



# TÜRK STANDARDI

## TS EN 31010

Temmuz 2010

ICS 03.120.10; 31.020

---

### **Risk Yönetimi - Risk değerlendirme teknikleri (IEC/ISO 31010:2009)**

Risk management - Risk assessment techniques  
(IEC/ISO 31010:2009)

Gestion des risques -  
Techniques d'évaluation des risques  
(CEI/ISO 31010:2009)

Risikomanagement -  
Verfahren zur Risikobeurteilung  
(IEC/ISO 31010:2009)

---

**TÜRK STANDARDLARI ENSTİTÜSÜ**  
**Necatibey Caddesi No.112 Bakanlıklar/ANKARA**

## Milli Önsöz

- Bu standard; kaynağı EN 31010:2010 standardı olan TS EN 31010:2010 Türk standardının Mühendislik İhtisas Kurulu'na bağlı TK29 Yönetim Sistemleri Teknik Komitesi marifetiyle hazırlanan Türkçe tercümesidir.
- CENELEC resmi dillerinde yayınlanan diğer standard metinleri ile aynı haklara sahiptir.
- Bu standardda kullanılan bazı kelime ve/veya ifadeler patent haklarına konu olabilir. Böyle bir patent hakkının belirlenmesi durumunda TSE sorumlu tutulamaz.
- Bu standardda atıf yapılan standartların milli karşılıkları aşağıda verilmiştir.

EN, ISO, IEC vb. No	Adı (İngilizce)	TS No	Adı (Türkçe)
ISO/IEC 73: 2009	Guide Risk management – Vocabulary- Guidelines for use in standards	TSE ISO Guide 73: 2012	Risk yönetimi - Terimler ve tarifler
ISO 31000: 2009	Risk management – Principles and guidelines	TS ISO 31000: 2011	Risk yönetimi - Prensipler ve kılavuzlar

TS EN 31010: 2010 standardı, EN 31010: 2010 standardı ile birebir aynı olup, Avrupa Elektroteknik Standardizasyon Komitesi'nin (CENELEC, Avenue Marnix 17 B-1000 Brussels) izniyle basılmıştır.

Avrupa Standardlarının herhangi bir şekilde ve herhangi bir yolla tüm kullanım hakları Avrupa Elektroteknik Standardizasyon Komitesi (CENELEC) ve üye ülkelerine aittir. TSE kanalıyla CENELEC'den yazılı izin alınmaksızın çoğaltılamaz.

## **Risk Yönetimi - Risk değerlendirme teknikleri (IEC/ISO 31010:2009)**

**Risk management - Risk assessment techniques  
(IEC/ISO 31010:2009)**

**Gestion des risques -  
Techniques d'évaluation des risques  
(CEI/ISO 31010:2009)**

**Risikomanagement -  
Verfahren zur Risikobeurteilung  
(IEC/ISO 31010:2009)**

Bu Avrupa Standardı CENELEC tarafından 01 Mayıs 2010 tarihinde onaylanmıştır. CENELEC üyeleri, bu Avrupa Standardına hiçbir değişiklik yapmaksızın ulusal standard statüsü veren koşulları öngören CEN/CENELEC İç Yönetmeleri'ne uymak zorundadırlar.

Bu tür ulusal standartlarla ilgili güncel listeler ve bibliyografik atıflar, Merkez Sekretarya'ya veya herhangi bir CENELEC üyesine başvurarak elde edilebilir.

Bu Avrupa Standardı, üç resmi dilde (İngilizce, Fransızca, Almanca) yayınlanmıştır. Başka herhangi bir dile tercümesi, CENELEC üyesinin sorumluluğundadır ve resmi sürümleri ile aynı statüde olduğu Merkez Sekretarya'ya bildirilir.

CENELEC üyeleri sırasıyla, Almanya, Avusturya, Belçika, Birleşik Krallık, Bulgaristan, Çek Cumhuriyeti, Danimarka, Estonya, Finlandiya, Fransa, Hırvatistan, Hollanda, İrlanda, İspanya, İsveç, İsviçre, İtalya, İzlanda, Kıbrıs (Güney Kıbrıs Rum Yönetimi), Letonya, Litvanya, Lüksemburg, Macaristan, Malta, Norveç, Polonya, Portekiz, Romanya, Slovakya, Slovenya ve Yunanistan'ın milli standard kuruluşlarıdır.

# **CENELEC**

**Avrupa Elektroteknik Standardizasyon Komitesi  
European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung**

**Yönetim Merkezi: Avenue Marnix 17, B - 1000 Brussels**



## Ön söz

ISO TMB "Risk yönetimi" çalışma grubu ile IEC TC 56 "Güvenilebilirlik" Teknik Komitesi tarafından hazırlanan, IEC/ISO 31010'un 1. baskısı olan 56/1329/FDIS, dokümanının metni, IEC-CENELEC oylamasına sunulmuş ve 01/05/2010 tarihinde EN 31010 olarak CENELEC tarafından kabul edilmiştir.

Bu dokümanın bazı unsurlarının patent haklarına konu olabileceğine dikkat edilmelidir. Böyle herhangi bir patent hakkının belirlenmesi durumunda CEN ve CENELEC sorumlu tutulamaz.

Aşağıdaki tarihler tespit edilmiştir:

- Özdeş ulusal standard olarak yayınlayarak veya onay duyurusu yaparak EN'nin ulusal düzeyde uygulamaya konması gereken en son tarih (dop) 01.02.2011
- EN ile çelişen ulusal standartların yürürlükten kaldırılması gereken en son tarih (dow) 01.05.2013

Ek ZA CENELEC tarafından eklenmiştir.

## Onay bilgisi

IEC/ISO 31010: 2009 Uluslararası Standardının metni hiçbir değişiklik yapılmaksızın CENELEC tarafından Avrupa Standardı olarak kabul edilmiştir.

Resmi baskısında, kaynak için belirtilen standartlara aşağıdaki notların eklenmesi gerekir:

IEC 60300-3-11	Not - EN 60300-3-11 olarak uyumlaştırılmış.
IEC 61078	Not - EN 61078 olarak uyumlaştırılmış.
IEC 61165	Not - EN 61165 olarak uyumlaştırılmış.
IEC 61508 serisi	Not - EN 61508 serisi uyumlaştırılmış (değiştirilmemiş).
IEC 61511 serisi	Not - EN 61511 serisi uyumlaştırılmış (değiştirilmemiş).
IEC 61649	Not - EN 61649 olarak uyumlaştırılmış.
ISO 22000	Not - EN ISO 22000 olarak uyumlaştırılmış.

## Ek ZA (Zorunlu hükümler)

### Bu standardda atıf yapılan uluslararası standartlar ile bu standartlara karşılık gelen Avrupa standartları

Aşağıdaki atıf yapılan dokümanlar, bu dokümanın uygulanması için zaruridir. Tarih belirtilen atıflarda, sadece belirtilmiş olan baskı geçerlidir. Tarih belirtilmemiş atıflarda, atıf yapılan dokümanın en son baskısı (tadiller dahil) kullanılır.

**Not** – Uluslararası bir standardda, CENELEC tarafından (mod) ile gösterilen ortak değişiklikler yapıldığında, ilgili EN/HD uygulanır.

<u>Doküman Numarası</u>	<u>Tarih</u>	<u>Doküman adı</u>	<u>EN/HD</u>	<u>Tarih</u>
ISO/IEC Guide 73	-	Risk yönetimi - Terimler ve tarifler –Kullanım kılavuzu	-	-
ISO 31000	-	Risk yönetimi - Prensipler ve kılavuzlar	-	-



IEC/ISO 31010

1. Baskı 2009-11

# ULUSLARARASI STANDARD

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



**Risk Yönetimi – Risk değerlendirme teknikleri**

**Risk management – Risk assessment techniques**

**Gestion des risques – Techniques d'évaluation des risques**



BU YAYIN, TELİF HAKKI KORUMALIDIR.  
Copyright © 2009 IEC, Cenevre, İsviçre

Tüm hakları saklıdır. Aksi belirtilmedikçe, bu yayının herhangi bir bölümü herhangi bir şekilde ya da fotokopi ve mikrofilm dahil aşağıda adresi verilen IEC'den yazılı izin alınmaksızın ya da dokümanı talep edenin ülkesindeki IEC üyesi Ulusal Komitenin yazılı izni olmaksızın elektronik veya mekanik herhangi bir yolla çoğaltılamaz ya da kullanılamaz.

