoriden birine konu-

lur. Kategori I en düşük tehlike potansiyeli taşıyan fabrika elemanlarının kategorisi ve kategori III ise en yüksek tehlike potansiyeli taşıyan fabrika elemanlarının kategorisidir.

Tablo 56: Fabrika Elementleri Kategorileri.

KATEGORİ	YANGIN VE PATLAMA İNDEKSİ (F)	TOKSİTİTE İNDEKSİ (T)
Kategori I	$F < 65$	$T < 6$
Kategori II	$65 \leq F < 95$	$6 \leq T < 10$
Kategori III	$F \geq 95$	$T \geq 10$

Bazı durumlarda, yangın ve patlama indeksi ile toksitite indeksi için ayrı ayrı kategoriler bulunur, bu durumda en yüksek olan seçilir.

12.6.2. Temel Emniyet İndeksi (Inherent Safety Index -ISI) ve Entegre Temel Emniyet İndeksi (Integrated Inherent Safety Index -I2SI)

Temel Emniyet İndeksi -ISI yöntemi ise 1995 yılında Edward and Lawrence tarafından geliştirilmiştir, daha sonra bu yaklaşım esas alınarak başka indisler de geliştirilmiştir. Entegre Temel Emniyet İndeksi I2SI ise Khan F.I. & Amyotte, P. tarafından 2003 yılında geliştirilmiş ve EN 6601 standartı haline gelmiştir. ISI'nın ana mantığında ise işyerlerinde ve işletmelerde birçok değişik proses, makine ve sistem bir arada bulunmakta ve bunlar birbirleri ile bütünleşik bir biçimde çalışmaktadır. Özellikle fiziksel olarak büyük, teknolojik olarak karmaşık, çok fazla sayıda operasyonun, çok çeşitli ürün gruplarının olduğu sistemlerde kayıpların kontrol edilmesi gerekmektedir. Bu kayıplar ise yangın, patlama, toksikolojik maruziyet ya da çevresel hasar olabilir.

Temel emniyet indeksi (IISI), kimyasal temel emniyet indeksi (ICI) ile proses temel emniyet indeksi (IPI) ile bulunan sürecin bir toplamıdır. Bu indeksler, ayrı olarak her süreç alternatifi için hesaplanır, ve sonuçlar, birbirleriyle kıyaslanır.

$$I_{ISI} = I_{CI} + I_{PI}$$

Kimyasal temel emniyet indeksi (ICI), işletme veya tesiste kullanılan kimyasalın reaktiflik, yanıcılık, patlayıcılık, zehirlilik ve aşındırıcılığı ile ilgilidir. Her bir süreçte kullanılan kimyasalın reaktifliği, yanıcılığı, patlayıcılık, zehirlilik ve aşındırıcılığı her madde için kararlaştırılır. Kimyasal temel emniyet indeksi, her

bir hat ve yan tepkimeler de dikkate alınarak süreç alanında kimyasal maddeler için belirlenen kimyasal etkileşimin maksimum değeri için hesaplanır.

$$I_{CI} = I_{RM,\,max} + I_{RS,\,max} + I_{INT,\,max} + (I_{FL} + I_{EX} + I_{TOX})_{max} + I_{COR,\,max}$$

Proses temel emniyet indeksi (I_{PI}) hesaplanırken ise, tesis veya prosete mevcut bulunan her bir süreç için sıcaklık, basınç, malzeme emniyeti ve proses yapısal değerlerine göre hesaplama yapılır.

$$I_{PI} = I_I + I_{T,\,max} + I_{p,\,max} + I_{EQ,\,max} + I_{ST,\,max}$$

Entegre Temel Emniyet İndeksi I2SI ise, birçok kimyasalın ve değişik proses ve süreçlerin bir arada kullanıldığı tesislerdeki emniyeti sağlamak ve riski en aza indirmek maksadıyla geliştirilmiştir. İndeks iki ideksin birbirine oranlanması sonucunda elde edilmektedir;

I2SI = ISPI/HI

• **HI; Hasar İndeksi:**

Tehlike ve kontrol ölçümlerinin her ikisini de göz önüne alarak sürecin zarar potansiyelinin ölçüsüdür, 1 ila 200 arasında değer alabilmektedir.

HI = DI/PHCI

DI, zarar indeksi, PHCI ise proses ve tehlike kontrol indeksidir, 1 ila 100 arasında değer alır. Zarar endeksi; yangın ve patlama (DIfe), akut toksisite (DIac), kronik toksisite (DIch) ve çevresel hasar indeski (DIch) baz alınarak aşağıdaki bağıntıdan, PHCI ise 10 ayrı kontrol aşaması için aşağıdaki bağantıdan elde edilir;

$$DI = Min\left\{200, \left[(DI_{fe})^2 + (DI_{ac})^2 + (DI_{ch})^2 + (DI_{en})^2\right]^{1/2}\right\}$$

$$PHCI = \begin{bmatrix} PHCI_p + PHCI_t + PHCI_f + PHCI_l + PHCI_c \\ + PHCI_{iv} + PHCI_b + PHCI_{fr} + PHCI_s + PHCI_d \end{bmatrix}$$

• **ISPI İndeksi:**

Doğal emniyet ilkelerinin uygulanabilirliğinin ölçüsüdür ve 1'den 200'e değer alabilmektedir.

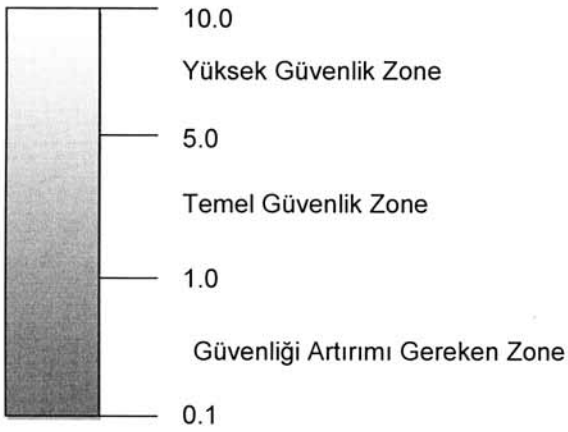
ISPI = ISI/PHCI

ISI hesaplaması, bir tesis veya ünitedeki tehlikeyi azaltmak için uygulanabilirlik ve yeteneğin alanında temel alınarak hesaplanır.

$$ISI = Min\left\{200, \left[(ISI_m)^2 + (ISI_{su})^2 + (ISI_a)^2 + (ISI_{si})^2 + (ISI_l)^2\right]^{1/2}\right\}$$

Şekil 55: ISI Yönteminin Uygulama Şeması

Şekil 56: I2SI Zone Haritası (Khan, Veitch ve Amyotte 2004: 16)



12.6.3. Çevre Sağlık ve Emniyet İndeksi – Environment Health &Safety Index (EHS)

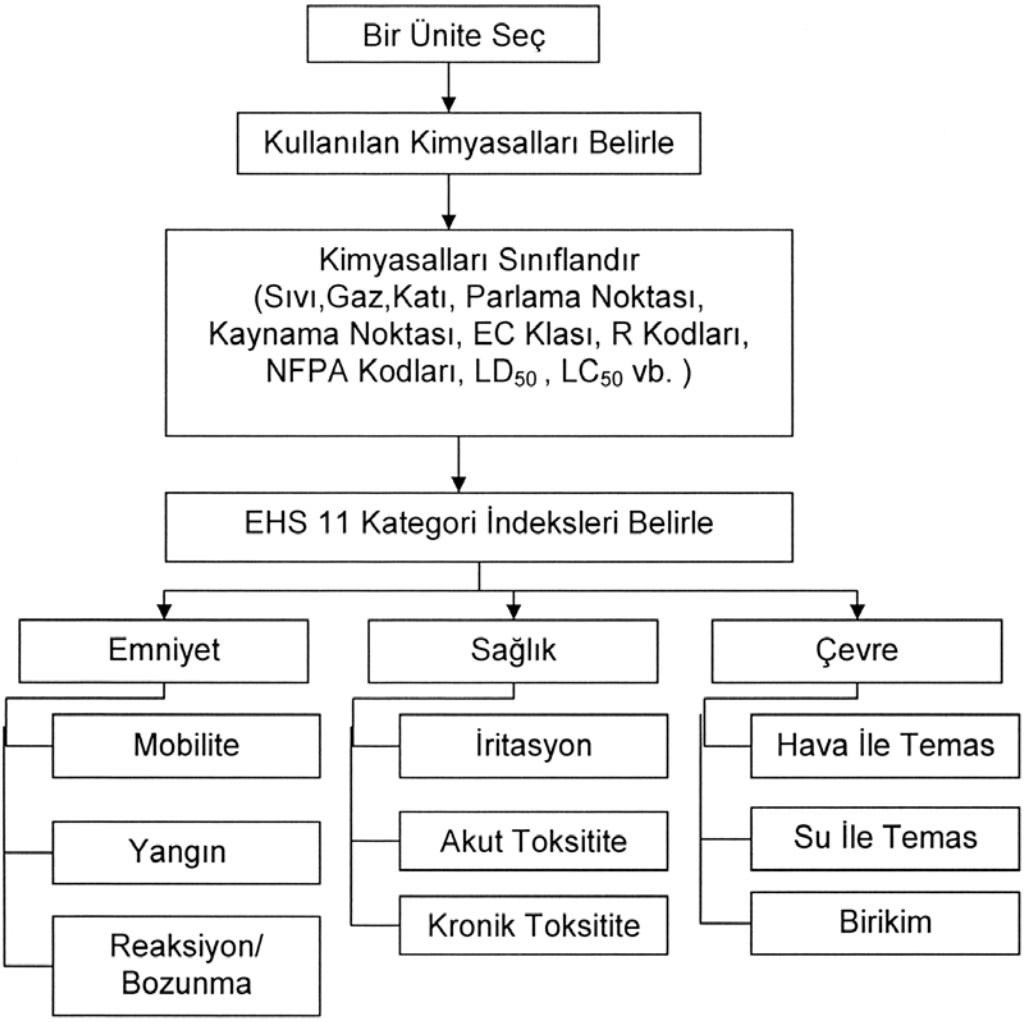
Çevre Sağlık ve Emniyet İndeksi – EHS bir tesis veya prosesin tehlike derecelendirmesini yapmak üzere Koller, Fischer ve Hungerbühler tarafından 2000 yılında geliştirilmiş, özellikle de erken dizayn aşamasında kullanımı oldukça yaygın olan bir indekstir. Bu yöntem aynı DOW F&EI gibi çok popular olmuş ve daha sonraları bu yöntemden SREST Katman Değerlendirme İndeksi (SREST Layer Assessment Index), SWeHI İndeksi (Safety Weighted Hazard Index) vb. bir çok indeks gelişmiştirilmiştir.

Sistem mimarisinden, kullanılan materyallere, proseslere ve parçalara kadar yapılan seçimlerin analiz ve testinin yapılması güvenilirlik açısından önem taşımaktadır. EHS tehlike derecelendirme indeksi, bir endüstri kompleksi içindeki fabrikaya ait birbirinden ayrı elementlerin sınıflandırılmasının nasıl yapıldığını göstermektedir.

Bir tesis veya prosesdeki kritik sistemlerin çökmesi durumunda insan hayatını veya çevreyi tehdit edebilecek ya da büyük ekonomik zarar verebilecek durumlar (örneğin; yangın, patlama, toksik kimyasallara maruziyet, çevresel kirlilik vb.) yaratırlar. Genellikle "Kritik Sistem"ler karmaşık sistemlerdir ve bu sistemlerdeki hatalar çoğunlukla tek bir durumdan oluşmaz çünkü bu tip sistemler tek bir noktadan oluşabilecek kusura karşı dayanıklıdırlar. EHS yöntemi proses veya sistemdeki tehlikelerin kapsamının sistematik olarak daha iyi anlaşılmasını ve güvenilirliğinin test edilmesini sağlamaktadır.

EHS metodundaki her bir kategori için indeksler prosedürde verilen 11 değişik katagori için verilen tablolardan bulunmaktadır. Bu tablolarda kimyasallar fiziksel ve kimyasal özellikleri, zehirlilik, yanıcılık, çevre ve güvenlik verilerine göre sınıflandırılmışlardır. Sistemin parçalarını bilen insanların tecrübelerini birleştirmek, buna dayanarak sistemin tümü üzerinde bir yorum yapmak, değişiklikler gerçekleştirmek veya alternatifler denemek için geliştirilmiştir.

Şekil 57: EHS Medotu Uygulama Şeması



13. BÖLÜM: BÜYÜK ENDÜSTRİYEL KAZALARIN KONTROLÜ HAKKINDA YÖNETMELİK GEREĞİNCE RİSK DEĞERLENDİRMESİ METODOLOJİSİ: ARAMIS PROJESİ

Özellikle 20. yüzyıl başlarından itibaren tehlikeli maddelerin artan üretimi, kullanımı ve depolanması yüzünden büyük endüstriyel kaza olasılığı büyük oranlarda artmıştır. Dolayısıyla da tüm halkın, çalışan kesimin ve çevrenin korunması gereği doğmuş, büyük endüstriyel kazaların önlenmesi için sistematik yaklaşım ihtiyacı belirmiştir.

Birçok insanın hayatını kaybettiği önemli kazalar kayda değer ilgi çekmekle birlikte psikolojik etkide oluşturmuştur. Çernobil, Mexico City, Zeebrugge vb. yerlerde yaşanan büyük endüstriyel kazalar toplumun kabul edebileceğinin çok üzerinde bir zararla sonuçlanmıştır. Büyük endüstriyel kazaları ve nedenlerini anlatan geniş bir literatür bulunmaktadır. Bu kazalardan birçok ders çıkarılmıştır. Özellikle ilgi çeken nokta, işyerinin planlanması ve işletilmesinden sorumlu olan üst yönetimin rolüdür. Bu tip ciddi deneyimler kimyasal ve nükleer tesislerde uygulanan mevzuatı değiştirmiş ve katılaştırmıştır. Ayrıca başlıca tehlikeli tesislerde güvenlik ve güvenilirlik analizinin gerekliliğini ortaya çıkarmış, organizasyonel faktörlerin de bu analizlere dahil edilmesinin zorunluluk olduğu anlaşılmıştır.

Kazalar incelendiğinde, yangın ve patlamaların meydana geldiği kazaların coğrafi ve iklimsel etkileri sınırlı olabilmektedir. Ancak Fransa'nın Toulouse şehrinde meydana gelen felakette olduğu gibi zehirli maddelerin havaya, suya ya da toprağa yayılmasıyla oluşan "DOMİNO ETKİSİ" sonucunda bu etkiler çok büyük boyutlara ulaşabilmektedir.

Tarihsel olarak en büyük endüstriyel felaket 1984 yılında Hindistan Bhopal'de meydana gelmiştir. Bu endüstriyel felaket sonucunda 2.000 ile 4.000 arası insan öldüğü ve 200.000 ile 400.000 civarında yaralanan veya kazadan etkilenen olduğu tahmin edilmektedir. Birçok insanın hayatını kaybettiği önemli kazalar kayda değer ilgi çekmekle birlikte psikolojik etkide de bulunmuştur. Çernobil, Mexico City, Enschede vb. gibi büyük endüstriyel kazaların tümü toplumun kabul edebileceğinin çok üzerinde bir zararla sonuçlanmıştır. Bu kazalardan birçok ders çıkarılabilir ancak burada özellikle işyerinin planlanması ve işletilmesinden sorumlu olan üst yönetimin rolü büyük bir önem arz etmektedir.

Bu tip ciddi deneyimler kimyasal ve nükleer tesislerde uygulanan mevzuatı değiştirmiş ve katılaştırmıştır. Ayrıca başlıca tehlikeli tesislerde güvenlik analizinin gerekliliğini ortaya çıkarmış, organizasyonel faktörlerin de bu analizlere

dâhil edilmesinin zorunluluk olduğu anlaşılmıştır. Kasım, 1989'da ILO Yönetim Kurulu'nun 244. toplantısında alınan karar uyarınca, Cenevre'de 8-17 Ekim 1990 tarihlerinde büyük endüstriyel tehlikelerin önlenmesine ilişkin uygulama kodu hazırlanması maksadıyla bir uzmanlar toplantısı düzenlenmiştir. Bu uzmanlar toplantısında Büro tarafından hazırlanan taslağa dayalı uygulama kodu gözden geçirilmiş ve son şeklini almıştır. Toplantıda bu koda "Büyük Endüstriyel Kazaların Önlenmesi" adı verilmesi kararlaştırılmıştır. Ancak hazırlanan bu kod büyük endüstriyel kazaların önlenmesi için tüm ilgililere sadece pratik tavsiyeler niteliğinde kalmıştır. Üç Mil Adası'ndaki ve Çernobil' deki nükleer kazalardan sonra otoriteler nükleer tesislerin güvenli işletilmesi için birçok çalışmalar yürütmüştür. Ancak klasik endüstriye ilişkin risk değerlendirme çalışmalarının hızla başlamasında İtalya Seveso'daki büyük endüstriyel kaza dönüm noktası olmuştur.

Kimyasal bir reaksiyon sonucu meydana gelen Seveso'daki kaza, dioksin yayılmasına neden olmuş ve kimya endüstrisinde işlem gören ürünlerin sebep olabileceği kazaların aniden bilincine varılmasına yol açmıştır. Bu kaza birçok yönden nükleer bir kazayı hatırlatmaktadır. Bölgede yaşayanların göremediği ve üzerinde yaşadıkları toprakların etkilenip etkilenmediğini anlayamadıkları bir toksik ürün yayılması olmuştur. Bu arada, radyo ve televizyonda uzmanlar sürekli olarak hiçbir riskin mevcut olmadığını söylerlerken başkaları dioksinin, insan eli ile hiç bir zaman üretilmemiş, en yüksek dozlu zehirler arasında olduğunu vurgulamışlardır. Sonuç olarak, herkes paniğe kapılmış ve mevcut durumda bu kaza sonucunda belirlenmiş hiçbir kurban olmamasına rağmen, Seveso çok ciddi bir kaza olarak hafızalarda yer etmiştir. Bhopal (Hindistan) kazası resmi kayıtlara geçen 2000 (gerçekte daha fazla) ölüm ile sonuçlanmış olmasına karşın, düzenlemeler üzerine daha az etkide bulunmuştur.

Avrupa'da Seveso'nun etkisi çok büyük olmuş ve Fransa'da 1984'de, belli sayıda sınıflandırılmış endüstri için tehlike araştırmaların yapılmasını talep eden ve o zamanın çevre bakanı olan Mme Huguette Bouchardeau tarafından imzalanmış bir sirküler ile vücuda getirilen ünlü Seveso yönergesinin Avrupa Topluluğu mevzuatına dahil edilmesine neden olmuştur.

Burada altı çizilmesi gereken nokta ilk kez Fransızca resmi bir metinde, tesislerse tehlike araştırmalarının gerçekleştirilmesi için kullanılmak üzere, risk değerlendirmesinin temel yöntemlerinden hata ağaçlarının kullanımını önermiştir. 1988'de Kuzey Denizi'nde Piper Alpha platformunda meydana gelen yangından sonra (167 ölü), Kuzey Denizi'ndeki çevre kirliliğini araştıran çeşitli ülke-

lerin (İngiltere, Norveç, Hollanda) güvenlik otoriteleri tarafından talep edilen güvenlik araştırmaları sayısında önemli ölçüde artış olmuştur.

İtalya'nın Seveso kasabasında 1976'da gerçekleşen ciddi endüstriyel kazayı takiben, endüstriyel donanımlarda kaza önleme üzerine bir Direktif olan Seveso Direktifi (82/501/EEC) kabul edilmiştir. Daha sonra Hindistan, Bhopal'de 1984 yılında ve İsviçre, Basel'de 1986 yılında gerçekleşen iki büyük kaza ve Mexico City'de doğal gaz patlaması sonucunun 500 ölü, 4.000 yaralı ile sonuçlanması bu direktifin tekrar gözden geçirilmesi gereğini doğurmuştur.

Tablo 57: 1959-2004 Yılları Arasında Meydana Gelen Kaza ve Felaketler

Yıl	Yer	Olay	Hasar
1959	Minamata, Japonya	Su yollarına cıva deşarj edilmesi	400 ölü, 2,000 yaralı
1973	Fort Wayne, A.B.D.	Demiryolu kazası ile vinil klorür dökülmesi.	4500 tahliye
1974	Flixborough, İngiltere.	Patlamada siklohekzan açığa çıkması	23 ölü, 104 yaralı, 3,000 tahliye
1976	Seveso, İtalya	Dioksin sızıntısı	193 yaralı, 730 tahliye
1978	Los Alfaquez, İspanya	Ulaşım kazasında propilen dökülmesi.	216 ölü, 200 yaralı
	Xilatopec, Meksika	Karayolu kazasında gaz tankeri patlaması.	100 ölü, 150 yaralı
	Manfredonia, İtalya	Fabrikadan amonyak sızıntısı	10,000 tahliye
1979	Threemile Adası, A.B.D.	Nükleer reaktör kazası	200,,,000 tahliye
	Novosbirsk, Rusya	Kimya fabrikasında patlama	300 ölü
	Mississagua, Kanada	Demiryolu kazası ile klor ve bütanın çevreye yayılması.	200,000 tahliye
1980	Summerville, A.B.D	Demiryolu kazası ile fosfortriklorür dökülmesi	300 yaralı, pek çok tahliye
	Tacoa, Venezüella	Petrol yangını ve patlaması	145 ölü, 1,000 tahliye
1982	Taft, A.B.D.	Patlamada kimyasallardan akrolein açığa çıkması	17,000 tahliye
1984	Sao Poulo, Brezilya	Petrol boru hattında patlama	508 ölü
	St. J.Ixhuatepec, Meksika	Gaz tankı patlaması	452 ölü, 4,248 yaralı, 300,000 tahliye
	Bhopal, Hindistan	Pestisit fabrikasından sızıntı siyan gazı	72,500 ölü, binlerce yaralı, 200,000 tahliye

1986	Çernobil, Rusya	Nükleer reaktör kazası	725 ölü, 300 yaralı, 90,000 tahliye, Avrupa ülkelerine yayılma
	Basel, İsviçre	Pestisit fabrikasında yangın	Ren nehrinde kirlilik
1987	Kotka, Finlandiya	Limanda monoklorobenzen dökülmesi	Deniz tabanı kirliliği
1991	Körfez Savaşı, Basra Körfezi	Petrol dökülmesi	Deniz kirliliği
1992	Alaska	Petrol dökülmesi	Deniz kirliliği
2000	Enschede, Hollanda	Havai fişek fabrikasında patlamada	21 kişi hayatını kaybetti. 800 kişi yaralandı ve 1 km^2 çaplı alanda 5300 kişi patlamadan ve sonuçlarından etkilendi.
2000	Baia Mare, Romanya	Yüksek konsantrasyonda siyanür içeren atık havuzunun aşırı yağışlarla yıkılması sonucu arıtılmamış siyanür atık Tuna Nehri'ne karıştı.	Nehir kirliliği
2001	Toulouse	Gübre tesisi patlaması sonucu standart dışı amonyum nitrat yayılımı	Geniş alanda etkilenme

II. Direktif (96/82/EEC), 1996 yılında kabul edilmiştir ve 82/501/EEC sayılı Direktif'in yerini almıştır. Enschede ve Toulouse kazalarına tepki olarak AB, amonyum nitratla birlikte, patlayıcı ve yanıcı maddelerle ilgili Seveso II yönetmeliğindeki kuralları tekrar gözden geçirmiş ve daha da sertleştirmiştir. AB, Enschede, Baia Mare ve Toulouse'daki kazalardan sonra SEVESO II'nin kapsamını genişletmiş ve SEVESO II'de görülen bazı aksaklıkların da çözümü için bazı ek çalışmalar yaparak 2003/105/EEC sayılı direktifi 16 Aralık 2003 tarihinde yayınlamıştır. Seveso II Direktifi adını alan veya diğer bir adıyla COMAH Direktifi; tehlikeli maddeler içeren büyük endüstriyel kazaların önlenmesine yönelik çeşitli kontrol yükümlülükleri getirmiştir.

Seveso II direktifi, "Önemli Kaza" terimi ile; yönetmelik kapsamındaki herhangi bir yerde çalışmanın sürdüğü anda kontrol dışında meydana gelen gelişmeler sonucunda oluşan ve insan hayatı ve/veya çevre üzerinde ani veya sonradan ortaya çıkan etkilere sahip, tesisin içinde veya dışında ve bir veya birkaç tehlikeli maddeyi içeren önemli bir sızıntı, yangın veya patlamayı belirtmektedir.

Direktif, büyük kaza zararları vermeye neden olabilecek miktarlarda belirli tehlikeli maddelerin bulunduğu kuruluşlara uygulanmaktadır. Bir işletme, eğer Ek

I'in, Bölüm 1 ve 2'sinde listelenmiş olan tehlikeli maddelerin depolanması Ek'te belirtilen miktarın üzerindeyse Direktif'in hükümlerine tabidir.

Seveso II Direktifi'nin faaliyet alanı yalnızca kuruluşlardaki tehlikeli maddelerin mevcudiyeti ile ilgilidir. Uzman yetkili aynı zamanda, kuruluşların bulundukları yer ve yakınlıkları nedeniyle büyük bir kazanın meydana gelme olasılığının artması (DOMİNO ETKİSİ) söz konusu ise, bahsi geçen kuruluşları veya kuruluş gruplarını tanımlamalıdır.

Seveso II Direktifi; askeri kuruluşlar, iyonize edici radyasyon zararları, tehlikeli maddelerin taşınması ve ara depolanması, boru hatlarında taşıma; sondaj kuyuları (Borehole) yoluyla madenlerde ve taş ocaklarında minerallerin araştırılması ve işlenmesi, atık depolama (metan patlamaları riski) için uygulanmamaktadır.

Direktifin Temel Şartları ise aşağıdaki gibidir;

- Direktif, büyük kaza zararları vermeye neden olabilecek miktarlarda belirli tehlikeli maddelerin bulunduğu kuruluşlara uygulanmaktadır,
- Direktif, iki-seviyeli bir yöntem izlemektedir; yani Ek I'de belirtilmiş her madde için iki farklı sınırlandırıcı nicelik mevcuttur (eşik değerleri), bir alt seviye ve bir de üst seviye. Bir kuruluşta bulunan maddelerin niceliği arttıkça, o kuruluşun neden olduğu zararın da arttığı varsayılmaktadır. Buna bağlı olarak, Direktif üst seviyeli kuruluşlara, alt seviyeli kuruluşlardan daha çok zorunluluk yüklemektedir,
- Büyük endüstriyel kazaları önlemek için sistem kurulması gerekmektedir; Büyük endüstriyel kaza riskini, bulundukları yer ve kullandıkları tehlikeli maddeler nedeniyle, arttıran tesislerin veya tesis gruplarının tanımlanması kayıt, altına alınarak Avrupa Komisyonuna bildirilmesi gerekmektedir,
- Yetkili otoritelerce Domino Etkileri dikkate alınarak, büyük endüstriyel kazaları engellemek ve etkilerini en aza indirgemek yükümlülüğü getirilmektedir,
- Büyük endüstriyel kaza sırasında uygulanacak tesis dışı acil durum planlarının hazırlanması, gözden geçirilmesi, test edilmesi ve revize edilmesi gerekmektedir,
- Halkın direktifin uygulanmasına ilişkin gizlilik gerektiren belirli bilgiler dışında bilgilere erişebiliyor olmasının sağlanması, büyük kaza etkilerine maruz kalacak bireylere ve diğer üye ülkelere güvenlik önlemleri ve pro-

sedürleri konularında bilgi sağlanması, ÇED bağlantısının kurulması gerekmektedir,

- Arazi kullanım ve diğer ilgili politikalarda büyük endüstriyel kazalara karşı koruma ile ilgili hedeflerin dikkate alınmasının sağlanması, ve bu politikaların uygulanmasını kolaylaştıracak destek prosedürlerin oluşturulması gerekmektedir.

Yukarıda sayılan şartlara bağlı olarak, Direktif üst seviyeli kuruluşlara, alt seviyeli kuruluşlardan daha çok zorunluluk yüklemektedir, ayrıca üretim sürecinde belli bir miktarın üzerinde kimyasal depolayan firmalara yeni yükümlülükler getirilecektir. Buna göre, kuruluşların yükümlülükleri aşağıda verilmiştir;

- Alt-seviye kuruluşların yükümlülükleri; bildirim, büyük kazaları önleme politikası, modifikasyonlar, kaza raporları ve yetkililerle işbirliğidir.
- Üst-seviye kuruluşların yükümlülükleri ise; alt-seviye kuruluşların yükümlülüklerine ek olarak, güvenlik raporu ile dahili acil durum planları hazırlanması ve kamunun bilgilendirilmesidir.
- Yerel yönetimlerin ise; bölgesel harici acil durum planları hazırlanması ve arazi kullanımı politikalarına Direktifte öngörülen kısıtları eklemeleri beklenmektedir.

Aynı zamanda kamunun bilgilendirilmesine dair zorunluluklar bulunmaktadır. Bir diğer gereklilik ise büyük endüstriyel kaza riskini, bulundukları yer ve kullandıkları tehlikeli maddeler nedeniyle, arttıran tesislerin veya tesis gruplarının tanımlanması kayıt altına alınarak Avrupa Komisyonuna bildirilmesi yükümlülüğünün getirilmiş olmasıdır.

Direktifte yer alan yükümlülüklerin işletme sahipleri tarafından yerine getirilmesinin sağlanması ve direktifin hükümlerine uymayan tesislerin çalışmalarının yasaklanması da sanayi açısından önem arzeden bir konudur. İşletme sahiplerinin, yetkili otorite tarafından konan yasaklara karşı gelmesi durumunda konunun mahkemeye intikal ettirilmesi öngörülmektedir.