IEC telif hakları ile ilgili herhangi bir sorunuz olması halinde ya da bu yayınlı ilgili ilave haklar konusunda bilgi talebiniz olması halinde, detaylı bilgi için lütfen aşağıdaki adresle veya IEC üyesi Ulusal Komitenizle temasa geçiniz.

IEC Merkez Ofis  
3, rue de Varembé  
CH-1211 Geneva 20  
İsviçre  
e-posta: [inmail@iec.ch](mailto:inmail@iec.ch)  
Web: [www.iec.ch](http://www.iec.ch)

## IEC hakkında

Uluslararası Elektroteknik Komisyonu (IEC), tüm elektrik, elektronik ve ilgili teknolojiler konusunda Uluslararası Standardlar hazırlayan ve yayınlayan önde gelen (lider) küresel kuruluştur.

## IEC yayınları hakkında

IEC yayınlarının teknik muhtevası, IEC tarafından sürekli gözden geçirilmektedir. En son baskıyı aldığınızdan emin olun, bir düzeltme ya da tadil yayınlanmış olabilir.

▪ IEC Yayınları kataloğu için: [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

IEC on-line kataloğu, çeşitli kriterlerle (atıf numarası, metin, teknik komite) arama yapabilmeyi sağlar. Ayrıca projeler, yürürlükten kaldırılmış ve yerine geçen yayınlar konusunda da bilgi verir.

▪ IEC Just Published: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Tüm yeni IEC yayınlarını hakkında bilgi sahibi olun. 'Just Published', yeni çıkan tüm yayınları ayda iki kez detaylı olarak verir. On-line ya da e-posta yoluyla da mevcuttur.

▪ Electropedia: [www.electropedia.org](http://www.electropedia.org)

İngilizce ve Fransızca 20 000'in üzerinde terim ve tanımları kapsayan dünyanın önde gelen çevrimiçi elektronik ve elektrik terimleri sözlüğü. Online Uluslararası Elektroteknik Sözlük olarak da bilinir.

▪ Müşteri Hizmetleri Merkezi: [www.iec.ch/webstore/custserv](http://www.iec.ch/webstore/custserv)

Bu yayınlı ilgili düşüncelerinizi iletmek isterseniz ya da daha fazla yardıma ihtiyacınız varsa, lütfen Müşteri Hizmetleri Merkezi Sık Sorulan Soruları ziyaret ediniz ya da bizimle temas kurunuz:

e-posta: [csc@iec.ch](mailto:csc@iec.ch)

Tel.: +41 22 919 02 11

Faks: +41 22 919 03 00





IEC/ISO 31010

1. Baskı 2009-11

**ULUSLARARASI  
STANDARD  
INTERNATIONAL  
STANDARD  
NORME  
INTERNATIONALE**



**Risk Yönetimi – Risk değerlendirme teknikleri**

**Risk management – Risk assessment techniques**

**Gestion des risques – Techniques d'évaluation des risques**

ULUSLARARASI  
ELEKTROTEKNİK  
KOMİSYONU

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE  
CODE PRIX **XD**

ICS 03.100.01

ISBN 2-8318-1068-2



# İçindekiler

Sayfa

<b>ÖN SÖZ</b> .....	<b>3</b>
<b>Giriş</b> .....	<b>5</b>
<b>1 Kapsam</b> .....	<b>6</b>
<b>2 Atıf yapılan standard ve/veya dokümanlar</b> .....	<b>6</b>
<b>3 Terimler ve tarifler</b> .....	<b>6</b>
<b>4 Risk değerlendirme kavramları</b> .....	<b>6</b>
4.1 Amaç ve faydalar .....	6
4.2 Risk değerlendirmesi ve risk yönetim çerçevesi .....	7
4.3 Risk değerlendirmesi ve risk yönetimi prosesi .....	7
4.3.1 Genel .....	7
4.3.2 İletişim ve istişare .....	7
4.3.3 Kapsam oluşturma .....	7
4.3.4 Risk değerlendirme .....	8
4.3.5 Risk iyileştirme .....	9
4.3.6 İzleme ve gözden geçirme .....	9
<b>5 Risk değerlendirme prosesi</b> .....	<b>9</b>
5.1 Genel bakış .....	9
5.2 Risk belirleme .....	10
5.3 Risk analizi .....	10
5.3.1 Genel .....	10
5.3.2 Kontrol değerlendirmeleri .....	11
5.3.3 Sonuç analizi .....	11
5.3.4 Olabilirlik analizi ve olasılık tahmini .....	12
5.3.5 Ön analiz .....	12
5.3.6 Belirsizlikler ve duyarlılıklar .....	12
5.4 Risk kıyaslama .....	13
5.5 Dokümantasyon .....	13
5.6 Risk değerlendirmesinin izlenmesi ve gözden geçirilmesi .....	14
5.7 Risk değerlendirmesinin yaşam döngüsü aşamalarında uygulanması .....	14
<b>6 Risk değerlendirme tekniklerinin seçimi</b> .....	<b>14</b>
6.1 Genel .....	14
6.2 Tekniklerin seçimi .....	14
6.2.1 Kaynakların varlığı .....	15
6.2.2 Belirsizliğin niteliği ve derecesi .....	15
6.2.3 Karmaşıklık .....	16
6.3 Risk değerlendirmesinin yaşam döngüsü aşamalarında uygulanması .....	16
6.4 Risk değerlendirme tekniklerinin türleri .....	16
<b>Ek A - (Bilgi için) - Risk değerlendirme tekniklerinin karşılaştırılması</b> .....	<b>17</b>
<b>Ek B - (Bilgi için) - Risk değerlendirme teknikleri</b> .....	<b>24</b>
<b>Kaynaklar</b> .....	<b>74</b>

<b>Şekil 1 - Risk değerlendirmesinin risk yönetim prosesine katkısı .....</b>	<b>9</b>
<b>Şekil B.1 - Doz - tepki eğrisi.....</b>	<b>32</b>
<b>Şekil B.2 - IEC 60300-3-9 dan bir FTA örneği.....</b>	<b>41</b>
<b>Şekil B.3 - Örnek olay ağacı.....</b>	<b>43</b>
<b>Şekil B.4 - Neden-sonuç analizi örneği.....</b>	<b>45</b>
<b>Şekil B.5 - Ishikawa veya Balık-kılıcı diyagramı .....</b>	<b>47</b>
<b>Şekil B.6 - Neden-ve-Etki analizi örnek ağaç formülasyonu .....</b>	<b>47</b>
<b>Şekil B.7 - İnsan güvenilirlik değerlendirmesi örneği .....</b>	<b>52</b>
<b>Şekil B.8 - İstenmeyen sonuçlar için kullanılan Papyon (Bow tie) diyagramı .....</b>	<b>53</b>
<b>Şekil B.9 - Markov sistem örneği diyagramı .....</b>	<b>57</b>
<b>Şekil B.10 - Durum geçişi örnek diyagramı.....</b>	<b>58</b>
<b>Şekil B.11 - Örnek Bayes Ağı.....</b>	<b>63</b>
<b>Şekil B.12 - ALARP konsepti .....</b>	<b>65</b>
<b>Şekil B.13 - Etki kriteri çizelgesi kısmi örneği .....</b>	<b>69</b>
<b>Şekil B.15 - Risk derecelendirme matrisi kısmi örneği .....</b>	<b>70</b>