Ayrıca Hükümetler de genel anlamda büyük endüstriyel kazaları engellemek için önlemlerin alınması ve bu kazaların neden olacağı etkilerinin en aza indirgenmesi ve büyük kazaların takip edilmesi, belirli önlemlerin alınmasının sağlaması, bilgilerin toplanması ve analiz edilmesi dahil, zararlara çare bulunması, gelecekteki kazaların önlenmesi için öneriler hazırlanması gibi konularda da sorumlu kılınmışlardır.

Seveso Direktifine göre, bütün sanayi kuruluşlarının bir acil durum hareket planı yapma ve uygulama sorumluluğu vardır. Kimyasal madde üreten ve kullanan sanayiler, endüstriyel risklerin kaynağı hem de en çok zarar gören taraf olarak, çalışma esnasında en yüksek güvenlik standartlarına uymak sorumluluğunu taşımaktadırlar. Seveso Direktifi kapsamında, bu maddelerin insanlara ve çevreye en az zararlı etkiye sahip olmasına çalışılmak, bu maddeleri işleyen işçiye, kullananlara ve üretim bölgesi sakinlerine kimyasal maddelerin nitelikleri, üretim süreçleri ve karşılaştırmalı riskleri konusunda en geniş açıklamalar yapılmak ve en önemlisi de dahili ve harici olmak üzere acil eylem planları hazırlamak zorundadırlar.

Türkiye'de Çevre ve Şehircilik Bakanlığı, Çevre ile ilgili Mevzuatının Analizi Projesi kapsamında AB'den gelen teknik ve finansal yardımlarla Tehlikeli Madde İçeren Kazaların Kontrolüne İlişkin Seveso II Direktifinin uyumlaştırılması konusundaki çalışmalarını, LİFE 03 TCY/000064 proje çalışmaları kapsamında 2004 yılında başlatmıştır. Bu çalışmalar sonucunda; Seveso II Direktifi ile uyumlu olarak; "Büyük Endüstriyel Kazaların Kontrolü Hakkında Yönetmelik" 18 Ağustos 2010 tarihli ve 27676 sayılı Resmi Gazete 'de yayımlanmıştır.

Çevre ve Şehircilik Bakanlığı tarafından 31 Temmuz 2012 tarihli ve 28370 sayılı Resmî Gazetede yayımlanan yönetmelik ile yürürlük tarihinde değişiklik yapılmıştır. Bakanlık daha önce 18 Ağustos 2010 tarihli ve 27676 sayılı Resmi Gazete yayımlanmış olan "Büyük Endüstriyel Kazaların Kontrolü Hakkında Yönetmelik" kapsamında gerekli çalışmaların tamamlanması için belirlenen 18 Ağustos 2012 son tarihini, 1 Ocak 2014 olarak değiştirmiştir.

Son olarak ise; 30 Aralık 2014 tarih ve 28867 sayılı Mükerrer Resmi Gazete'de Büyük Endüstriyel Kazaların Önlenmesi ve Etkilerinin Azaltılması Hakkında Yönetmelik yayınlanmıştır ve eski yönetmelik iptal edilmiştir. Böylece yapılan değişiklikle birlikte, yönetmelik kapsamında, işletmelerin yapmakla yükümlü oldukları "bildirim" dışındaki "Büyük Kaza Önleme Politikası, Güvenlik Raporu, Dahili Acil Durum Planı" hazırlanması ve sunulması ile ilgili yükümlülükler, 1 Ocak 2016 tarihine ötelenmiştir.

13.1. SEVESO III Direktifi

Seveso II Direktifi, büyük kaza zararları vermeye neden olabilecek miktarlarda belirli tehlikeli maddelerin bulunduğu kuruluşlara uygulanmaktadır. Bir işletme, eğer Ek I'in , Bölüm 1 ve 2'sinde listelenmiş olan tehlikeli maddelerin depolanması Ek'te belirtilen miktarın üzerindeyse Direktif'in hükümlerine tabidir.

Seveso II Direktifi'nin faaliyet alanı yalnızca kuruluşlardaki tehlikeli maddelerin mevcudiyeti ile ilgilidir. Uzman yetkili aynı zamanda, kuruluşların bulundukları yer ve yakınlıkları nedeniyle büyük bir kazanın meydana gelme olasılığının artması (Domino Etkisi) söz konusu ise, bahsi geçen kuruluşları veya kuruluş gruplarını tanımlamalıdır.

2012/18/EEC sayılı SEVESO III Direktifi, 26 Haziran 2012 tarihinde AB Bakanlar Konseyi'nde kabul edilmiştir. Yeni direktif 1 Ocak 2015 tarihinde yürürlüğe girecektir, "Tehlikeli Maddelerle İlgili Büyük Kaza Risklerinin Kontrolüne İlişkin Yönerge" 96/82/EC Sayılı SEVESO II Yönergesi ise 2015 yılında yürürlükten kaldırılacaktır. Yeni direktif kapsamında;

- Tehlikeli maddelerin tanımlandığı Ek I kısmı, maddelerin sınıflandırılması ile ilgili AB mevzuatına yani CLP tüzüğüne uyumlu hale getirilecektir,
- Büyük çaptaki kazalarla ilgili kamuoyunun güvenli bilgiye erişimi ve karar almada daha etkili şekilde yer alması sağlanacaktır,
- Denetim mekanizmaları daha sıkı kurallara tabi olacak ve devletin ilgili birimlerine yeni yükümlülükler getirilecektir.

Seveso III Direktifi çerçevesinde ise; mevcut Direktif'in, tehlikeli madde ve karışımları listeleyen I numaralı Ek'ini, madde ve karışımların sınıflandırılması, etiketlenmesi ve ambalajlanmasına ilişkin 1272/2008/EC sayılı Tüzük'te (CLP Tüzüğü) yapılan değişikliklere göre revize eden yeni 2012/18/EEC sayılı Direktif, sağlığa zararlı maddeleri de CLP Tüzüğü'ndeki kategorilere uygun olarak yeniden tanımlanmaktadır. Buna göre, Seveso II Direktifi'ndeki 3 "Çok toksik" kategorisi "Akut toksik 1"e, "Toksik" kategorisi "Akut toksik 2"ye (tüm maruziyet yolları) ve "Akut toksik 3"e (dermal ve soluma yolları) dönüştürülmüş olacaktır.

Mevcut düzenlemede daha genel özellikleriyle belirtilen fiziksel tehlikelere ilişkin oksitleyici, patlayıcı, alevlenebilir madde kategorileri tanımlarının yerini de, CLP Tüzüğü'nde yer alan spesifik kategori tanımları yer alacaktır.

Güvenlik kurallarının eksiksiz ve etkin uygulanmasının sağlanması için, tesislere yönelik denetim standartlarını sıkılaştıran yeni düzenleme, mümkün olabilecek en yüksek seviyede güvenliğin tesis edilebilmesi amacıyla, alınması gereken önlemlere yenilerini eklerken, idari yüklerin hafifletilebilmesi için mevzuatta da basitleştirmeye gitmektedir. Düzenleme ayrıca, halkın Direktif kapsamındaki alanlarda güvenlikle ilgili bilgilere erişiminin ve karar mekanizmalarına katılımının artırılmasının yanı sıra, bilginin toplanması, yönetimi ve paylaşımına iliş-

kin süreçlerin iyileştirilmesini ve denetim mekanizmalarının sıkılaştırılmasını da içermektedir.

13.2. ARAMIS Projesi Nedir?

Avrupa Komisyonu'nun beşinci çerçeve programında yer alan ve ortaklaşa yatırım yapılan bir Avrupa projesi olarak geliştirilmiş olan ARAMIS (Accidental Risk Assessment Methodology for IndustrieS) projesi işletmelere Seveso Direktifi çerçevesinde uygulayabilecekleri risk değerlendirmesi için bir metodoloji sunmaktadır.

ARAMIS Projesi toplam 7 modülden oluşmaktadır. Her modül ayrıntılı olarak örnekler de içermektedir. Ayrıca ARAMIS Projesinin modülleri internet üzerinden tüm kullanıcılara açıktır. Modüllere; http://mahb.jrc.it internet sayfasında projeler sayfasından ulaşılabilmektedir. Projenin bitimini müteakip çalıştayların bildirileri de web sitesinde ulaşılabilir konumdadır. Bunun yanında çalıştaylarla bağlantılı olarak, proje esnasında elde edilen sonuçların geniş bir şekilde yaygınlaştırılmasını sağlamak için katılımcılar makalelerini uluslararası bilimsel dergilerde ve konferanslarda yayınlanmışlardır. Proje için oluşturulan konsorsiyum on farklı organizasyondan oluşmaktadır. Bunlar **Tablo 58**'de sunulmuştur.

Tablo 58: Ortak Organizasyonlar

Organizasyon Adı	Kısa Adı	Ülke
1. Institut National de l'Environnement Industriel et des Risques Accidental Risk Division	INERIS	FRANSA
2. European Commission - Joint Research Centre - Institute for the Protection and Security of the Citizen- Major Accident Hazard Bureau	EC-JRC-IPSC-MAHB	İTALYA
3. Faculté Polytechnique de Mons Major Risk Research Center	FPMs-MRRC	BELÇİKA
4. Universitat Politecnica de Catalunya Centre for Studies on Technological Risk (CERTEC)	UPC	İSPANYA
5. Association pour la Recherche et le Développement des Méthodes et Processus Industriels	ARMINES	FRANSA
6. Risø National Laboratory System Analysis Department	RISOE	DANİMARKA
7. Universita di Roma Dipartimento Ingegneria Chimica	UROM	İTALYA
8. Central Mining Institute Safety Management and Technical Hazards	CMI	POLONYA
9. Delft University of Technology Safety Science Group	TUD	HOLLANDA
10. Institution of Chemical Engineers European Process Safety Centre	IChemEEPSC	İNGİLTERE

ARAMIS - Seveso II Direktifi Kapsamındaki Endüstrilerde Kaza Riski Değerlendirme Metodolojisi (**Accidental Risk Assessment Methodology for IndustrieS**), SEVESO II direktifinin özel gereksinimlerine cevap verebilmek amacıyla Avrupa Komisyonu'nun V. Çerçeve programında yer alan ve ortaklaşa yatırım yapılan bir Avrupa projesi olarak geliştirilmiştir. Proje "Enerji, Çevre ve Sürdürülebilir Gelişme" alanındaki "Araştırma ve Teknolojik Gelişim için V. Çerçeve Programı" kapsamında, "Büyük Doğal ve Teknolojik Tehlikelerle Mücadele" başlıklı bölümü ile ilgili kabul edilmiştir.

Toplam üç yıl süre ile devam eden proje, 2002 yılının Ocak ayında başlanmış ve tamamlanmıştır. Bu metodoloji, sanayiciye kendi işyerlerinde ve özellikle de proseslerinde yeterli bir risk kontrolü olduğunu göstermede yardımcı olmak için inşa edilmiştir. Avrupa Birliği tarafından desteklenen ve dördüncü çerçeve programı kapsamında düzenlenen ASSURANCE ve I-RISK projelerinin sonuçları üzerine kurulmuştur.

ASSURANCE kelimesi, "Kimya Kuruluşlarına ait Risk Analizinin Tutarsızlıklarının Değerlendirilmesi" anlamına gelen ingilizce proje başlığının baş harfleri kullanılarak oluşturulmuştur. I-RISK projesi ise, kantitatif risk değerlendirmesi ile güvenlik denetiminin, büyük kazaların kontrolünde iki ayrı değerli araç olduğu düşüncesinden ortaya çıkmıştır. Bu nedenle ana hedef, risklerin kontrolü ve izlenmesi için bir yönetim modeli geliştirmek ve daha sonra bu modeli dinamik yapıda olan kantitatif risk değerlendirmesi yöntemine dahil etmektir. Projenin sonucunda tümleşik teknik ve yönetime dayalı bu modelin çok sağlam olduğu ve denetim kurumlarına yeni bir yol gösterdiği açıkça görülmüştür.

Bu iki proje ve katılımcı ülkelerde gerçekleşen kazlardan edinilen tecrübelerle birlikte, her bir tesis işleticisine özgü büyük kaza senaryolarının tespiti ile bunları hem engelleme hem de hafifletme önlemlerini dikkate alan ve tutarlı kurallara dayanan bir yöntemin gerekliliğini ortaya çıkarmıştır. Ayrıca bu yöntem ile güvenlik önlemleri bir güvenlik yönetim sistemi içinde kontrol edilebilir hale gelmiştir. Hem yetkili kuruluşların risk uzmanları hem de endüstri kökenli risk uzmanları arasında uzlaşma oluşmasını sağlayacak, risk tabanlı kararların verilmesinde tutarsızlıkları azaltacak bir risk değerlendirme metoduna olan gereksinim de böylece ortaya çıkmıştır. ARAMIS projesi de, bu gereksinimlere çözüm yolu sunmak amacıyla başlamıştır.

Bu metodolojinin bir avantajı sanayicilere proses emniyetini sağlamak için hangi bariyerlerin (kontrol önlemleri) risk kontrolü üzerinde etkisi olduğunu ya da

hangilerinin geliştirilmesi gerektiğini göstermesidir. İşverenlere; proseste güvenliği ve güvenilirliği artırmak için hangi kontrol önlemlerine yatırım yapmaları gerektiğini belirlemeleri açısından yardımcı olur ve en önemlisi ise kantitatif olarak ALARP seviyesini tespit etmelerini sağlar. Güvenlik bariyerlerinin performansının değerlendirilmesi sanayicilerin fabrikada daha etkili güvenlik düzeyi oluşturabilecek güvenlik fonksiyonlarını (bariyerler) tanımalarını sağlar. Bunun yanında, yasal otoritelerin risk kontrolünü değerlendirebilmesi ve riskin azaltılmasında rol alan bariyerlerin detaylı kontrol edilebilmesi için de geniş ve kapsamlı bir analiz yapılmasını temin eder. Yönetmelik gereğince devlete verilmesi gereken Güvenlik Raporu içerisinde kantitatif risk değerlendirmesi ile ALARP seviyesinin rahatlıkla incelenebilmesi için kolay ve anlaşılabilir gösterim sağlar.

Proses endüstrisinde risk değerlendirmesindeki en temel nokta olası kaza senaryolarının tanımlanmasıdır. Ancak bilhassa deterministik yöntemlerde, kullanılan güvenlik sistemleri ve uygulanan güvenlik politikaları hesaba katılmadan en temel kötü senaryolar dikkate alınır. Bu yöntem risk derecesinin var olandan yüksek olarak tahmin edilmesine yol açar ve güvenlik sistemlerinin uygulanmasını desteklemez. ARAMIS projesinin amaçlarından birisi de bu problemle yüzleşebilecek bir metodolojinin geliştirilmesidir.