# ULUSLARARASI ELEKTROTEKNİK KOMİSYONU

## Risk Yönetimi – Risk değerlendirme teknikleri

### ÖN SÖZ

- 1) Uluslararası Elektroteknik Komisyonu (IEC), tüm ulusal elektroteknik komitelerden (IEC Ulusal Komiteler) oluşan dünya çapında bir standardizasyon kuruluşudur. IEC'nin amacı, elektrik ve elektronik alanlarda standardizasyonla ilgili tüm sorulara dair uluslararası işbirliğini desteklemektir. IEC, bu amacı gerçekleştirmek için ve diğer faaliyetlerine ek olarak Uluslararası Standardlar, Teknik Şartnameler, Teknik Raporlar, Herkesin Kullanımına Açık Şartnameler (PAS) ve Rehberler (bundan böyle 'IEC Yayını/Yayınları' olarak anılacaktır.) yayınlar. Yayınların hazırlanması görevi teknik komitelere verilmiştir; üzerinde çalışma yapılan konu ile ilgilenen herhangi bir IEC Ulusal Komitesi, bu hazırlık çalışmasına katılabilir. IEC ile işbirliği içindeki Uluslararası kuruluşlar, kamu kuruluşları ve sivil toplum kuruluşları da bu hazırlık çalışmalarına katılabilir. IEC, iki kuruluş arasındaki anlaşma çerçevesinde belirlenen şartlara uygun olarak Uluslararası Standardizasyon Kuruluşu (ISO) ile yakın işbirliği içindedir.
- 2) IEC'nin teknik konulara dair resmi kararları veya mutabakatları, teknik komitelerin konuyla ilgilenen tüm IEC Ulusal Komitelerinden üyeleri olduğu için, mümkün olduğunca ilgili konulardaki uluslararası fikir birliği anlamına gelir.
- 3) IEC Yayınları, uluslararası kullanım için tavsiyeler şeklindedir ve IEC Ulusal Komiteleri tarafından da bu anlamda kabul edilirler. IEC Yayınlarının teknik muhtevasının doğru olmasını sağlamak için her türlü gayret gösterilmiş olsa da, IEC yayınlarının nihai kullanıcı tarafından kullanım yolları ya da nihai kullanıcıların yanlış yorumlamaları konusunda sorumlu tutulamaz.
- 4) IEC Ulusal Komiteleri, uluslararası tektipliği desteklemek için IEC yayınlarını kendi ulusal ve bölgesel yayınlarına azami ölçüde şeffaf bir biçimde uygulamayı taahhüt ederler. Herhangi bir IEC Yayını ile karşılık gelen ulusal veya bölgesel yayın arasındaki herhangi bir farklılık, ulusal veya bölgesel yayında açıkça belirtilmelidir.
- 5) IEC, uygunluk onaylaması yapmaz. Bağımsız belgelendirme kuruluşları uygunluk değerlendirmesi hizmeti verir ve bazı alanlarda IEC uygunluk markalarını kullanır. IEC, bağımsız belgelendirme kuruluşlarının gerçekleştirdiği herhangi bir hizmetten sorumlu tutulamaz.
- 6) Tüm kullanıcılar, bu yayının son baskısına sahip olduklarından emin olmalıdırlar.
- 7) Herhangi bir kişisel yaralanma, mal hasarı ya da herhangi bir diğer hasardan ve bu IEC yayınının ya da diğer herhangi bir IEC yayınının yayınlanmasından, kullanımdan, ya da buna dayanılmasından kaynaklanan masraflar (yasal ücretler dâhil) veya harcamalardan dolayı IEC ve IEC'nin yöneticileri, çalışanları, hizmetlileri veya teknik komitelerinin üyeleri ve uzmanları ve IEC Ulusal Komiteleri dahil temsilcileri doğrudan ya da dolaylı olarak sorumlu tutulamaz.
- 8) Bu yayında verilen Normatif atıflara dikkat edilmelidir. Atıf yapılan yayınların kullanımı, bu yayının doğru uygulaması için kaçınılmazdır.
- 9) Bu IEC Yayınının bazı unsurlarının patent haklarına konu olma ihtimaline dikkat edilmelidir. IEC bu tür herhangi bir ya da tüm patent haklarının belirlenmesi durumunda sorumlu tutulamaz.

ISO/IEC 31010 Uluslararası standardı; IEC Teknik Komitesi 56: Güvenilirlik tarafından, ISO TMB "Risk Yönetimi" çalışma grubu ile birlikte hazırlanmıştır.

Bu standard metni aşağıdaki dokümanlara dayalıdır:

FDIS	Oylama raporu
8/1260/FDIS	8/1264/RVD

Bu standardın onaylanması ile ilgili oylamaya dair tüm bilgi, yukarıdaki çizelgede gösterilen oylama raporunda bulunabilir. ISO, 18 oy dışında 17 üye kuruluşları tarafından standard onaylanmıştır.

Bu yayın, ISO/IEC Direktifleri, Bölüm 2'ye uygun olarak yazılmıştır.

Komite, yayınlarla ilgili bilgilerin yer aldığı "<http://webstore.iec.ch>" internet adresinde gösterilen değişmezlik tarihine kadar, bu yayının muhtevasının değişmemesine karar vermiştir. Bu tarihte, yayın:

- Yeniden onaylanır,
- Yürürlükten kaldırılır,
- Revize edilen bir baskı ile yer değiştirir veya
- Tadil edilir.

**ÖNEMLİ - Bu yayının kapak sayfası üzerindeki “colour inside-renkli iç kısım” logosu, içeriğin doğru anlaşılabilmesi için yararlı olacağı düşünülen renkleri içerdiğini gösterir. Bu nedenle, kullanıcılar bu dokümanı renkli yazıcı kullanarak yazdırmalıdır.**

## Giriş

Her tür ve büyüklükteki kuruluşlar, hedeflerine ulaşmalarını etkileyebilecek çok çeşitli risklerle karşılaşır.

Bu hedefler; kuruluşun stratejik girişimlerinden operasyonlarına, proseslerine ve projelerine kadar çeşitli faaliyetleri ile ilgili olabilir ve sosyal, kültürel, politik ve itibar etkilerinin yanı sıra, toplumsal, çevresel, teknolojik, güvenlik ve emniyet sonuçları, ticari, finansal ve ekonomik ölçüler ile de yansıtılabilir.

Kuruluşun yer aldığı tüm faaliyetler, yönetilmesi gereken riskler içerir. Risk yönetimi prosesi; belirsizliği ve gelecekteki olayların ve durumların (istenen veya istenmeyen) olasılığını ve uzlaşılan hedefler üzerindeki etkisini göz önünde bulundurarak karar vermeye yardımcı olur.

Risk yönetimi, mantıksal ve sistematik yöntemlerin aşağıdakiler için uygulanmasını içerir:

- Proses boyunca iletişim ve istişare,
- Herhangi bir faaliyet, proses, fonksiyon veya ürünle ilişkili risklerin belirlenmesi, analiz edilmesi, kıyaslanması, iyileştirilmesi için kapsamın oluşturulması,
- Risklerin izlenmesi ve gözden geçirilmesi,
- Sonuçların uygun şekilde raporlanması ve kayıt altına alınması.

Risk değerlendirmesi; risk yönetiminin bir parçası olup, hedeflerin nasıl etkilenebileceğini belirleyen, ilave iyileştirmeye gerek olup olmadığına karar vermeden önce riskleri, etkileri ve olasılıkları bakımından analiz etmek için yapılandırılmış bir proses sunar.

Risk değerlendirmesi aşağıdaki temel sorulara cevap arar:

- Ne olabilir ve neden (riskin belirlenmesi ile) ?
- Sonuçlar nelerdir?
- Gelecekte meydana gelme olasılığı nedir?
- Riskin sonuçlarını en aza indiren veya riskin olasılığını azaltan etkenler var mıdır ?

Riskin seviyesi tolere edilebilir veya kabul edilebilir seviyede midir ve ilave iyileştirmeye gerek var mıdır ? Bu standard, risk değerlendirme tekniklerinin seçiminde ve bunların kullanılmasında mevcut iyi uygulamaların yansıtılmasını amaçlamaktadır ve henüz üzerinde profesyonel uzlaşmaya varılmamış yeni ve gelişmekte olan yöntemler dâhil edilmemiştir.

Bu standard genel amaçlı bir yapıda olduğu için, pek çok sektöre ve değişik sistem türlerine kılavuzluk sağlayabilir. Bu sektörlerde, belirli uygulamalar için tercih edilen özel hazırlanmış yöntem ve ayrıntılı değerlendirme seviyeleri sağlayan belirli standartlar mevcut olabilir. Söz konusu standartlar, eğer bu standardla uyum halinde ise, bu standartlar genellikle yeterli olacaktır.

## 1 Kapsam

Bu standard, ISO 31000 için destekleyici bir standarddır ve risk değerlendirmelerinde kullanılmak üzere sistematik tekniklerin seçimi ve uygulanması için kılavuzluk bilgilerini kapsar.

Bu standardda uygun olarak yapılan risk değerlendirmesi, risk yönetimi ile ilgili diğer faaliyetlere katkıda bulunur.

Bu standardda, farklı tekniklerin uygulamasının tanıtımı yapılmakta olup, kavramların ve uygulamasının ayrıntılarının anlatıldığı diğer uluslararası standartlara atıf yapılmıştır.

Bu standard belgelendirme, düzenleyici veya sözleşmeye dayalı kullanım amaçlı değildir.

Bu standard, risk analizine ihtiyaç duyulduğunu gösteren özel kriterler sunmadığı gibi, belli bir uygulama için gerekli olan risk analiz yöntemini de belirlemez.

Bu standard, tüm tekniklere atıfta bulunmaz ve bir tekniğin bu standardda bulunmaması, o tekniğin geçersiz olduğu anlamına gelmez. Bir yöntemin belirli bir durum için uygulanabilir olması, söz konusu yöntemin uygulanmasının zorunlu olduğu anlamına gelmez.

**Not** - Bu standard, güvenlikle özel olarak ilgilenmez. Bu standard genel bir risk yönetimi standardı olup, güvenlik konusuna yapılan her türlü atıf bilgi niteliğindedir. IEC standartları için güvenlik açısından tanıtım kılavuzu ISO/IEC Guide 51'de verilmiştir.

## 2 Atıf yapılan standard ve/veya dokümanlar

Aşağıdaki atıf dokümanları, bu dokümanın uygulanması için zaruridir. Tarih belirtilen atıflarda, belirtilmiş olan baskı geçerlidir. Tarih belirtilmemiş atıflarda, atıf yapılan dokümanın en son baskısı (tadiller dahil) kullanılır.

ISO/IEC Guide 73, *Risk management – Vocabulary - Guidelines for use in standards* (TSE ISO Guide 73, Risk yönetimi - Terimler ve tarifler)

ISO 31000, *Risk management – Principles and guidelines* (TS ISO 31000 Risk yönetimi - Prensipler ve kılavuzlar)

## 3 Terimler ve tarifler

Bu dokümanın amaçları bakımından, ISO/IEC Guide 73'te bulunan terim ve tarifler uygulanır.

## 4 Risk değerlendirme kavramları

### 4.1 Amaç ve faydalar

Risk değerlendirmesinin amacı, belirli risklerin nasıl iyileştirileceği ve seçenekler arasında nasıl tercih yapılacağı üzerine bilgilendirilmiş kararlar vermek için kanıta dayanan bilgi ve analiz sağlamaktır.

Risk değerlendirmesi uygulamasının bazı temel faydaları aşağıda verilmektedir:

- Riskleri ve hedefler üzerindeki potansiyel etkilerini anlamak,
- Karar vericiler için bilgi sağlamak,
- İyileştirme alternatiflerinin seçimine yardımcı olabilmek için risklerin anlaşılmasına katkıda bulunmak,
- Sistemlerde ve kuruluşlarda risklere önemli katkı sağlayıcıları ve zayıf öğeleri belirlemek,
- Alternatif sistem, teknoloji veya yaklaşımlardaki risklerle kıyaslamak,
- Riskleri ve belirsizlikleri iletmek,
- Önceliklerin oluşturulmasına yardımcı olmak,
- Olay sonrası incelemeleri temel alarak, olayları önlemeye yönelik katkıda bulunmak,
- Farklı risk iyileştirme yöntemlerini seçmek,
- Düzenleyici şartları yerine getirmek,
- Önceden tanımlı kriterlerle karşılaştırıldığında, riskin kabul edilip edilmeyeceğinin kıyaslanmasına yardımcı olmak için bilgi sağlamak,
- Tamamen bertaraf etmek üzere riskleri değerlendirmek.



## 4.2 Risk deęerlendirmesi ve risk ynetim erevesi

Bu standard, risk deęerlendirmesinin ISO 31000'de tarif edilen risk ynetim prosesi ve erevesi kullanılarak gerekleřtirildięini varsayar.

Bir risk ynetim erevesi, risk ynetimini kuruluř genelinde her seviyede iine dhil edecek politikalar, prosedrler ve organizasyonile ilgili dzenlemeleri saęlar.

Bu erevenin bir parası olarak, risklerin ne zaman ve nasıl deęerlendirileceęine dair karar verilmesinde kuruluřun bir politikası veya stratejisi olmalıdır.

zellikle, risk deęerlendirmesini gerekleřtirecek kiřiler ařaęıdaki konular hakkında belirsizlik bırakmamalıdır:

- Kuruluřun hedefleri ve kapsamı,
- Tolere edilebilecek risk trleri ve byklkleri ve kabul edilmeyen risklerin nasıl iyileřtirileceęi,
- Risk deęerlendirmesinin kuruluřun proseslerine nasıl entegre edileceęi,
- Risk deęerlendirmesinde kullanılacak yntemler ve teknikler ve bunların risk ynetim prosesine katkısı,
- Risk deęerlendirmesinin gerekleřtirilmesinde hesap verebilirlik, sorumluluk ve yetki,
- Risk deęerlendirmesi gerekleřtirmek iin mevcut kaynaklar,
- Risk deęerlendirmesinin nasıl raporlanıp gzden geirileceęi.

## 4.3 Risk deęerlendirmesi ve risk ynetimi prosesi

### 4.3.1 Genel

Risk deęerlendirmesi, ISO 31000'de tanımlanan ve ařaęıdaki adımları ieren, risk ynetimi prosesinin ana unsurlarından oluřur:

- İletiřim ve iřtiřare,
- Kapsamın oluřturulması,
- Risk deęerlendirmesi (risk belirleme, risk analizi ve risk kıyaslamadan oluřur),
- Risk iyileřtirme,
- İzleme ve gzden geirme.

Risk deęerlendirmesi tek bařına bir faaliyet deęildir ve risk ynetim prosesinin dięer bileřenleri ile tam olarak entegre edilmelidir.

### 4.3.2 İletiřim ve iřtiřare

Bařarılı bir risk deęerlendirmesi, paydařlarla etkin iletiřim ve iřtiřareye baęlıdır.

Paydařların risk ynetim prosesine dhil edilmesi ařaęıdaki durumlarda yardımcı olacaktır:

- İletiřim planının oluřturulması,
- Kapsamın uygun řekilde tanımlanması,
- Paydařların ıkarlarının anlařılması ve dikkate alınmasının gvence altına alınması,
- Riskleri tanımlamak ve analiz etmek iin farklı alanlardaki uzmanlıkların bir araya getirilmesi,
- Riskleri deęerlendirirken farklı grřlerin uygun řekilde dikkate alındıęının temini,
- Risklerin doęru řekilde tanımlanmasının temini,
- Risk iyileřtirme planının onaylanması ve desteklenmesinin saęlanması.

Paydařlar; deęiřiklik ynetimi, proje ve program ynetimi ve finansal ynetim gibi dięer ynetim disiplinleri ile birlikte, risk deęerlendirme prosesi ara yzne katkıda bulunmalıdır.

### 4.3.3 Kapsam oluřturma

Kapsam oluřturma, riskleri ynetmek iin temel parametreleri tanımlar ve prosesin geri kalanı iin kapsam ve risk kriterlerini tayin eder. Kapsam oluřturma, deęerlendirilen belirli bir riskin arka planı olduęu kadar, bir btn olarak kuruluřu ilgilendiren i ve dıř parametrelerin dikkate alınmasını ierir.

Kapsam oluřturulurken, risk deęerlendirme hedefleri, risk kriterleri ve risk deęerlendirme programı belirlenir ve zerinde uzlařılır.