ARAMIS'in genel amacı, endüstriyel kuruluşlar için risk değerlendirmesinde kullanılan deterministik ve risk bazlı yöntemlerin kuvvetli yönlerini birleştiren, kazalara yönelik yeni bir risk değerlendirme metodolojisini oluşturmaktır. Bu yöntem esas olarak şu adımlardan oluşmaktadır:

- Büyük çaplı kaza tehlikelerinin tanımlanması metodolojisi (MIMAH),
- Kaza senaryolarının tanımlanması metodolojisi (MIRAS),
- Güvenlik önlemlerinin belirlenmesi ve performanslarının değerlendirilmesi,
- Güvenlik yönetimi etkinliğinin önlemlerin güvenilirliğine göre değerlendirilmesi,
- Referans senaryoların risk ağırlıklarının değerlendirilip haritalandırılması,
- Fabrika ve çevresindeki maruziyet değerlerinin değerlendirilip haritalandırılmasıdır.

Beşinci AB Çerçeve Programında ortaklaşa yatırım yapılan bu 3 yıllık proje Ocak 2002'de başlamış ve 2004 yılının sonunda sona ermiştir. Bir yıl sonra ise bu metodoloji tamamlanmış ve çıktıları yayınlanmıştır. Projenin tüm Avrupa'da Seveso II direktifinin eş zamanlı olarak uygulanmasını destekleyen ve hızlandıran bir araç haline gelmesi amaçlanmıştır.

Bu proje çalışmasının ilk sonucu, kullanılan ekipman ve malzemenin tiplerine bağlı olarak oluşturulan geniş kapsamlı hata ve olay ağaçlarının oluşturulması yoluyla gerçekleştirilen "Büyük Çaplı Kaza Tehlikelerinin Tanımlanması Metodolojisi" (MIMAH)'ın geliştirilmesidir. Buradaki "büyük çaplı kaza" teriminden hiçbir güvenlik sistemine sahip olmadığı varsayılan ekipmanlarla meydana gelen en kötü kaza senaryoları anlaşılmalıdır.

İkinci bir yöntem olan "Referans Kaza Senaryolarının Tanımlanması Metodolojisi" (MIRAS), güvenlik sistemlerinin kazaların olası sonuçları ve frekansları üzerine etkilerini dikkate almaktadır. Bu metodoloji ile daha gerçekçi kaza senaryolarının tanımlanması sağlanmaktadır. Referans olarak alınan kaza senaryolarının seçimi, kazaların frekanslarına ve önem derecelerine göre oluşturulan "risk matrisi" denilen bir araç yardımıyla yapılır.

13.3. SEVESO Kuruluşlarında Büyük Kaza Senaryolarının Tanımlanması

Kaza senaryolarının tanımlanması Güvenlik Yönetim Sistemi'nin en önemli modülü olan C Modülünün bir parçasıdır. Bu modül risk değerlendirmesinde bir önemli bir noktadır ve ALARP seviyesinin değerlendirilmesinde de temel oluşturmaktadır. Muhtemel kaza senaryolarının belirlenmesi risk değerlendirmede önemli bir noktadır. Ancak, deterministik yaklaşımda sadece kötü durum senaryoları dikkate alınmakta, genellikle güvenlik araçlarının ve uygulanan güvenlik senaryolarının etkisi dikkate alınmamaktadır. Bu yaklaşım risk seviyesinin olduğundan fazla olarak tahmin edilmesine yol açmakta ve güvenlik sistemlerinin uygulanmasını teşvik edici olmamaktadır.

ARAMIS Avrupa Projesi'nde amaç, birinci aşamada güvenlik sistemlerini dikkate almadan büyük kazaları tanımlamaktır, ikinci aşamada ise tanımlanan kaza senaryoları için güvenlik sistemleri, kazaların nedenleri ve olasılıkları derinlemesine incemektir. Son aşamada ise güvenlik sistemlerini dikkate alarak büyük kaza senaryosunu yeniden değerlendirmektir. Bu hedefe ulaşabilmek için iki ana adım tanımlanmıştır. Birinci hedef büyük kaza tehlikelerinin tanımlanması için bir metodoloji (MIMAH) gelitirilmesi, ikinci hedef ise MIMAH metodolojisi tarafından tanımlanan senaryolar üzerinden güvenlik bariyerleri (kontrol önlemleri) hakkında çalışma yapmak üzere bir metodoloji (MIRAS) geliştirilmesidir.

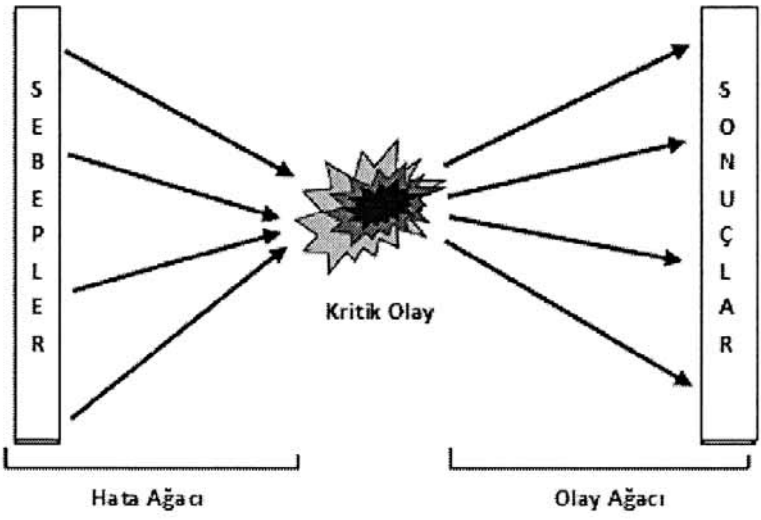
13.4. Büyük Çaplı Kaza Tehlikelerinin Tanımlanması (MIMAH)

Büyük kaza tehlikelerinin belirlenmesi ARAMIS projesinde kısaltması MIMAH olan "Büyük Kaza Tehlikelerinin Tanımlanması Metodolojisi" ile ger-

çekleştirilir. Büyük kaza tehlikeleri, hiçbir güvenlik bariyeri uygulanmadan ya da yetersiz olarak uygulandığı varsayılarak bir fabrikada ortaya çıkabilecek kazaları ifade etmektedir. Büyük Çaplı Kaza Tehlikelerinin Tanımlanması Metodolojisi (MIMAH), dikkate alınan ekipmanlara ve kullanılan maddelere bağlı olarak ne tür büyük çaplı kazaların meydana gelebileceğini tanımlamamıza olanak sağlar. "Büyük çaplı kaza" teriminden hiçbir güvenlik sisteminin (güvenlik yönetim sistemleri dahil) olmadığı veya etkin olarak kullanılmadığı varsayılan alanlarda meydana gelen en kötü kaza senaryoları anlaşılmalıdır. Büyük Kaza Tehlikeleri sadece ekipmanların karakteristiklerine ve ekipmanlarla kullanılan kimyasalların tehlikeli özelliklerine bağlı olacaktır.

MIMAH, büyük çaplı kazalara ait tehlikelerin belirlenmesini sağlayan bir yöntemdir. Genellikle bir hata ağacı ile olay ağacından meydana gelen "Papyon Diyagramları"nın kullanılması ile uygulanır. Papyonun merkezinde kritik olay yer alır. Kritik olay (CE) genellikle içeriğin (loss of containment – LOC) veya fiziksel bütünlüğün kaybedilmesi (loss of physical integrity – LPI) olarak tanımlanır. Papyon diyagramının sol tarafına hata ağacı denilir ve ele alınan kritik olaya ait olası sebeplerin tanımlanmasına yardımcı olur. Papyonun sağ tarafına olay ağacı denir ve kritik olayın olası sonuçlarının tanımlanmasını sağlar.

Şekil 58: Papyon Diyagramı



Kimyasal maddelerin kullanıldığı, üretildiği veya depolandığı tesisler için riskin tanımlanmasında, meydana gelmesi olası tüm kritik olayların listelenmesi için MIMAH'tan yararlanılabilir. Daha sonra bu kritik olayların her biri için MIMAH bu olaylardan sonra meydana gelebilecek ikincil olaylar ve tehlike olgusu bakımından olası sonuçların tanımlanmasına imkan sağlamaktadır.

13.4.1. MIMAH'ın Adımları

Analize başlanmadan önce bazı verilerin toplanması gerekir. Diğer bazı veriler de farklı adımlar süresince elde edilebilir. İlk olarak tesis yerleşim planı, proseslerin tanımlanması, ekipmanın ve tesiste kullanılan boruların belirlenmesi gibi tesis hakkında genel bilgilere ihtiyaç vardır. Ayrıca depolanan ve kullanılan maddelerle ve bu maddelerin tehlikeli özellikleri ile ilgili bilgilerin elde edilmesi gerekir. Tanımlanmış olan "Büyük Çaplı Kazalara Sebep Olan Tehlikeler" sadece ele alınan ekipmanın cinsiyle, fiziksel durum şartlarıyla ve kullanılan kimyasalların tehlikeli özellikleri ile ilişkilendirilmiştir. MIMAH yönteminde aşağıdaki 7 adım izlenmektedir:

Adım 1: Gerekli bilgilerin toplanması

Adım 2: Tesis içerisinde tehlike potansiyeli olan ekipmanların belirlenmesi

Adım 3: Uygun tehlikeli ekipmanın seçilmesi

Adım 4: Seçilen her ekipman ile ilgili kritik olayların ilişkilendirilmesi

Adım 5: Her bir kritik olay için hata ağaçlarının oluşturulması

Adım 6: Her bir kritik olay için olay ağaçlarının oluşturulması

Adım 7: Seçilen her ekipman için papyon diyagramlarının çizilmesi

ARAMIS projesinde seçilen yaklaşım papyon metodudur. Bu metod referans kaza senaryolarının açıklanması için çok iyi yapılandırılmış bir araçtır, kritik olayların(papyonun orta noktası) tanımlanmasına olanak sunar, büyük kaza senaryosunun (olay ağacı) yapılanmasını oluşturur, kazaların sepebleri (hata ağacı) üzerinde beyin fırtınası yapılmasına olanak sağlar, olasılıkların tahmin edilmesi ile güvenlik bariyerlerinin yerleştirilmesi için imkan sağlar. Ayrıca papyon yaklaşımı "Güvenlik Yönetim Sistemi"nin de en önemli parçasıdır. Büyük Çaplı Kazalara Yönelik Tehlikelerin Belirlenmesi Metodolojisinin uygulanabilmesi için gerekli olan minimum bilgi listesi aşağıdaki gibidir:

1. Tesis hakkında genel bilgiler (tesis ve bu tesisteki prosesler hakkında genel bir fikre sahip olabilmek için);

- Tesis yerleşimi,
- Proseslerin kısaca açıklanması,
- Kullanılan ekipmanların ve boru hatlarının kısaca açıklanması,
- Tesisteki ilgili ekipman listesiyle ilişkili işlenen ve depolanan maddelerin listesi,
- Bu maddelerin tehlikeli özellikleri (risk ibareleri, tehlike sınıflaması).

2. Tehlike potansiyeli olan her bir ekipman için;
   - Ekipmanın adı,
   - Büyüklüğü (hacim, boyutları),
   - Çalışma basıncı ve sıcaklığı,
   - İşlenen maddeler,
   - Bu maddelerin fiziksel hali,
   - Ekipman "içerisindeki" madde miktarı (madde içerik miktarı için kg veya akış halinde olanlar için kg/sn),
   - Bu maddelerin kaynama noktaları.

13.4.2. Ekipman Tipolojisi

Ekipmanlar fonksiyon ve işlem durumlarına göre genel kategorilerle sınıflandırılırlar. Gerekli bir kural tüm bu sınıflandırma esnasında akılda tutulmalıdır: aynı kategoride sınıflandırılan ekipman aynı genel papyonu üretmelidir. **Tablo 59**'da kullanılan ekipmanların tipolojisi verilmiştir.

Tablo 59: Ekipman tipolojisi

İŞARETLEME	Ekipman Tipi
EQ1	Yığın olarak katı halde depolama
EQ2	Küçük paketler halinde katı olarak depolama
EQ3	Küçük paketler halinde sıvı olarak depolama
EQ4	Basınç altında depolama
EQ5	Yalıtılmış halde depolama
EQ6	Atmosferik basınçta depolama
EQ7	Kriyojenik olarak depolama

EQ8	Basınçlı taşıma (iletim) ekipmanı/aracı
EQ9	Atmosferik Taşıma (iletim) ekipmanı/aracı
EQ10	Boru iletim ağı
EQ11	Prosese dahil edilmiş ara depolama ekipmanı
EQ12	Maddelerin fiziksel veya kimyasal olarak ayrışması için kullanılan ekipmanlar
EQ13	Kimyasal reaksiyonlar içeren ekipmanlar
EQ14	Enerji üretimi ve ısı değişiminde kullanılan ekipmanlar
EQ15	Paketleme ekipmanları
EQ16	Diğer ekipmanlar

13.4.3. Madde Tipolojisi

Metodoloji; Avrupa Birliğinde, tehlikeli maddelerin paketlenmesi ve etiketlenmesi ile ilgili 67/548/EC Direktifi çerçevesindeki sınıflandırmayı kullanmaktadır. ARAMIS projesi SEVESO II Direktifi'nin yapısına uymaktadır. Bunun nedeni ARAMIS tipolojisinin Direktif 67/548/EC'de tanımlanmış olan risk yaklaşımlarının da bulunduğu, SEVESO II direktifinin tehlike kategorilerini temel almasıdır. Aynı zamanda Seveso III Direktifi çerçevesinde CLP Tüzüğü'ne geçiş için de kolaylık sunmaktadır.

Tablo 60: Tehlikeli Maddelerin Ssınıflandırılması

Kategori	**Risk İfadeleri**
Çok toksik	R26, R100
Toksik	R23, R101
Oksitleyici	R7, R8, R9
Patlayıcı	R1, R2, R3, R4, R5, R6, R16, R19, R44, R102
Alevlenebilir	R10, R18
Kolay alevlenebilir	R10, R11, R17, R30
Çok kolay alevlenebilir	R10, R11, R12
Suyla şiddetli reaksiyona giren	R14, R15, R29, R14/15, R15/29
Başka bir maddeyle şiddetli reaksiyona giren	R103, R104, R105, R106
Çevre için tehlikeli (su ortamları için)	R 50, R51
Çevre için tehlikeli (su ortamları dışındaki ortamlar için)	R54, R55, R56, R57, R59

Tablo 61: Maddenin Özelliklerine Göre Referans Olarak Alınacak Kütleler

	Referans Alınan Kütle Ma (kg)		
Maddenin Özellikleri	**Katı**	**Sıvı**	**Gaz**
1 Çok toksik	10.000	1.000	100
2 Toksik	100.000	10.000	1.000
3 Oksitleyici	10.000	10.000	10.000
4 Patlayıcı (Seveso II Direktifi Ek 1 Tanım 2a)	10.000	10.000	---
5 Patlayıcı (Seveso II Direktifi Ek 1 Tanım 2b)	1.000	1.000	---
6 Alevlenebilir	---	10.000	---
7 Kolay alevlenebilir	---	10.000	---
8 Çok kolay alevlenebilir	---	10.000	1.000
9 Çevre için zararlı	100.000	10.000	1.000
10 R14, R14/15, R29 risk ibareleri kombinasyonlarında yukarıda verilen özellikler tarafından kapsanmayan sınıflandırma	10.000	10.000	---

Bu metodu kullanabilmek için, ekipmanlara ait şu bilgiler gereklidir:

- Ekipmanın adı,
- Ekipmanın tipi,
- Kullanılan tehlikeli madde,
- Maddenin fiziksel hali,
- Kaynama sıcaklığı (°C olarak),
- Çalışma sıcaklığı (°C olarak),
- Risk ibareleri,
- Tehlike sınıflandırılması,
- Ekipman içindeki maddenin kütlesi (kg olarak) veya içinde akış olan ekipman için (borular gibi) 10 dakikada geçen tehlikeli madde kütlesi.