Belirli bir risk deęerlendirmesi iin kapsam oluřturma, i, dıř ve risk ynetim kapsamının tanımlanmasını ve risk kriterinin sınıflandırılmasını iermelidir:

- a) Dış kapsamın oluşturulması, kuruluşun ve sistemin çalıştığı ortamın tanınması ile ilgilidir, bu ortam aşağıdakileri içerir:
- Kültürel, politik, yasal, mevzuata ilişkin, finansal, ekonomik ve rekabet ortamı etkenleri, bu etkenler uluslararası, ulusal, bölgesel veya yerel olabilir,
  - Kuruluşun hedefleri üzerinde etkisi bulunan anahtar faktörler ve eğilimler,
  - Dış paydaşların algıları ve değerleri.
- b) İç kapsamın oluşturulması aşağıdakilerin anlaşılmasını içerir:
- Kuruluşun kaynak ve bilgi bakımından yeterliliği,
  - Bilgi akışı ve karar alma prosesleri,
  - İç paydaşlar,
  - Hedefler ve bunları başarmak için uygulanan stratejiler,
  - Algılar, değerler ve kültür,
  - Politikalar ve prosesler,
  - Standartlar ve kuruluş tarafından adapte edilmiş referans modelleri ve
  - Yapılar (örneğin, idari yapı, roller ve sorumluluklar).
- c) Risk yönetimi prosesinde kapsamın oluşturulması aşağıdakileri içerir:
- Hesap verebilirlik ve sorumlulukların ve tanımlanması,
  - Özel olarak dâhil etme ve hariç tutmaları da içeren, risk yönetim faaliyetlerinin sınırlarının tanımlanması,
  - Zaman ve yer bakımından, proje, proses, fonksiyon ve faaliyetin sınırlarının tanımlanması,
  - Belirli bir proje veya faaliyetin, kuruluşun diğer projeleri ve faaliyetleri ile olan ilişkisinin tanımlanması,
  - Risk değerlendirme metodolojisinin tanımlanması,
  - Risk kriterlerinin tanımlanması,
  - Risk yönetim performansının nasıl kıyaslanacağına tanımlanması,
  - Alınması gereken kararlar ve yapılması gereken faaliyetlerin tanımlanması ve belirlenmesi,
  - Gerekli çalışmaların kapsamı veya çerçevesinin tanımlanması, bu çalışmaların sınırları, hedefleri ve gerçekleşmesi için gerekli olan kaynakların belirlenmesi.
- d) Risk kriterinin tanımlanması, aşağıdaki konular hakkında karar almayı içerir.
- Dahil edilecek sonuçların niteliği, türleri ve bu sonuçların nasıl ölçüleceği,
  - Olasılıkların hangi yollarla ifade edileceği,
  - Risk seviyesinin nasıl belirleneceği,
  - Risk iyileştirmeye ihtiyaç olduğunda, buna nasıl karar verileceği ile ilgili kriterler,
  - Riskin ne zaman kabul edilebilir ve/veya tolere edilebilir olduğuna karar verme kriterleri,
  - Risklerin birleşimlerinin dikkate alınıp alınmayacağı, dikkate alınacaksa nasıl alınacağı,

Kriterler aşağıdaki gibi kaynakları temel alabilir:

- Üzerinde mutabık kalınmış proses hedefleri,
- Şartnamelerde tanımlanmış kriterler,
- Genel veri kaynakları,
- Güvenlik entegrasyon seviyeleri gibi, genel kabul görmüş sanayi kriterleri,
- Kuruluşa ait risk iştahı,
- Belirli donanım veya uygulamalar için yasal ve diğer şartlar.

#### 4.3.4 Risk değerlendirme

Risk değerlendirmesi; risk belirleme, risk analizi ve risk kıyaslamasından oluşan genel prosestir.

Riskler; projeler, bireysel faaliyetler, spesifik riskler için kuruluş seviyesinde veya birim seviyesinde değerlendirilebilir. Farklı kapsamlar için farklı araçlar ve tekniklerin kullanılması uygun olabilir.

Risk değerlendirme; risklerin, nedenlerinin, sonuçlarının ve olasılıklarının anlaşılmasını sağlar. Bu bilgiler aşağıdakiler hakkında karar almak için girdi sağlar:

- Bir faaliyetin gerçekleştirilmesinin gerekip gerekmediği,
- Fırsatların nasıl en üst seviyeye yükseltilebileceği,
- Risklerin iyileştirme ihtiyacının olup olmadığı,
- Farklı riskler ile ilgili seçenekler arasında seçim yapma,

- Risk iyileştirme seçeneklerini öncelik sırasına koyma,
- Zararlı riskleri tolere edilebilir seviyeye getirecek en uygun risk iyileştirme stratejilerinin seçimi.

#### 4.3.5 Risk iyileştirme

Risk değerlendirilmesinin tamamlanmasını takiben gerçekleştirilen risk iyileştirme; riskin meydana gelme olasılığını ve/veya etkisini değiştirmek için bir veya daha fazla ilgili seçenek arasında seçim yapmayı, üzerinde uzlaşma sağlamayı ve bu seçeneklerin uygulanmasını içerir.

Yukarıdaki işlemleri, riskin tekrar değerlendirilerek yeni seviyesinin anlaşılması ve önceden belirlenmiş kriterlere göre tahammül edilebilirliğinin tespit edilmesine bağlı olarak daha fazla iyileştirme gerekip gerekmediğine dair karar verilmesi şeklindeki döngüsel bir proses takip eder.

#### 4.3.6 İzleme ve gözden geçirme

Risk yönetimi prosesinin bir parçası olarak, riskler ve kontroller, aşağıdakileri doğrulamak için düzenli bir şekilde izlenmeli ve gözden geçirilmelidir:

- Riskler hakkındaki varsayımların geçerliliğini koruduğu,
- İç ve dış kapsam da dâhil, risk değerlendirmelerinin dayandığı varsayımların geçerliliğini koruduğu,
- Beklenen sonuçların elde edildiği,
- Risk değerlendirme sonuçlarının gerçek deneyimlerle uyumlu olduğu,
- Risk değerlendirme tekniklerinin doğru olarak uygulandığı,
- Risk iyileştirmelerinin etkin olduğu.

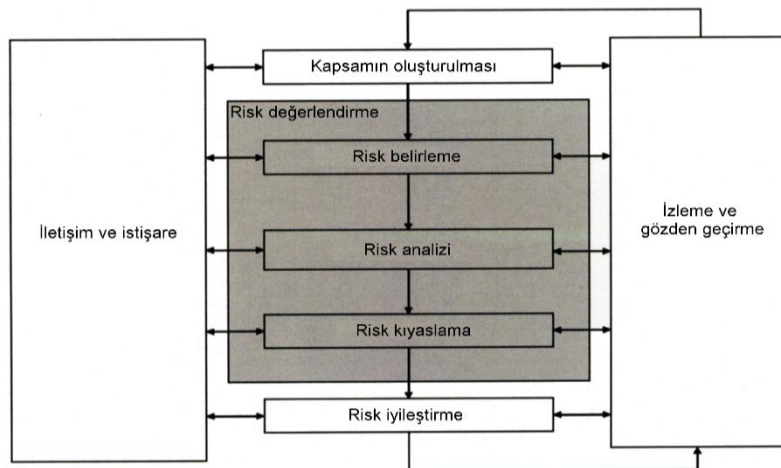
İzleme ve gözden geçirme ile ilgili hesap verebilme durumu belirlenmelidir.

## 5 Risk değerlendirme prosesi

### 5.1 Genel bakış

Risk değerlendirmesi, hedeflerin gerçekleşmesini etkileyen risklerin ve mevcut kontrollerin yeterliliği ve etkinliğinin sorumlular ve karar vericiler tarafından gelişmiş seviyede anlaşılmasını sağlar. Bu, riskleri iyileştirebilmek için en uygun yaklaşımla kararın verilebilmesine temel sağlar. Risk değerlendirmesinin çıktısı, kuruluşun karar verme proseslerinin girdisini oluşturur.

Risk değerlendirme; risk belirleme, risk analizi ve risk kıyaslamasından oluşan genel prosesdir (bk. Şekil 1). Prosesin uygulanma şekli, sadece risk yönetim prosesinin kapsamına değil, aynı zamanda risk değerlendirmenin uygulanması için kullanılacak yöntem ve tekniklere de bağlıdır.



Şekil 1 - Risk değerlendirmesinin risk yönetim prosesine katkısı

Riskler çok çeşitli neden ve sonuçları kapsayabileceğinden, risk değerlendirme çok disiplinli bir yaklaşımı gerektirebilir.

## 5.2 Risk belirleme

Risk belirleme; risklerin ortaya çıkartılması, tanınması ve kayıt altına alınması prosesidir.

Risk belirlemenin amacı, kuruluşun veya sistemin hedeflerine ulaşmasını etkileyebilecek ne tür durumların ortaya çıkabileceğinin veya mevcut olabileceğinin tanımlanmasıdır. Kuruluş; risk belirlendikten sonra, tasarım özellikleri, insan, prosesler ve sistemler gibi mevcut kontrolleri tanımlamalıdır.