13.4.4. Tehlikeli Ekipmanın Seçimi

İlgili tehlikeli ekipmanın seçiminde genel olarak prensip şu şekilde ifade edilmektedir: "tehlikeli maddeler içeren bir ekipman, eğer bu ekipmanın içindeki tehlikeli madde miktarı, tehlikenin eşik şiddetine eşit veya eşik şiddetinden daha büyük bir tehlike yaratacak kadar büyükse o zaman bu madde ilgili tehlikeli ekip-

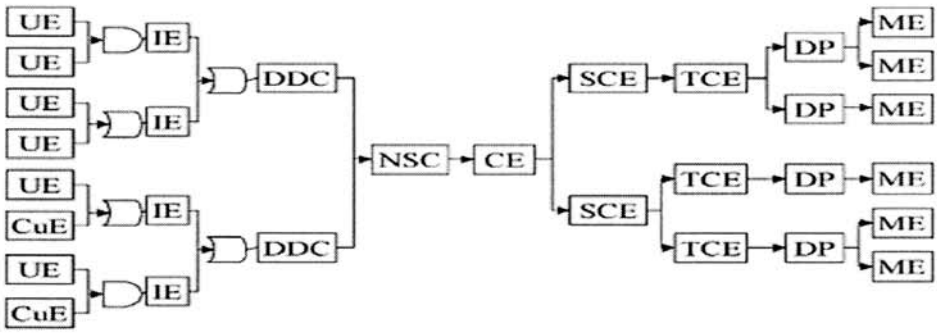
man olarak tanımlanmalıdır." Eşik şiddeti değeri maddenin tehlikeli özelliğinin cinsine, fiziksel durumuna, buharlaşma eğilimine ve özellikle bir diğer tehlikeli ekipmana göre konumunun ne olduğuna (olası domino etkileri) bağlıdır.

İlgili tehlikeli ekipmanların seçiminde kullanılan yöntem, Seveso Güvenlik Raporunun yazılmasında el kitabı olarak kullanılan ve Valon Bölgesi (Belçika – Fransa'nın güneyinde yer alan bölge) tarafından önerilen bir yöntemdir. Ekipmanların seçiminde kullanılan bu metot körü körüne uygulanmamalıdır. İçerdiği maddelerin özelliklerinden veya ekipman içinde veya dışındaki özel koşullardan dolayı tehlikeli olduğu düşünülen bir ekipman, ilgili tehlikeli bir ekipman olarak seçilebilir ve MIMAH metodolojisine göre incelenebilir.

13.4.5. Bow-Tie (Papyon) Yaklaşımı

Papyon yaklaşımı kaza senaryolarını oluşturmak için geliştirilmiş bir yöntemdir. Papyonun sol kısmı, hata ağacı olarak adlandırılır, kritik olayların muhtemel sebeplerini tanımlar. Papyon diyagramının merkezinde kritik olay (CE) bulunur. Sıvılar için kritik olay genellikle içeriğin kaybedilmesi (loss of containment – LOC) olarak tanımlanır. Katılar için veya daha özel olarak katı halde depolama için kritik olay, maddenin kimyasal veya fiziksel halinde değişikliğe yol açan fiziksel bütünlüğün kaybedilmesidir (loss of physical integrity – LPI).

Şekil 59: Papyon Yaklaşımı



İstenmeyen olaylar (UE) ve mevcut olaylar (CuE)'ın kombinasyonları birleştirildiğinde Kritik olayı tetikleyen Gerekli ve Yeterli Koşullara neden olan (NSC) Direk Sonuçlara (DC) götüren Detaylı Direk Sonuçlar (DDC)'a götürür. Papyonun sağ kısmı olay ağacı olarak adlandırılır ve kritik olayın muhtemel

sonuçlarını tanımlar. Kritik olay CE, ikincil kritik olaylara(SCE) sebep olur bu da üçüncü derecede kritik olaylara yol açar (TCE), sonuçta Tehlikeli Fenomen (DP) olarak adlandırılan olaylarla sonuçlanır. Ana olaylar(ME) olarak tanımlanan tehlikeli fenomenden dolayı hedeflerin(insanlar, yapı, çevre,…) etkilenmesini tanımlayarak sonlanır.

MIMAH'ta aşağıda sayılan 12 farklı kritik olay ele alınmıştır:

- Bozulma(CE1)
- Patlama(CE2)
- Materyallerin yer değiştirmesi (hava ile sürüklenme)(CE3)
- Materyallerin yer değiştirmesi (sıvı ile sürüklenme)(CE4)
- Yangın başlangıcı (LPI)(CE5)
- Ekipmanın cidarında buhar fazında yırtılma meydana gelmesi (CE6)
- Ekipmanın cidarında sıvı fazında yırtılma meydana gelmesi (CE7)
- İçeriğinde sıvı fazda kimyasal bulunan borusunda sızıntı (CE8)
- İçeriğinde gaz fazda kimyasal bulunan borusunda sızıntı (CE9)
- Ani Yırtılma (Felakete neden olan çatlak) (CE10)
- Ekipmanın parçalanması – Kanal çökmesi (CE11)
- Prosesin bir bölümünün veya çatının Çökmesi (CE12)

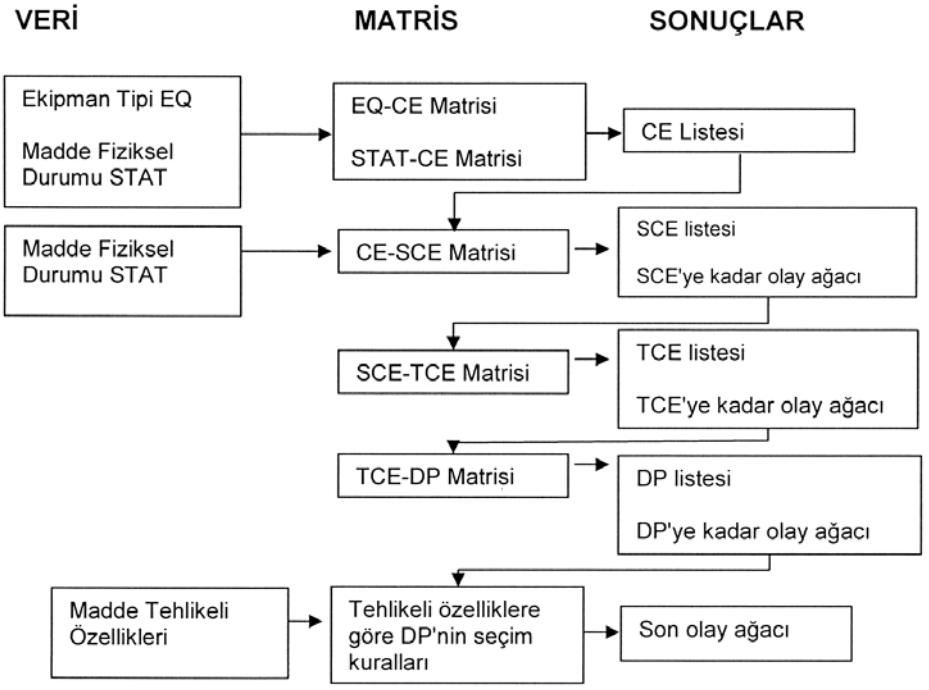
13.4.6. MIMAH Metodolojisi'nde Matrislerin Kullanımı

Birinci aşamada, matrisler verilen bir maddeyi içeren ekipmanın hangi kritik olayla ilişkisi olduğunu ve olay ağacını tanımlamak için kullanılır. **Şekil 60**'da MIMAH tarafından takip edilen adımların özeti verilmiştir.

İlk olarak; ekipman tipi(EQ) ile kritik olay(CE) arasında bağlantı var ise 'X' işareti konularak CE-EQ matrisi hazırlanır. Diğer taraftan boş hücre kritik olayın üst kolonu ile ekipman tipinin üst kolonunun ilişkilendirilemeyeceğini ifade etmektedir. İkinci matris ise, ekipman tipine göre ve muhafaza ettiği madde tipine göre her bir kritik olay(CE) için hazırlanır(STAT-CE matrisi).

İkinci aşamada; verilen ekipman ve kullanılan maddenin fiziksel durumu ile hangi kritik olayların ilişkilendirileceğine karar vermek mümkündür. Birinci sıra ekipman, ikinci sıra maddenin fiziksel durumu ve üçüncü olarak da kritik olay kombinasyonu için son sırada, 'X' işareti ile hangi kritik olayların

Şekil 60: MIMAH Tarafından Takip Edilen Adımlar



seçileceğini belirlemek maksadı ile CE'nin EQ ve STAT'la ilişkilendirilmesi matrisi hazırlanır.

Üçüncü olarak verilen bir kritik olaydan sonra hangi ikincil olayların oluşabileceğini bilmek gerekmektedir. Bu kullanılan maddenin fiziksel durumuna bağlıdır, aynı kritik olay değişik madde tiplerinde değişik ikincil olaylara yol açabilir. Kritik olayları(CE), madde durumunu (STAT) ve ikincil kritik olayları(SCE) bağlayan bir matris hazırlanır. Bazı hücrelerin tarandığı gözlenemektedir, bunun anlamı ilgilenilen kritik olay ve fiziksel durumun, uyumsuz olduğudur ve bu yüzden ikincil kritik olaylar da oluşmaz.

Dördüncü aşamada, ikincil kritik olay (SCE) ile üçüncül kritik olay (TCE) çarpılandığı bir matrisin tanımlanması gerekmektedir. SCE ; ikincil kritik olay listesi aşağıda verilmiştir;

- Yangın (SCE1)

- Yıkımsal [felaket boyutunda] kopma veya yırtık (SCE2)
- Birikim [Havuz] oluşması (SCE3)
- Tank içinde birikme (Aktarım) (SCE4)
- Gaz jeti (SCE5)
- Kabarma (SCE6)
- İki halli [fazlı] Jet (SCE7)
- Aeresol (Sis veya Sprey Şeklinde) (SCE8)
- Patlama (SCE9)
- Maddelerin hava akımı tarafından sürüklenmesi (SCE10)
- Maddelerin bir sıvı tarafından sürüklenmesi (SCE11)
- Ayrışma- Bozulma (SCE12)

TCE ; üçüncül kritik olay listesi aşağıda verilmiştir;

- Yangın (TCE1)
- Yıkımsal [felaket boyutunda] kopma veya yırtık (TCE2)
- Tank içindeki birikimin tutuşması (TCE3)
- Birikimin tutuşması (TCE4)
- Gaz yayılması (TCE5)
- Toksik ikincil ürünler (TCE6)
- Gaz jeti tutuşması (TCE7)
- Gaz kabarcığı tutuşması (TCE8)
- İki halli jetin tutuşması (TCE9)
- Aeresol jeti tutuşması (TCE10)
- Birikimin tutuşmaması / Birikimin yayılması (TCE11)
- Patlama (TCE12)
- Toz bulutu tutuşması (TCE13)
- Toz yayılması (TCE14)

DP; tehlikeli olaylar (fenomenler) listesi aşağıda verilmiştir;

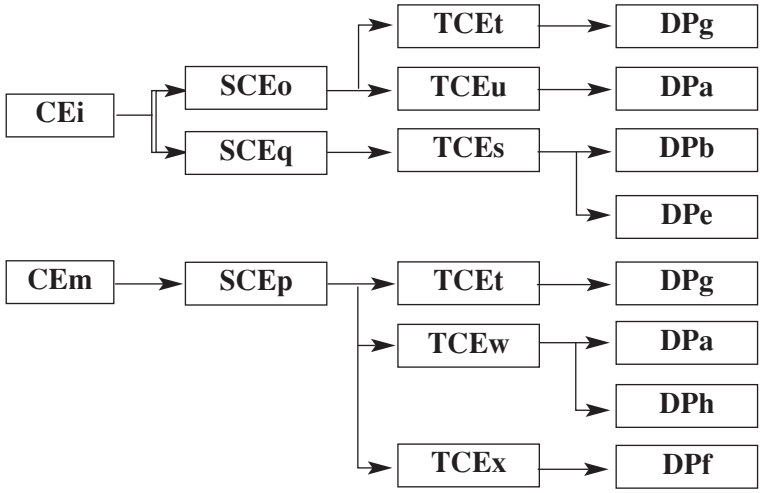
- Birikim yangını (DP1)
- Tank yangını (DP2)
- Jet yangını (DP3)
- Buhar Bulutu Patlaması – VCE (DP4)
- Ani yangın (Flashfire) (DP5)
- Toksik bulut (DP6)
- Yangın (DP7)
- Yerinden fırlama (DP8)
- Aşırı başınç artışı (patlama) (DP9)
- Ateş topu (DP10)
- Çevresel hasar (DP11)
- Toz patlaması (DP12)
- Kaynama taşması ve böylelikle oluşan birikim yangını (DP13)

Özet yapacak olursak; bir kritik olayda yer alan maddenin farklı fiziksel hallere sahip olması, birbirinden farklı ikincil kritik olay veya olayların oluşmasına sebep olabilir. Bu yüzden kritik olaylar (CE) ve maddenin fiziksel hali (STAT) ile ikincil kritik olayları (SCE) ilişkilendiren bir matris oluşturulur. Aynı şekilde, ikincil kritik olaylarla (SCE) üçüncül kritik olayları (TCE) daha sonra ise üçüncül kritik olaylarla (TCE) tehlikeli olayları (DP) eşleştiren matrisler tanımlanır. Bu eşleştirmeler, tehlikeli maddenin fiziksel halinden bağımsızdır.