Risk belirleme prosesi; hedefler üzerinde önemli etkiye ve bu etkinin niteliğine sahip olabilecek risk (fiziksel zarar kapsamında tehlike) olaylar, durumlar veya koşulların neden ve kaynağının belirlenmesini içerir.

Risk belirleme yöntemleri aşağıdakileri içerebilir:

- Delile dayalı yöntemler, örnek olarak kontrol listeleri ve geçmiş dönem verilerin gözden geçirmeleri,
- Bir uzman ekibinin, sistematik bir proses izleyerek, yapılandırılmış soru setleri ile riskleri belirlemeye yönelik sistematik ekip yaklaşımları,
- HAZOP benzeri tümevarımlı usavurma teknikleri.

Risk belirlemenin doğruluğunu ve eksiksizliğini geliştirmek için, beyin fırtınası ve Delphi yöntemi gibi çeşitli destekleyici teknikler kullanılabilir.

Mevcut kullanılan tekniklerden bağımsız olarak, risk belirlenmesinde insani ve organizasyon ile etkenlere yeterli dikkatin gösterilmesi önemlidir. Bu nedenle, donanım ve yazılım olayları kadar, insani ve kurumsal etkenlerle beklentilerden sapmalar da risk belirleme prosese dâhil edilmelidir.

## 5.3 Risk analizi

### 5.3.1 Genel

Risk analizi; riski kavramayı geliştirme ile ilgilidir. Risk analizi; risk değerlendirmesine, risklerin iyileştirilmesinin gerekli olup olmadığına ve en uygun iyileştirme stratejilerine ve yönetimlerine girdi sağlar.

Risk analizi; mevcut kontrollerin bulunmasını (veya bulunmamasını) ve etkinliklerini dikkate alarak tanımlanmış risk olaylarının sonuçlarının ve olasılıkların belirlenmesini içerir. Sonuçlar ve sonuçların olasılıkları daha sonra risk seviyesini belirlemek için birleştirilir.

Risk analizi, risklerin nedenleri ve kaynaklarının, sonuçların ve bu sonuçların meydana gelme olasılıklarının dikkate alınmasını içerir. Sonuçları ve olasılıkları etkileyen etkenler tanımlanmalıdır. Bir olayın birden fazla sonucu olabilir ve birden fazla hedefi etkileyebilir. Mevcut risk kontrolleri ve bunların etkinlikleri hesaba katılmalıdır. Bu analizler için çeşitli yöntemler Ek B'de açıklanmaktadır. Karmaşık uygulamalar için birden fazla teknik gerekebilir.

Risk analizi normal olarak, risk seviyesini ölçebilmek için bir olay, durum veya koşuldaki ve bunlarla ilişkili olasılıklarda ortaya çıkabilecek bir dizi sonucun tahminini içerir. Bununla birlikte, sonuçların çok önemsiz olduğu veya olasılığın aşırı derecede düşük beklendiği durumlarda, karar vermek için tek bir parametre yeterli olabilir.

Bazı durumlarda, birden çok sayıda olayın veya koşulun ya da belirgin olarak tespit edilemeyen bir olayın neticesi olarak bir sonuç ortaya çıkabilir. Bu durumda risk değerlendirmesi, koruma seviyesi veya kurtarma stratejileri ile ilgili muamelelerin tanımlanması bakımından sisteme ait unsurların önemliliği ve zafiyetleri üzerine yoğunlaşır.

Risklerin analizinde kullanılan yöntemler kalitatif, yarı-kantitatif veya kantitatif olabilir. Gerekli ayrıntı derecesi belirli bir uygulamaya, güvenilir verinin bulunmasına ve kuruluşun karar verme şartlarına bağlıdır. Bazı yöntemler ve analizin ayrıntı derecesi mevzuatla belirlenebilir.

Kalitatif değerlendirme; sonuç, olasılık ve risk seviyesini, önem seviyelerine göre "yüksek", "orta" ve "düşük" gibi belirler, sonucu ve olasılığı birleştirebilir ve riskin sonuç seviyesini kalitatif bir kriterlere göre kıyaslar.

Yarı-kantitatif yöntemler, sonuç ve olasılık için sayısal derecelendirme ölçekleri kullanır ve bir formül vasıtasıyla risk seviyesini oluşturmak için sonuç ve olasılığı birleştirir. Ölçekler, doğrusal ya da logaritmik veya başka bir çeşit eşleştirme olabilir, kullanılan formüller de değişiklik gösterebilir.

Kantitatif analizler, sonuçlar ve olasılıkları hakkında pratik değer tahmininde bulunur ve kapsam oluşturulurken risk seviyesi değerini spesifik birimler ölçeğinde üretir. Tam sayısal analiz; analiz edilecek sistem veya faaliyet hakkında yetersiz bilgi, veri yetersizliği, insan etkeni vs. ya da sayısal analiz için gerekli olan çabanın karşılığının bulunmaması nedeniyle her zaman mümkün olmayabilir veya istenmeyebilir. Bu tür durumlarda, alanlarında bilgi sahibi uzmanlar tarafından gerçekleştirilecek karşılaştırmalı yarı-kantitatif veya kalitatif derecelendirme daha etkili olabilir.

Analizin kalitatif olduğu durumlarda, kullanılan tüm terimlerin açık tanımı verilmeli ve kullanılacak kriterlerin esası kayıt altına alınmalıdır.

Tam sayısallaşmanın gerçekleştirildiği durumlarda bile, hesaplanan risk seviyelerinin tahminden ibaret olduğu bilinmelidir. Kullanılan yöntem ve verilerdeki hassasiyet ve doğruluk payı ile risk seviyelerine atanan değerlerin tutarsızlığa düşmemesini güvence altına almak için özen gösterilmelidir.

Risk seviyeleri, o risk için en uygun olan terimler ve risk kıyaslamasına yardımcı olacak şekilde ifade edilmelidir. Bazı durumlarda, riskin büyüklüğü, çeşitli sonuçlar üzerine olasılık dağılımı olarak ifade edilebilir.

### 5.3.2 Kontrol değerlendirmeleri

Riskin seviyesi, mevcut kontrollerin etkinliği ve yeterliliğine bağlıdır. Ele alınması gereken sorular içerisinde aşağıdakiler de bulunmalıdır:

- Belirli bir risk için mevcut kontroller nelerdir?
- Bu kontroller, riskleri tolere edilebilir bir seviyede kontrol altında bulundurmaya için yeterli derecede iyileştirme yetkinliğine sahip midir?
- Uygulamada kontroller kendilerinden beklenen şekilde işlemekte midir? ve gerektiğinde etkinlikleri kanıtlanabilir mi?

Bu sorular, sadece düzenli dokümantasyon ve yürürlükte güvence prosesleri mevcut ise güven içerisinde cevaplanabilir.

Belirli bir kontrol veya ilişkili kontrol kümesinin etkinliği kalitatif, yarı-kantitatif veya kantitatif olarak ifade edilebilir. Çoğunlukla, yüksek derecede doğruluk teminatı bulunmaz. Böylelikle, kontrollerin geliştirilmesinde veya farklı risk iyileştirme yöntemlerinin sağlanmasında en iyi şekilde çaba sarf edilip edilmediği hakkında hüküm verilebilir.

### 5.3.3 Sonuç analizi

Sonuç analizi, belirli bir olay veya durumun oluştuğunu varsayarak ortaya çıkabilecek etkinin türünü ve doğasını belirler. Bir olayın farklı tür ve büyüklükte etkileri olabilir ve bu olay farklı hedefleri ve paydaşları etkileyebilir. Kapsam oluşturulurken, analiz edilecek sonuçların türleri ve etkilenecek paydaşlara karar verilir.

Sonuç analizi, çıktılarının basit bir tanımından ayrıntılı kalitatif modelleme veya zafiyet analizine kadar değişkenlik gösterebilir.

Etkiler, düşük önem ancak yüksek olasılığa veya yüksek önem ve düşük olasılığa veya bunların arasında bir sonuca sahip olabilir. Bazı durumlarda, yöneticilerin genellikle en çok önemsendiği çok büyük etki potansiyeli olan riskler üzerinde odaklanması daha uygundur. Diğer durumlarda, gerek yüksek gerekse düşük öneme sahip risklerin ayrı ayrı analiz edilmesi önemli olabilir. Örneğin, sık görülen ancak düşük etkiye (veya kronik) sahip problemler, yüksek veya uzun dönemli etkilere sahip olabilir. Bununla birlikte, bu iki risk türünü yönetmek genellikle çok farklıdır, bu nedenle ayrı olarak analiz edilmeleri faydalı olur.