13.4.7. Hata Ağacının Oluşturulması

Papyonun sol tarafı, ya da hata ağacı, kritik bir olayın mümkün olan nedenlerini tanımlar. Bu hata ağaçlarının yapılmasındaki amaç kaza senaryolarının olasılık ve şiddetini hesaplayabilmek ve meydana gelme olasılıklarını azaltabilmek için de bariyer önermeyi sağlamaktır. Bu yüzden hata ağaçları kritik olaylar ve onların oluşmasında etkisi olan yönetim ve güvenlik fonksiyon ve engellerini de içeren tüm unsurlar arasında bağlantı kurmaya elverişli olmalıdır. Bu ağaçlar olasılık değerlendirmesi için de temel sağlamalıdır. Kazaların gerçek sebepleri ve sonuçları üzerine yapılan araştırmalar geniş kapsamlı papyon

Şekil 61: Olay Ağacı Oluşturma Örneği



diyagramları ile ve aynı zamanda diğer risk analizi araçlarının (HAZOP veya bir kazanın olası sebeplerini ortaya koyan diğer sistematik risk analizi metotları; Örneğin; Proses FMEA, What If, HAZID vb..) yardımıyla yapılabilir. Özellikle HAZOP yöntemi, proses ekipmanları için olası sebeplerin tanımlanması amacıyla oluşturulan kapsamlı hata ağaçlarının oluşturulmasında en sık kullanılan ve en tamamlayıcı yöntem olarak gözükmektedir. Burada aynı zamanda tesis içerisinde yapılan diğer proses emniyeti risk analizlerinin kullanılması da mümkündür (Örn;RCM, RBI, Fonsiyonel Güvenlik vb.).

ARAMIS metodolojisinde önerilen kısmi hata ağaçları bulunmaktadır. Bu genel hata ağacları senaryo tanımlanması adımında kullanılmak için iyi bir araçtır. Amaç; analiz takımı ve operatörler, dizayn ve proses mühendisleri arasında tartışma için temel oluşturmaktadır. Ancak mutlaka kapsamlı hata ağaçları prosesteki muhtemel hatalar hakkında yapılan HAZOP metodolojisi vb. risk değerlendirmeleri yapıldıktan sonra oluşturulmalıdır.

13.5. Referans Kaza Senaryolarının Belirlenmesi Metodolojisi (MIRAS)

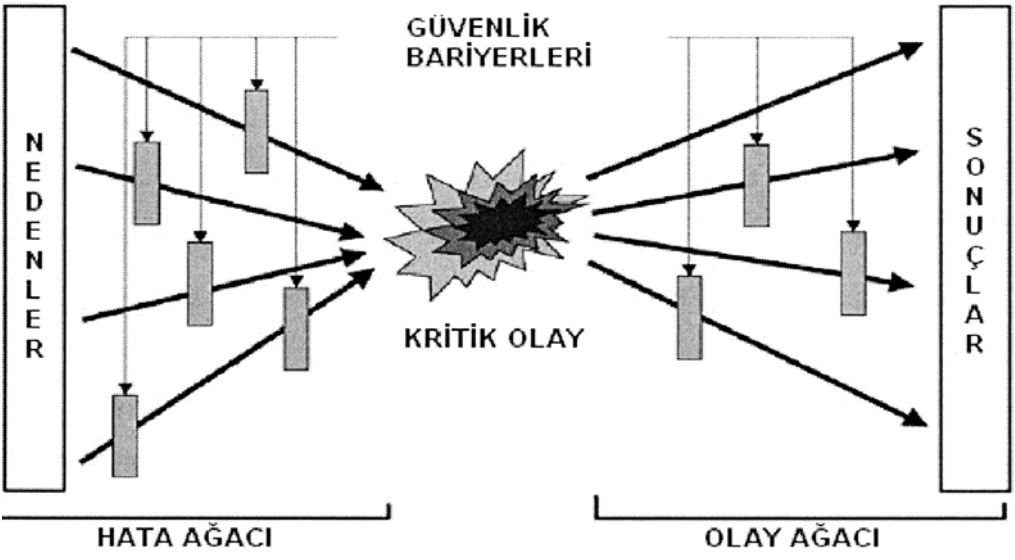
ARAMIS projesi kazanın neden ve sonuçlarını açık bir şekilde ortaya koyan papyon diyagramlarını kullanmayı önermektedir. Papyon diyagramları üzerinde tanımlanan güvenlik bariyerleri senaryoların hareketini ve büyük kazaların mey-

dana gelme frekansının nasıl azaltılabileceğini ya da kazaların etkisinin azaltılmasının nasıl sağlanacağını göstermektedir. Kaza Senaryolarının Tanımlanması Metodolojisi (MIRAS); kazalara ilişkin sebeplerin, olasılık değerlerinin ve güvenlik sistemlerinin derinlemesine incelenmesini ve büyük çaplı kazalara ait tehlikelerden daha gerçekçi senaryoların elde edilmesini sağlar. Referans kaza senaryoları (RAS), güvenlik sistemlerini de (güvenlik yönetim sistemi dahil) hesaba katarak kullanılan ekipmanlara ait gerçek tehlike potansiyellerini yansıtır, bu şekilde hazırlanan Büyük Kaza Senaryoları daha gerçekçi bir yaklaşım kazanır.

MIRAS'ın amacı MIMAH ile belirlenen büyük çaplı kazalara ait tehlikeler arasından Referans Kaza Senaryolarının (RAS) seçilmesidir. Referans senaryolar, bir tesisteki risk şiddetinin belirlenmesi için modellenmesi gereken, tesisin ve çevresinin maruziyet düzeyi ile karşılaştırılabilecek senaryolardır. Bu referans kaza senaryolarını tanımlayabilmek için MIRAS metodolojisi şunları hesaba katar:

- Ekipman üzerinde veya çevresinde kurulu güvenlik sistemleri,
- Güvenlik yönetim sistemi,

Şekil 62: Papyon Diyagramı ve Bariyerlerin Güvenilirliği



- Kazanın meydana gelme frekansı,
- Kazanın potansiyel olası sonuçları.

13.5.1. MIRAS'ın Amaçları ve Temel Adımları

Referans senaryolar, bir tesisteki risk şiddetinin belirlenmesi için modellenmesi gereken, tesisin ve çevresinin maruziyet düzeyi ile karşılaştırılabilecek senaryolardır. Bu amaca 8 adımda ulaşılır. MIMAH ile oluşturulan her bir papyon diyagramı için tüm adımlar uygulanmalıdır.

MIRAS Adım 1: Gereken Verileri Topla

MIRAS'ın uygulanması için MIMAH kısmında toplanan verilere başka veriler de eklenmelidir. Bu verilerden bazıları örneğin başlangıç olaylarının frekans/olasılık değerleri, incelenen ekipmana ait güvenlik sistemleri ve güvenlik prosedürleri, güvenlik bariyerlerinin performansının değerlendirilmesi ile ilgili bilgiler, tutuşma olasılıkları vb. olarak sayılabilir.

MIRAS Adım 2: Adım 3 veya Adım4'ten Birini Seç

Adım 3 ve Adım4 aynı şeyi amaçlamaktadır: ele alınan papyon diyagramındaki kritik olay için yıllık frekans değerlerinin tahmin edilmesi. Yapılacak ilk seçim, kritik olayın frekansını belirlemek için kullanılan güvenlik bariyerlerinin etkilerini de dikkate alarak hata ağaçlarının tümüyle analiz edilmesidir (Adım 3). Buna alternatif olabilecek diğer bir yöntem kritik olayın frekansının doğrudan doğruya tahmin edilmesidir (Adım 4).

İlk yöntem eğer kullanılabilir veriler mevcutsa tercih edilmelidir. Bu metot biraz daha fazla zaman alıyor olsa bile kritik olaydan (papyon diyagramının sol tarafında yer alan kısım) korunabilmek için uygulanan ilgili güvenlik sistemlerinin incelenmesine imkan sağlar. İkinci yöntemde tesisin korunma derecesi dikkate alınmaz fakat analiz için harcanan zaman daha kısadır.

MIRAS Adım 3: Hata Ağacını Analiz Ederek Kritik Olayın Frekansını Hesapla

Eğer bu yöntem seçilirse dört adım takip edilmelidir. İlk olarak tetikleyici olaylara ait frekanslar (hata ağacının sol alt kısmı) değerlendirilmelidir. İkinci olarak hata ağacındaki olayları etkileyen güvenlik bariyerleri (kontrol önlemleri) tanımlanmalıdır. Daha sonra bu güvenlik bariyerlerinin performansı değerlendirilmeli ve son olarak tüm bu parametreler, kritik olayın frekansının belirlenmesinde dikkate alınmalıdır.

Tablo 62: Başlatıcı Olay Frekanslarının Kalitatif Tanımları

YILLIK GERÇEKLEŞME FREKANSLARI		SINIF
Kalitatif Tanım	**Kantitatif Tanım**	**Sıralama**
Çok düşük sıklık(gerçekleşmesi zor)	$F \leq 10^{-4}$ /yıl	F_4
Düşük sıklık(1000 yılda bir)	10^{-4} /yıl < $F \leq 10^{-3}$ /yıl	F_3
Düşük sıklık (100 yılda bir)	10^{-3} /yıl < $F \leq 10^{-2}$ /yıl	F_2
Mümkün-yüksek sıklık (10 yılda bir)	10^{-2} /yıl < $F \leq 10^{-1}$ /yıl	F_1
Oluşması muhtemel- çok yüksek sıklık (sahada birçok kez yaşanmış)	$F \geq 10^{-1}$/yıl	F_0

MIRAS Adım 3A: Tetikleyici Olay Frekanslarını (veya olasılıklarını) Tahmin Et

Bu adımın amacı, kritik olayın meydana gelmesine sebep olan hata ağacındaki her bir dalın ilk sebepleri niteliğinde olan tetikleyici olay frekanslarının elde edilmesidir. ARAMIS, tetikleyici olayların frekanslarına ait kullanılabilir verilerin genel taslağını vermektedir. Bununla ilgili tam veriler ve açıklamalar ARAMIS metodolojisinin internet sayfasından bulunabilir. Ancak verilerle ilgili bazı noktaları vurgulamak gerekmektedir:

- Bu alanda kesinlikle bir veri yetersizliği mevcuttur. Yayınlanan verilerin sentezinden elde edilen sonuçlar, farklı türdeki tetikleyici olayların frekanslarına ait verilerin miktarında ve elde edilen verilerde büyük bir çelişki olduğunu göstermiştir.
- Eğer mümkünse ve kullanılabilir veriler mevcutsa tesise özgü verilerin kullanılması tavsiye edilebilir veya en azından tetikleyici olay frekansları fabrika çalışanları ile birlikte Tablo 62'de verilen kalitatif frekans aralıklarından yararlanılarak tahmin edilmeye çalışılmadır.

MIRAS Adım 3B: Güvenlik Fonksiyonlarını ve Güvenlik Bariyerlerini Hata Ağacı Üzerinde Tanımla

Hata ağacındaki her bir olayın tüm dalları derinlemesine incelenmeli ve şu soru sorulmalıdır: "Bu olaydan korunmayı ve sakınmayı sağlayan veya bu olayı

kontrol eden herhangi bir güvenlik bariyeri mevcut mu?" Eğer verilen cevap evetse bu güvenlik bariyeri bu dal üzerine yerleştirilmelidir. Bariyer eğer bu olaydan sakınmayı veya korunmayı sağlıyorsa bu daldan olaya doğru yukarı yönde yerleştirilmelidir. Bu tanımlamalar endüstriyel kuruluşlarda çalışanların yardımı alınarak ve proses ve enstrümantasyon diyagramarı veya akış diyagramları kullanılarak yapılmalıdır. ARAMIS metodolojisi; papyon diyagramında yer alan tüm olaylar için güvenlik fonksiyonları ve güvenlik bariyerlerine ait bir kontrol listesi önermektedir.

MIRAS Adım 3C: Güvenlik Bariyerlerinin Performansının Değerlendirilmesi

Güvenlik bariyerleri tanımlandıktan ve hata ağacı üzerine yerleştirildikten sonra bu bariyerlerin kritik olay frekansı üzerindeki etkilerini değerlendirmek gerekir. İlk olarak, kritik olayla ilgili olduğu düşünülen bir bariyerin bazı minimum gereksinimleri karşılaması gerektiğini vurgulamak gerekir. Bir bariyer bir kritik olayla ilişkilendirildiğinde, bariyerin performansı şu 3 parametreye göre belirlenir:

- Talep anında hata olasılığı (PFD) ile ilgili olan güvenlik seviyesi (LC),
- İstenilen derecede koruma sağlayabilecek olan kapasitesi (spesifik boyutlar veya hacim, fiziksel güç v.b.) veya etkinlik değeri (E),
- ve bariyerin cevap verebilme süresi (RT).

Birinci adımda, belirlenen güvenlik derecesi, "tasarım" güvenlik seviyesidir. Bu bir bariyerin, kurulduğunda, aynı cevap verebilme süresine sahip olma ve aynı güvenlik derecesini sağlayabilme açısından etkin olabileceğinin varsayılmasıdır. Fakat güvenlik bariyerinin performansı başlangıçtan itibaren hayat döngüsü içersinde düşüş gösterebilir. Bunun birden fazla sebebi vardır: kötü bakım programı, operatörlerin bilgilerini zamanla yitirmeleri, bazı ekipmanların engel teşkil etmesi vb… Tüm bu sebepler güvenlik yönetim sisteminin kalitesiyle ilişkilendirilebilir.

İkinci adımda bu yüzden güvenlik yönetim sisteminin performansının ve bu sistemin güvenlik bariyerlerinin performansı üzerindeki etkilerinin değerlendirilmesi gerekmektedir.

MIRAS Adım 3D: Kritik Olayın Frekansını Hesapla

Tetikleyici olaylara ait karakteristik özelliklerin değerlendirilmesinden, güvenlik bariyerlerinin tanımlanıp performanslarının belirlenmesinden sonra bu

bölümde ilgili kritik olayın frekansının hesaplanabilmesi için hata ağacının analiz edilmesi gerekmektedir. Örneğin; temel üç bariyeri açıklayacak olursak;

- "Kaçınma" bariyerleri daha alt kademelerde yer alan olayın imkansız olaylar olduğunu göstermektedir. Bu yüzden bu bariyere karşılık gelen hata ağacının dalı kritik olayın frekansını artık hiçbir şekilde etkilemeyecektir.
- "Kontrol" ve "Korunma" bariyerleri için şu kural geçerlidir: "Eğer bir dalda yer alan güvenlik bariyerinin güvenlik seviyesi n ise bir alt kademede yer alan olayın frekansı 10 n kadar azalır."

Hata ağacındaki çeşitli olayların frekansları ve kritik olayın frekansı, güvenlik bariyerlerinin hesaba katılması ile bu şekilde hesaplanabilir.

MIRAS Adım 4: Kritik Olay Frekansını Kapsamlı Kritik Olay Frekanslarından Yararlanarak Tahmin Et

Eğer kritik olayın frekansı, hata ağacının analizi esas alınarak hesaplanamıyorsa (Adım 3), kullanılabilecek diğer bir yöntem bu frekansın geniş kapsamlı kritik olay frekanslarından yararlanılarak tahmin edilmesidir. MIRAS, toplanan verilerin özetlenmesi ve ele alınan ekipmanın cinsine bağlı olarak değişen çeşitli kritik olay frekansları için belirlenen değerleri veya değer aralıklarını gösteren bir tablo oluşturulmasını önermektedir. Frekans değerlerinin aralıkları belirlendiğinde, bu aralıkta, eğer güvelik seviyesi düşükse nispeten daha yüksek bir değer, eğer yüksekse nispeten daha düşük bir değer seçilmelidir. Literatürde yer alan bilgiler bu değerlerin daha kesin bir şekilde belirlenebilmesi için daha açık bir yöntem önermemektedirler.

MIRAS Adım 5: Tehlikeli Olgulara (DP) Ait Frekansları Belirle

Bu bölümde amaç, olay ağacında adım adım ilerleyerek her bir tehlikeli olguya ait frekansların elde edilmesidir. İlk olarak ağaçtaki geçiş olasılıkları tartışılacak ve olay ağacı tarafındaki güvenlik bariyerleri tehlikeli olguların olası sonuçlarına ve frekanslarına olan etkilerini değerlendirebilmek adına dikkate alınacaktır.

13.5.2. Olay Ağaçlarında Geçiş Olasılıklarının Değerlendirilmesi

Olay ağaçlarında iki seçenekli birçok seçim aşamasının şartlı olasılık terimleri cinsinden ifade edilmesi gerekmektedir: örneğin ani bir tutuşma olayı olabilir mi? Eğer böyle bir olasılık yoksa gecikmeli tutuşma meydana gelebilir mi? Bir buhar bulutunun gecikmeli olarak tutuşması durumunda bu olay bir buhar

bulutu patlamasıyla mı (VCE) yoksa aniden parlayan bir yangınla mı sona erecektir?

Tutuşma ve VCE olasılıkları birçok parametreye bağlı iken (örneğin maddenin yanabilirliği, yangın kaynağı, tutuşturma kaynaklarının cinsi ve ortamdaki varlığı, meteorolojik şartlar ve bölgenin engelleme durumu…) bu parametreler ve bu olasılık değerleri endüstriyel uzmanlarla yerinde tartışılmalıdır. Analistlere yardımcı olabilmek için ARAMIS, olasılıklara ait bazı makul değerler önermektedir.

13.5.3. Olay Ağacındaki Güvenlik Bariyerlerinin Etkileri

Bu bölümdeki amaç ilk olarak olay ağacındaki güvenlik bariyerlerinin tanımlanması daha sonra bu bariyerlerin etkilerinin sayısal hale getirilmesidir. Güvenlik bariyerlerinin tanımlanmasında kullanılan metot, hata ağacındaki güvenlik bariyerlerinin tanımlanmasında kullanılan metotla aynıdır: olay ağacının sistematik olarak gözden geçirilmesi. Ağaçta yer alan her bir olaya ait tüm dallar incelenmeli ve şu soru sorulmalıdır: "Bu olaydan sakınmayı, korunmayı sağlayan ya da bu olayı kontrol eden bir güvenlik bariyeri var mı?" Eğer cevap evetse güvenlik bariyeri o dal üzerine yerleştirilmelidir. Bariyer eğer bir olaydan korunmayı sağlıyorsa genellikle bu olayın bir üst kademesine yerleştirilir. Eğer bu olayı kontrol altına alıyor ya da sınırlandırıyorsa bir alt kademeye yerleştirilmesi gerekir. Bu tanımlamalar endüstriyel kuruluşlarda çalışanların yardımı alınarak ve proses ve enstrümantasyon diyagramarı veya akış diyagramları vb. diyagramlar kullanılarak yapılabilir.

Daha sonra tanımlanan güvenlik bariyerlerinin performansının değerlendirilmesi yapılmalıdır. Bu prosedür hata ağaçlarındaki bariyerlerin performanslarının değerlendirilmesi prosedürü ile aynıdır. Kritik olayla ilişkili olduğu düşünülen bir bariyer, bazı minimum gereksinimleri karşılamak zorundadır. Ayrıca "Tasarım" güvenlik seviyesi, etkinlik değeri ve cevap verebilme süresi de değerlendirilmelidir.

MIRAS Adım 6: Tehlikeli Olgunun Olası Sonuçlarını Sınıflandır

Seçilen senaryolarda tanımlanan güvenlik fonksiyonlarının her birini yerine getirmek için kuruluşun yaptığı seçimlerin niteliğinin bir değerlendirmesini içerir. Başka bir deyişle, kuruluşa özgü tehlikeleri kontrol etmede en son tekniklerin kullanılıp kullanılmadığı değerlendirilir. İşte tam bu aşamada fabrikanın ALARP seviyesi belirlenmiş olur.

Tehlikeli olgulara ait kalitatif değerlendirmeler **Tablo 63**'de tanımlanan sonuçlara bağlı olarak belirlenen 4 sınıfa göre yapılır. Bu sınıflar, domino etkileri açısından meydana gelebilecek potansiyel sonuçlara ve insanlar ve çevre üzerindeki etkilerine göre belirlenmiştir.

13.5.4. Risk Şiddeti Değerlendirmesi ve Haritalandırması

Referans kaza senaryolarının (RAS) her biri, birbirinden farklı tehlikeli olgulara yol açabilecek olan tetikleyici olaylar yardımıyla tanımlantır. Her bir tehlikeli olgu için her bir tehlikeye özgü şiddet indeksi tanımlanır. Burada amaç herhangi bir tehlikeli etkinin 0-100 arasında değerler alan tek bir ölçek yardımıyla şiddetlerinin karşılaştırılması ve ölçülmesidir. Bu ölçüm birbirinden çok farklı yapı-

Tablo 63: Sonuç Kategorisi (ALARP)

Sonuç Frekansı (/yıl)	Sonuç Kategorileri			
	C1	C2	C3	C4
$10^{-1} – 10^{-2}$				
$10^{-2} – 10^{-3}$				
$10^{-3} – 10^{-4}$				
$10^{-4} – 10^{-5}$				
$10^{-5} – 10^{-6}$				
$10^{-6} – 10^{-7}$				
$10^{-7} – 10^{-8}$				

Kabul Edilemez

Kabul Edilebilir

daki risklerin karşılaştırılmasına imkan sağlar. Tehlikeli olguya bağlı olarak ele alınan olgunun farklı genlikteki değerleri için birbirinden farklı şiddet seviyeleri belirlenmiştir.

ARAMIS ile genel kantitatif risk değerlendirme metotları arasındaki temel farklardan birisi maruziyet ve şiddet değerlerinin potansiyel kaza senaryolarından ayrı olarak incelenmesidir. Bu bağlamda, şiddeti ölçümlemek için herhangi bir

olasılık fonksiyonunun kullanılması mümkün değildir fakat yoğunluğun karakterize edilebilmesi için eşik şiddet değerlerinin tanımlanması gerekmektedir.

13.6. Maruziyetlerin Değerlendirilmesi

ARAMIS'in yeniliklerinden birisi de maruziyet değerlerinin tehlike bölgesinden bağımsız olarak belirlenmesine imkan vermesidir. Bu, yerel otoritelere, operatörün yalnızca kurulumun potansiyel tehlikesi üzerinde faaliyet gösterebildiği maruziyeti azaltarak global risk düzeyini azaltmak için etkin kararlar alma imkanını taşıdığı için temel olarak ilgi görmektedir.

Maruziyet düzeyleri, çok kriterli karar – yardım yöntemleri esas alınarak hesaplanır. Risk bilgisi taşıyan kararlara yerel popülasyonun da dahil edildiği yeni yönetim şekillerinin gelişmesiyle, bu yöntem, maruziyet değerlendirmesi çalışmasını hissedarların uzmanların değerlendirmeleri ile oluşan risk algıları üzerine kurmuştur. Bu yüzden fabrika ve çevresinin herhangi bir noktasındaki maruziyet düzeyi o noktada bulunan potansiyel hedef sayısına ve bu hedeflerin farklı olgulara karşı rölatif maruziyet değerlerine göre karakterize edilir. Global maruziyet düzeyi ise her bir hedefin maruziyet düzeylerinin doğrusal kombinasyonundan oluşmaktadır.

KAYNAKÇA

1. Özkılıç, Ö., İş Sağlığı ve Güvenliği Yönetim Sistemleri ve Risk Değerlendirme Metodolojileri, TİSK, Ankara, Mart, 2005
2. Özkılıç, Ö., Risk Değerlendirmesi Kavramı ve İnsan Hatalarını Önleme Metodlarına Genel Bakış, İş Müfettişleri Dergisi, Ankara, Haziran, 2005
3. Özkılıç, Ö., Risk Değerlendirmesi Kavramı, TİSK, İşveren Dergisi, Ankara, Haziran, 2005
4. Özkılıç, Ö., İş Sağlığı, Güvenliği ve Çevresel Etki Risk Değerlendirmesi; MESS, İstanbul, 2007
5. Özkılıç, Ö., Büyük Endüstriyel Kazaları Önleme Çalışmalarında Kritik Sistemlerin Tespiti Ve Risk Değerlendirme Yaklaşım ve Yöntemleri, V. ISG Kongresi, İstanbul, 2008
6. Özkılıç, Ö., ATEX Direktifleri Çerçevesinde Patlayıcı Ortam Sınıflandırma ve Patlayıcı Ortam Risk Değerlendirmesi, Sempozyum Tebliğleri Kitabı, Çimento Sektöründe İş Sağlığı ve Güvenliği Sempozyumu, İzmir, Kasım 2008
7. Özkılıç,Ö.,"Yeni İş Sağlığı ve Güvenliği Mevzuatı Çerçevesinde Risk Değerlendirmesi", İş Güvenliği Dergisi, İSGİAD, 29 (3) 10-14, 2008
8. HSE (1993) Draft offshore installations (fire and explosion, and emergency response) regulations and approved code of practice. Consultative Document 64, Health and Safety Executive, Sheffield, UK
9. HSE (1993). Draft Offshore Installations (Fire and Explosion, and Emergency Response) Regulations and Approved Code of Practice, Consultative Document 64, Health and Safety Executive, Sheffield, UK
10. Hungerbühler K., Shah S., Visentin F., Fischer U. (2004) A Top to Bottom Approach for Assessment of Safety, Health and Environmental Aspects in Early Development Stages of A Chemical Process, Institute of Chemical and Bioengineering Swiss Federal Institute of Technology (ETH), CH-8093 Zurich, Switzerland
11. Rostamzadeh B., Lönn H., Snedsbøl R., Torin J., (1999) A Distributed Computer Architecture for Safety-Critical Control Applications, New York, DACAPO

12. Sommerville I. (2004) Software Engeneering 7th Edition Capter 3, London, Addison Wesley Longman
13. MIL-STD-882-D Standard Practice For System Safety, 2000
14. ISO/IEC GUIDE 51 Safety aspects - Guidelines for their inclusion in standards
15. ISO GUIDE 73 Risk management - Vocabulary
16. ISO/IEC GUIDE 98-3 Supplement 2 - Uncertainty of measurement -- Part 3: Guide to the expression of uncertainty in measurement (GUM:1995) - Extension to any number of output quantities
17. ISO 31000:2009 Risk management -- Principles and guidelines
18. IEC 31010:2009 Risk management -- Risk assessment techniques
19. ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements
20. ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls
21. ISO 12100:2010 Safety of machinery -- General principles for design -- Risk assessment and risk reduction
22. IEC 62198 Project risk management-Application guide
23. EN 61508-7 Functional safety of electrical/electronic/programmable electronic safety-related systems -Part 7: Overview of techniques and measures
24. IEC 61882:2001Hazard and operability studies (HAZOP studies). Application guide
25. EN 61511-1:2004 Functional safety. Safety instrumented systems for the process industry sectorFramework, definitions, system, hardware and software requirements
26. IEC 62198:2001 Project risk management. Application guidelines
27. EN 61165:2006 Application of Markov techniques
28. EN 60300-3-11:2009 Dependability managementApplication guide. Reliability centred maintenance
29. EN 61025:2007 Fault tree analysis (FTA)
30. EN 50014:1998 Electrical apparatus for potentially explosive atmospheres. General requirements

31. EN 60812:2006 Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA)
32. EN 61649:2008 Weibull analysis
33. EN 61078:2006 Analysis techniques for dependability. Reliability block diagram and Boolean methods
34. EN 62551:2012 Analysis techniques for dependability. Petri net techniques
35. EN 60079-10-1:2009 Explosive atmospheresClassification of areas. Explosive gas atmospheres
36. EN 60079-10-2:2009 Explosive atmospheresClassification of areas. Combustible dust atmospheres
37. ISO 9001:2008 Quality management systems – Requirements, Edition: 4th, International Organization for Standardization
38. ISO 14001:2004 Environmental Management Systems - Specifications with Guidance for Use
39. OHSAS18001:2007 Occupational health and safety management systems. Requirements
40. IEC 61882 {Ed.1.0} Hazard and operability studies (HAZOP studies) - Application guide
41. Maintenance cycle report on IEC 61882 Ed. 1.0: Hazard and operability studies (HAZOP studies) - Application guide
42. IEC 61882, Ed.1: Hazard and operability (HAZOP) studies - Guide word approach
43. IEC 61882: Guide for Hazard and Operability Studies (HAZOP studies)
44. IEC 61882, Ed. 1: Hazard and operability studies (Hazop studies) - Application guide
45. Maintenance of IEC 61882 - Hazard and Operability Studies (HAZOP studies) - Application Guide (2001-05)
46. Maintenance cycle report on IEC 61882 Ed.1: Hazard and operability studies (HAZOP studies) - Application guide
47. International Labor Office, Major Hazard Control – A Practice Manuel, Geneva, 1991
48. Delvosalle C, Fievez C, Pipart A, Debray B., ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios

in process industries., Faculté Polytechnique de Mons, Major Risk Research Centre, 56 rue de l'épargne, 7000 Mons, Belgium

49. API Publication 581 – Risk Based inspection, Base Resource Document – 1st edition 2000
50. API Publication 580 – Recommended Practice for Risk Based inspection– 1st edition 2002
51. HSE, Best Practice for Risk Based Inspection as a part of Plant Integrity Management, Contract Research Report 363/2001
52. Ramesh J. P., Risk Based Inspection, Middle East Nondestructive Testing Conference & Exhibition - 27-30 Nov 2005 Bahrain, Manama
53. Andrews, J., Moss, B. (2002) Reliability and Risk Assessment, London, John Wiley & Sons; 2nd Edition
54. ALLAN, McMilan, Industrial Health and Safety, Butterworth-Heinemann,1998, 4th Edition
55. MOLAK, Vlasta, Fundamentals of Risk Analysis and Risk Management, GAIA UNLIMITED Inc.,Cincinnati, Ohio, 2005, 9 th Edition
56. Williams C.A. Jr., Smith M.L., Young P.C., Risk Management and Insurance, McGraw-Hill Book Company, 1995,7th Edition
57. Parker C.P., Risk Analysis and Management, McGraw-Hill Book Company, 1998, 6th Edition
58. AS/NZS 4804 (2001) Occupational Health and Safety Management Systems — General Guidelines on Principles, Systems and Supporting Techniques
59. AS/NZS 4360 (1999) Risk Management to Managing Occupational Health and Safety Risks
60. Shappell, S. & Wiegmann, D. (2001). Applying Reason: The Human Factors Analysis and Classification System (HFACS). Human Factors and Aerospace Safety, 1, 59-86
61. Shappell, S. & Wiegmann, D. (2000a). The Human Factors Analysis and Classification System (HFACS). (Report Number DOT/FAA/AM-00/7). Washington DC: Federal Aviation Administration