Sonuç analizi, aşağıdakileri içerebilir:

- Sonuçlar üzerinde etkisi olan ilgili tüm yardımcı faktörlerle birlikte sonuçları ele alınmak için mevcut kontrolleri göz önünde bulundurma,
- Orijinal hedefler ile risk sonuçlarını ilişkilendirme,
- Değerlendirmenin kapsamı ile uyumlu olması durumunda, gerek acil sonuçların ve gerekse belirli bir zaman sonra ortaya çıkabilecek sonuçları göz önünde bulundurma,
- Bağlantılı sistemler, faaliyetler, donanımlar ve kuruluşlar üzerinde etkisi olan sonuçlar gibi ikincil sonuçları dikkate alma.

### 5.3.4 Olabilirlik analizi ve olasılık tahmini

Olasılığı tahmin etmek için üç genel yaklaşım türü yaygın olarak kullanılır; bunlar ayrı ayrı kullanılabilirler gibi birlikte de kullanılabilirler.

- Geçmişe ait ilgili verinin, eskiden oluşmuş olay ve durumları tespit etmek ve dış değer hesaplaması ile gelecekte oluşma olasılığını tahmin etmek için kullanılması. Kullanılan veri, göz önünde bulundurulacak sistemin türü, tesis, kuruluş veya faaliyetleri ile ve aynı zamanda söz konusu kuruluşun işletim standartları ile ilgili olmalıdır. Geçmişe ait olarak, oluşma sıklığı çok düşük ise, bu takdirde yapılacak tahminler çok belirsiz olacaktır. Bu; özellikle geçmişte hiç oluşmamış olay, durum veya şartların gelecekte gerçekleşmeyeceğini öngörememe durumunda geçerli olur.
- Hata ağacı ve olay ağacı analizi gibi öngörü teknikleri kullanarak olasılık tahminleri (bk. Ek B). Geçmişe ait verilerin mevcut olmadığı veya yeterli olmadığı durumlarda, olasılığı; sistem, faaliyet, donanım veya kuruluş ve bunlarla bağlantılı başarı veya başarısızlık durumlarından türetmek gereklidir. Donanımlar için sayısal veri, insanlar, kuruluşlar ve işletim tecrübesinden kaynaklanan sistemler veya yayınlanmış veri kaynakları daha sonra en önemli olayın olasılığın tahmininin üretilmesi için birleştirilir. Öngörü tekniklerini kullanırken, analiz kapsamında aynı nedenden tesadüfi olarak sistem içerisindeki farklı parçaların aynı anda hata üretme olasılığının varlığına bir ihtiyat payı ayrıldığına güvence altına alınması önemlidir. Belirsizliklerin etkisi hesaplanarak yaşlanma veya diğer bozulma proseslerinden dolayı donanım kaynaklı ve yapısal hataların olasılığını çıkarmak için simülasyon tekniklerine ihtiyaç duyulabilir.
- Olasılığı tahmin etmek için sistematik ve yapısal bir proses dahilinde uzman görüşleri kullanılabilir. Uzman yorumları, tarihsel, sisteme özgü, kuruluşa özgü, deneysel, tasarım vb. ilgili mevcut tüm bilgileri kullanmalıdır. Uygun soruların formüle edilmesine yardımcı olan uzman görüşlerini temin etmek için birkaç yöntem vardır. Bu yöntemler, Delphi yaklaşımı, ikili karşılaştırmalar, kategori derecelendirmesi ve mutlak olasılık değerlendirmesini içerir.

### 5.3.5 Ön analiz

En önemli riskleri tanımlamak ve daha az önemli veya küçük olanlarını ilave analizlerin dışında bırakmak için riskler izlenmelidir. Burada amaç, kaynakların en önemli riskler üzerinde odaklanmasını temin etmektir. Toplamda büyük etkiye neden olacak sık oluşan düşük etkili risklerin elenmemesine özen gösterilmelidir.

İzleme işlemi, kapsamda tanımlanan kriterlere dayanmalıdır. Ön analizler, aşağıda belirtilen bir ya da daha fazla yol haritasını belirler:

- Daha ileri değerlendirmeye tabi tutmadan risklerin iyileştirilmesi kararı,
- İyileştirme gerektirmeyecek önemsiz risklerin ayrılması,
- Daha ayrıntılı seviye risk değerlendirmesi yapılarak ilerlenmesi.

Başlangıç varsayımları ve sonuçlar doküman haline getirilmelidir.

### 5.3.6 Belirsizlikler ve duyarlılıklar

Risk analizlerinde çoğunlukla önemli ölçüde belirsizlik bulunur. Belirsizliklerin doğru anlaşılması, risk analiz sonuçlarının yorumlanması ve etkin olarak iletilmesi için gereklidir. Riskleri belirlemek ve analiz etmek için kullanılan veri, yöntem ve modellerde bulunan belirsizliklerin analizi, bunların uygulanmasında önemli rol oynar. Belirsizlik analizi, sonuçları tanımlamak için kullanılan varsayımlar ve parametrelerdeki değişikliklerin bir araya gelmesinden kaynaklanan, sonuçlar içerisindeki değişim veya kusurun belirlenmesini içerir. Belirsizlik analizi ile yakından alakalı alan ise duyarlılık analizidir.

Risk analizi ile ilgili çoğunlukla önemli belirsizlikler vardır. Risk analiz sonuçlarının etkin bir şekilde yorumlanması ve aktarılması için belirsizliklerin anlaşılması gereklidir. Riskleri belirlemek ve analiz etmek için kullanılan veriler, yöntemler ve modellerde bulunan belirsizliklerin analizi, bunların uygulanmasında önemli rol oynar. Belirsizlik analizi, sonuçları tanımlamak için kullanılan parametre ve varsayımlardaki toplam sapmalardan kaynaklanan sonuçlardaki sapmaların veya hataların belirlenmesini içerir. Duyarlılık analizi, belirsizlik analizi ile yakın ilgisi olan bir alandır.

Duyarlılık analizi, tekil olarak girdi parametrelerindeki değişimlerin yol açacağı riskin büyüklüğün önemi ve ölçüsünün belirlenmesini içerir. Analiz, hangi verilerin daha hassas hangilerinin daha az hassas ve bu nedenle toplam hassasiyet üzerinde daha az etkisi bulunan verilerin tanımlanması için kullanılır.

Risk analizinin eksiksizliği ve doğruluğu, mümkün olduğu ölçüde tam olarak ifade edilmelidir. Belirsizlik kaynakları, mümkün olduğunda tanımlanmalı, gerek veri gerekse model/yöntem belirsizliklerini ele almalıdır. Analizin duyarlı olduğu parametreler ve duyarlılık derecesi belirtilmelidir.

#### 5.4 Risk kıyaslama

Risk kıyaslama; riskin önem seviyesini ve türünü belirlemek için, riskin tahmini seviyelerinin kapsam oluşturulurken tanımlanan risk kriteri ile karşılaştırılmasını içerir.

Risk kıyaslama, gelecekteki faaliyetlerle ilgili kararlar vermek için risk analizi esnasında elde edilen risk bilgilerini kullanır. Risk algılarını da içeren, etik, yasal, mali ve diğer hususlar da kararlar için girdi oluşturur.

Kararlar aşağıdakileri içerebilir:

- Bir riskin iyileştirme gerektirip gerektirmediği,
- İyileştirme öncelikleri,
- Bir faaliyetin gerçekleştirilip gerçekleştirilmeyeceği,
- Hangi yol/yolların izleneceği.

Kapsam oluşturulurken, alınması gereken kararların doğasına ve bu kararları almak için kullanılacak olan kriterlere karar verilir. Ancak, bu aşamada tanımlanmış riskler hakkında daha fazla bilgiye sahip olduğundan daha ayrıntılı bir şekilde tekrar gözden geçirilmeleri gerekir.

Risk kriterlerini tanımlamak için en basit çerçeve, riskleri ele alma ihtiyacı olanlar ve olmayanlar olarak ayıran tek düzey çerçevedir. Bu durum, cazip şekilde basit sonuçlar verir. Ancak riskleri tahmin etmede ve ele alma ihtiyacı olanlar ve olmayanlar arasında sınırın tanımlanmasındaki belirsizlikleri yansıtmaz.