62. Shappell, S. & Wiegmann, D. (1997b). A reliability analysis of the Taxonomy of Unsafe Operations (Abstract). Aviation, Space, and Environmental Medicine, 69, pp. 620

63. Instrument Society of America (ISA), "Application of Safety Instrument Systems for the Process Industries," ISA-ANSI Standard S84.01-1996, Instrument Society of America, Research Triangle Park, North Carolina, (1996)

64. US. Occupational Safety & Health Administration (OSHA). "Process Safety Management of Highly Hazardous Materials,", US OSHA Standard 29 CFR 1910.119, Washington, DC, Federal Register, 57 23060 (June 1992) 61, 9227 (March 7, 1996)

65. Kjellen U & Larsson TJ, (1980), Investigating Accidents and Reducing Risks – A Dynamic Approach, Journal of Occupational Accidents v3 pp:129-140, Amsterdam, Scientific Publishing Company

66. Knox NW and Eider EW, (1983), MORT User;s Manual for use with the Management Oversight and Risk Tree Analytical Logic Diagram, DOE 76/45-4, SSDC-4 (rev 2), GG & G Idaho

67. Livingston A D and Green M (1992). Evaluation of Incident Investigation Techniques and Associated Organisational Issues. 7th International Symposium on Loss Prevention and Safety Promotion in The Process Industries. Taormina, Italy

68. Paradies M, Unger L and Ramey-Smith A, (1992), Development and Testing of the NRC's Human Performance Investigation Process (HPIP), in International Conference on Hazard Identification and Risk Analysis, Human Factors and Human Reliability in Process Safety, Jan 15 - 17, Marriott Hotel (Airport), Orlando Florida, New York: American Institute of Chemical Engineers

69. Pate-Cornell ME, (1992), Learning from the Piper Alpha Accident: A Postmortem Analysis of Technical and Organisational Factors, Risk Analysis v13n2 pp:215-232

70. Armstrong, ME, Cecil, WL and Taylor, K, (1988), Root Cause Analysis Handbook DPSTOM - 81, EI du Pont de Nemours & Co, Savannah River Laboratory, Aiken SC29808

71. Layer of Protection Analysis, Simplified Process Risk Assessment, Centre for Chemical Process Safety, American Institute of Chemical Engineers, 2001
72. Kevin Corker , Human Factors & Reliability, San Jose State University ISE 222 Spring 2005
73. Risk-informed Approach to System Performance and Safety": Dr. Robert A. Bari Presented at NASA HQ. February 2, 2007
74. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, New Version 1.1 of November 12, 2002
75. "Fault Tree Handbook with Aerospace Applications',Version 1.1, NASA Publication, August 2002
76. Report of Voting on 56/1072/FDIS: IEC 60812 Ed. 2.0: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
77. Maintenance cycle report IEC 60812, Ed.2: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
78. Compilation of comments on 56/735/CD: IEC 60812: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
79. Compilation of comments on 56/797/CD: IEC 60812, Ed.2: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
80. Result of voting on 56/921/CDV: IEC 60812: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
81. Aydın, A.O. ve M. Kurt (2002) "Bilişim Ergonomisi", Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi,. 17(4) 93-115.
82. Büyük Endüstriyel Kazaların Önlenmesi, ILO Uygulama Kodu, Ankara-1991
83. Büyük Larousse Sözlük ve Ansiklopedisi 22.Cilt (1998) Milliyet Gazetecilik A.Ş., İstanbul
84. Coburn, A., Spence, R. (1992) Earthquake Protection, London, Wiley
85. Duru, S., Besbelli, N. (1997) Risk Değerlendirilmesi, Uluslararası Katılımlı 1. Ulusal Çevre Hekimliği Kongresi, Ankara, 19 (3) 95-99.

86. Finn, J. D. (1972) Instructional Technology, AECT, University of Southern California

87. Fitzpatrick, M., Bonnefoy, X. (1999) Guidance on the Development of Educatioal and Training Curricula. Environmental Health Services in Europe-4, Copenhagen: WHO Regional Publications, Euopean Series, No:84

88. Gigliotti, R., Jason, R. (1991) Emergency Planning for Maximum Protection -1st Edition, Boston, Butterworth-Heinemann

89. http://www.who.int

90. http://www.ilo.org

91. ISO/IEC Guide 51 (1999) Safety aspects -- Guidelines for their inclusion in standards

92. ISO/IEC Guide 73 (2002) Risk management - Vocabulary - Guidelines for use in standards

93. Prof. Hermann Knoflacher, Quantitative Risk Analysis Model for Transport of Dangerous Goods through Tunnels, Joint Project of OECD and PIARC Technical University, Vienna 2005

94. NRI MORT User's Manual, For use with the Management Oversight and Risk Tree analytical logic diagram, NRI-1 (2002), The Noordwijk Risk Initiative Foundation and Marathon Oil UK.

95. Mahmoud Shahrokhi, Alain Bernard, Energy Flow /Barrier Analysis, A Novel View, IRCCyN laboratory - Ecole Centrale de Nantes, 2003

96. European Organisation For The Safety Of Air Navigation, Review Of Techniques To Support The Eatmp Safety Assessment Methodology, EEC Note No. 01/04, Volume II – Annex, January 2004

97. Dino G. DiMattia, Faisal I. Khan and Paul R. Amyotte, Determination Of Human Error Probabilities For Offshore Platform Musters, 1Department of Chemical Engineering, Dalhousie University, Halifax, Nova Scotia, Canada B3J 2X4, 2005

98. B. Koutsky, Methodology of risk assessment used in an industrial case study, Institute of Chemical Technology, Prague, Czech Republic, November, 2006

99. B. Nedumaran, INDUSTRIAL SAFETY AND RISK MANAGEMENT, Department of Chemical Engineering, Sri Venkateswara College of Engineering Sriperumbudur, India, October 8, 2004
100. Bilal M. Ayyub, PhD, PE, Fault Tree Analysis (FTA), US Army Corps of Engineers, Technical Report for Contracts DACA31-96-D-0063, November 1998
101. Douglas A. Wiegmann, A Human Error Analysis of Commercial Aviation Accidents Using the Human Factors Analysis and Classification System (HFACS), Oklahoma City, February 2001
102. HAZOP Studies, Ministry of Defence Defence Standard 00-58 Issue 2 Publication Date 19 May 2000
103. ISA Technical Paper 6015, The Enhanced Approach to Process Hazard Analysis and Safety Instrument System Design
104. Wolfram Braasch, Risk Assessment, The Third International Conference on Quality Management, 2001
105. UK Health & Safety Commission. Approved Code of Practice -- Management of Health and Safety at Work Regulations 1992.
106. Kutay F. (1999) "Kalite Kontrol Ders Notları" Gazi Ünv. Müh. Mim. Fak., End. Müh., Ankara
107. Morgan, M. G. (1993), "Risk Analysis and Managment", Science journal, 1(1) 18-23.
108. Okuyama, S.E., Chang, E. (2004) Modeling Spatial Economic Impacts of Disasters, Berlin, SpringerVerlag
109. OHSAS 18001 (1999) İş Sağlığı ve İş Güvenliği Yönetim Sistemi – Spesifikasyonu, BSI
110. OHSAS 18001 (2007) Occupational health and safety management systems – Requirement, BSI
111. Riley, J.E., Cayless, S.M., Raw, G.J., J.E.Cheyne, A.J.T. ve Cox, S.J., (1997) Refinement of a Risk Assesment Procedure: Rating of Hazards, Healthy Buildings/IAQμ97 Global Issues and Regional Solutions Proceedings, Washington
112. Türkçe Sözlük (1992), Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, Milliyet Gazetecilik A.Ş., İstanbul

113. WHO The World Health Report (2002) Reducing risks, Promoting Healthy Life, France
114. Senge, Peter (1991). Beşinci Disiplin: Öğrenen Organizasyon Düşünüşü ve Uygulanışı. Çev. Ayşegül İldeniz, Ahmet Doğukan. İstanbul: Yapı Kredi Yayınları.
115. Senge, Peter (1996). "Rethinking Leadership in the Learning Organization", The Systems Thinker Newsletter, cilt 7, sayı 1
116. Dr. Tunç EVCİMEN, ÖĞRENEN ORGANİZASYONLAR, Yatay İlişkilerde Otorite ve Sorumluluk,
117. Araş. Gör. Seçil Bal TAŞTAN, ÖĞRENEN ORGANİZASYONLAR, Human Resources,2008
118. Özkan, T. ve Lajunen, T. (2003). Güvenlik kültürü ve iklimi. PiVOLKA, 2(10), 3-4.
119. Federal Aviation Authorities, "System Safety Handbook", Southern California Safety Institute, ABD, 3-17, 15-6,7,9,10,11, A-4,8,9,11,13, G-2,3 (2000).
120. Lay, R. and Strasser, G. 1987. Risk Management of Complex, Technology-Based Systems: Observations on Similarities and Differences, Lave, L. B., Plenum Press 179-188.
121. Brehmer, B. 1994. The Psychology of Risk, Singleton, W. T. and Hovden, J., John Willey & Sons, West Sussex.
122. Kerzner, R, H. 1998. Project Management: A Systems Approach to Planning, Scheduling and Controlling", John Willey & Sons, Canada, 87-88.
123. H. BAŞAK, M. GÜLEN, 2007. İnsansız Hava Aracı Kazalarının Önlenmesi İçin Risk Ölçümü ve Yönetimi Modeli, Pamukkale Üniversitesi Mühendislik Fakültesi Mühendislik Bilimleri Dergisi, 55-65.
124. Fıkırkoca, M., "Bütünsel Risk Yönetimi", 1.Basım, Pozitif Matbaacılık, Ankara, 13-35, 44, 48, 140,143,147, 152, 192, 205, 389-427 (2003).
125. MSC (Maritime Safety Committee). (2002). Guidelines For Formal Safety Assessment (FSA) For Use In The Imo Rule-Making Process. MSC/Circ. 1023.
126. Occupational Health And Safety Risk Management Handbook, Draft For Review, July 2002

127. Robert C. Menson, PhD, Risk Assessment Tools for Identifying Hazards and Evaluating Risks Associated with IVD Assays AACC Expert Access Live on Line, 06 July 2004
128. Bob Roberts, Risk & Reliability Engineer, San Diego, Feruaryb 2006
129. Hazard And Barrier Analysis Guidance Document, Office Of Operating Experience Analysis And Feedback, EH-33, November, 1996
130. Erik Hollnagel, IFE (N), Accident Analysis And Barrier Functions, Version 1.0, February 1999
131. Daniela Karin Busse, Cognitive Error Analysis in Accident and Incident Investigation in Safety-Critical Domains Department of Computing Science, University of Glasgow, September 2002
132. U. YILMAZ, 2005. Havacılıkta Risk Yönetimi ve Sivil Hava Taşımacılığında Risk Sahalarının İncelenmesi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara
133. Senge, Peter (1991). Beşinci Disiplin: Öğrenen Organizasyon Düşünüşü ve Uygulanışı. Çev. Ayşegül İldeniz, Ahmet Doğukan. İstanbul: Yapı Kredi Yayınları
134. Senge, Peter (1996). "Rethinking Leadership in the Learning Organization", The Systems Thinker Newsletter, cilt 7, sayı 1
135. Dr. Tunç EVCİMEN, ÖĞRENEN ORGANİZASYONLAR, Yatay İlişkilerde Otorite ve Sorumluluk
136. Araş. Gör. Seçil Bal TAŞTAN, ÖĞRENEN ORGANİZASYONLAR, Human Resources,2008
137. Özkan, T. ve Lajunen, T. (2003). Güvenlik Kültürü Ve İklimi. PiVOLKA, 2(10), 3-4.

NOTLAR:

NOTLAR:

Özlem ÖZKILIÇ

1970 yılında Ankara'da doğdu, ilköğrenimini Ankara'da, orta öğrenimini Kuşadası'nda tamamladı. Liseyi ise Ankara'da Kocatepe Mimar Kemal Lisesi'nde bitirdi. 1991 yılında Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Kimya Mühendisliği Bölümünden mezun oldu.

1995 yılında Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Kimya Mühendisliği Bölümünde, TÜBİTAK'tan burslu olarak "Batı Anadolu Klinoptilolit Zeolitlerinin Deterjanlarda Fosfatlar Yerine Kullanılabilirliğinin Araştırılması" üzerine yaptığı çalışma ile Yüksek Lisans eğitimini tamamladı.

1995 yılında yüksek lisans tezi TÜBİTAK tarafından bilim destek ödülüne layık görüldü.

1993 yılında Çalışma ve Sosyal Güvenlik Bakanlığı İş Teftiş Ankara Grup Başkanlığında İş Müfettişi Yardımcısı olarak göreve başladı. 1993 yılından 1997 yılına kadar İş Teftiş Ankara Grup Başkanlığında İş Müfettişi Yrd. ve daha sonra İş Müfettişi olarak görev yaptı.

1997 yılında İş Teftiş İstanbul Grup Başkanlığı'nda göreve başladı. 2000 – 2002 yılları ile 2009 - 2012 yılları arasında İş Teftiş İstanbul Grup Başkan Yardımcısı olarak görev yaptı.

İş Teftiş İstanbul Grup Başkanlığı'nda İş Başmüfettişi olarak görev yapmakta iken 2013 yılında emekli oldu ve A Sınıfı İş Güvenliği Uzmanı olarak danışmanlık ve eğitim konularında çalışmaya başladı.

ISBN: 978-605-9994-01-9

Yayın No: 338 / 15 Mayıs 2014

Hoşdere Cad. Reşat Nuri Sokak No: 108 Çankaya - ANKARA
Tel: (0312) 439 77 17 (Pbx) • Faks: (0312) 439 75 92-93-94
www.tisk.org.tr • E-mail: tisk@tisk.org.tr

Baskı:www.ajansturk.com.tr

TİSK

RİSK DEĞERLENDİRMESİ ATEX DİREKTİFLERİ - PATLAYICI ORTAMLAR BÜYÜK ENDÜSTRİYEL KAZALARIN ÖNLENMESİ VE ETKİLERİNİN AZALTILMASI - KANTİTATİF RİSK DEĞERLENDİRME SEVESO II VE SEVESO III DİREKTİFİ (COMAH DİREKTİFİ)