Riskin iyileştirilip iyileştirilmeyeceği ve nasıl iyileştirileceği ile ilgili karar, risk almanın maliyeti ve elde edilecek faydası ile gelişmiş kontrollerin uygulanmasının maliyetine ve fayda bağlıdır.

Genel yaklaşım, riskleri üç bölgeye ayırmaktır.

- a) Faaliyetten oluşacak fayda ne olursa olsun risk seviyesinin tolere edilmeyeceği ve maliyeti ne olursa olsun iyileştirmenin zorunlu olduğu, üst bölge,
- b) Fayda ve maliyetlerin hesaba katıldığı ve fırsatların muhtemel sonuçları dengelediği, orta bölge (gri alan),
- c) Risk seviyesinin ihmal edilebilir olarak kabul edildiği veya riski iyileştirme önlemlerine ihtiyaç duyulmayacak kadar küçük olduğu alt bölge.

Güvenlik uygulamalarında kullanılan "makul seviyede uygulanabilir" veya ALARP kriter sistemi, bu yaklaşımı takip eder. Orta bölgede, fayda ve maliyetlerin doğrudan kıyaslanabildiği düşük riskler için değişken bir ölçek mevcuttur. Bununla birlikte, ek azaltma maliyeti, tam anlamıyla, kazanılan güvenlik yararından fazla olana kadar, yüksek riskler için zarar potansiyeli azaltılmalıdır.

#### 5.5 Dokümantasyon

Risk değerlendirme prosesi, değerlendirme sonuçları ile birlikte doküman haline getirilmelidir. Riskler, anlaşılabilir terimlerle ifade edilmelidir ve risk seviyelerinin gösterildiği birimler belirgin olmalıdır.

Rapor kapsamı, değerlendirmenin hedeflere ve kapsamına bağlıdır. Çok basit değerlendirmeler hariç, dokümantasyon aşağıdakileri içerebilir:

- Hedefler ve kapsam,
- Sistemin ilgili bölümlerinin ve bunların fonksiyonlarının tanımlanması,
- Kuruluşun iç ve dış kapsamının özeti ve bunların değerlendirilen durum, sistem veya şartlarla nasıl bağlantılı olduğu,
- Uygulanan risk kriterleri ve bunların doğrulanması,
- Sınırlamalar, varsayımlar ve hipotezlerin doğrulanması,
- Değerlendirme metodolojisi,
- Risk belirleme sonuçları,
- Veriler, varsayımlar ve bunların kaynakları ve geçerli kılınması,
- Risk analizi sonuçları ve bunların kıyaslanması,

- Duyarlılık ve belirsizlik analizi,
- İzlenmesi gereken kritik varsayımlar ve diğer faktörler,
- Sonuçların tartışılması,
- Sonuçlar ve tavsiyeler,
- Kaynaklar.

Eğer risk değerlendirmesi süreklilik gösteren bir risk yönetim prosesini desteklerse, sistemin, kuruluşun, donanımın veya faaliyetin yaşam döngüsü boyunca bulundurulabilecek şekilde yürütülmeli ve doküman haline getirilmelidir. Değerlendirme; yönetim prosesinin ihtiyaçlarına uygun olarak, önemli yeni bilgilerin ortaya çıkması ve kapsam değişiklikleri durumunda güncellenmelidir.

## 5.6 Risk değerlendirmesinin izlenmesi ve gözden geçirilmesi

Risk değerlendirme prosesi; kapsam ve zaman içerisinde değişmesi beklenen faktörler ile risk değerlendirmesini değiştirecek veya geçersiz kılacak diğer faktörlerin önemini vurgular. Bu faktörler, sürekli izleme ve gözden geçirme için özel olarak tanımlanmalıdır, böylelikle gerekli olduğunda risk değerlendirmesi güncellenebilmelidir.

Risk değerlendirmesini geliştirmek için izlenmesi gereken veriler belirlenmeli ve toplanmalıdır.

Kontrollerin etkinliği de risk analizinde kullanılmak üzere izlenmeli ve belgelenmelidir. Kanıtlar ve dokümantasyonun oluşturulması ve gözden geçirilmesiyle ilgili hesap verebilirlik belirlenmelidir.

## 5.7 Risk değerlendirmesinin yaşam döngüsü aşamalarında uygulanması

Pek çok faaliyet, proje ve ürünün; ilk kavram ve tanım aşamasından, hizmetten çıkarma ve donanımın elde çıkarmanın bertarafını içerebilen, son tamamlamanın gerçekleşmesine kadar bir yaşam döngüsüne sahip bulunduğu düşünülebilir.

Risk değerlendirme, yaşam döngüsünün tüm aşamalarında uygulanabilir ve genellikle, her bir aşamada alınması gereken kararlara yardımcı olmak için farklı ayrıntı seviyelerinde birçok kere uygulanır.

Yaşam döngüsü evrelerinin farklı şartları vardır ve farklı tekniklere ihtiyaç duyarlar. Örneğin, kavram ve tanımlama aşamasında bir fırsat belirlendiğinde, devam edip edilmeyeceği konusunda karar vermek için risk değerlendirme kullanılabilir.

Çeşitli alternatiflerin mevcut olduğu durumlarda, olumlu ve olumsuz riskler arasında en iyi dengeyi sağlayan karara yardımcı olmak ve alternatif kavramları kıyaslamak için, risk değerlendirmesi kullanılabilir.

Tasarım ve geliştirme aşamasında, risk değerlendirmesi aşağıdaki alanlarda katkı verir:

- Sistem risklerinin tolere edilebilir seviyede olduğunu güvence altına alma,
- Tasarım iyileştirme prosesi,
- Maliyet etkinlik çalışmaları,
- Takip eden yaşam döngüsü aşamalarına etki eden risklerin belirlenmesi.

Faaliyet devam ettiği sürece, risk değerlendirme; normal ve acil şartlar için prosedürlerin geliştirilmesini destekleme amaçlı bilgi sağlamada kullanılabilir.

## 6 Risk değerlendirme tekniklerinin seçimi

### 6.1 Genel

Bu bölüm, risk değerlendirme tekniklerinin nasıl seçileceğini açıklamaktadır. Bir risk değerlendirmesinin gerçekleştirilmesinde veya risk değerlendirme prosesinin desteklenmesinde kullanılacak farklı araçlar ve teknikler, Ek'lerde listelenmekte ve daha ayrıntılı olarak açıklanmaktadır. Bazı durumlarda, birden daha fazla değerlendirme yönteminin kullanılması gerekli olabilir.

### 6.2 Tekniklerin seçimi

Risk değerlendirme, farklı derinlik ve ayrıntı seviyelerinde ve basitten karmaşığa, bir ya da daha fazla yöntem kullanarak ele alınabilir. Değerlendirme biçimi ve bunun çıktıları, oluşturulan kapsamın bir parçası olarak geliştirilen risk kriteri ile tutarlı olmalıdır. Ek A, risk değerlendirme tekniklerinin geniş kategorileri ile verilen risk



durumdaki faktörler arasındaki kavramsal ilişkiyi gösterir ve belirli bir duruma uygun risk değerlendirme tekniklerinin kuruluş tarafından nasıl seçilebileceği ile ilgili açıklayıcı örnekler sunmaktadır.

Genel ifade ile uygun teknikler aşağıdaki özellikleri göstermelidir:

- Gereçekleştirilebilir olmalı ve incelenmekte olan durum veya kuruluşa uygun olmalıdır,
- Sonuçları, riskin niteliğini ve nasıl iyileştirileceğini anlamayı artıracak bir şekilde sunulmalıdır,
- İzlenebilir, tekrarlanabilir ve doğrulanabilir bir şekilde kullanılabilir olmalıdır.

Konuyla ilgili ve konuya uygun olmasına göre tekniklerin seçim nedenleri verilmelidir. Farklı çalışmalardan elde edilen sonuçlar entegre edilirken, kullanılan teknikler ve çıktılar kıyaslanabilir olmalıdır.

Risk değerlendirmesinin yapılmasına karar verildiğinde, hedefler ve kapsam tanımlandığında, teknikler aşağıda verilen uygulanabilir faktörler temel alınarak seçilmelidir:

- Çalışmanın hedefleri. Risk değerlendirmesinin hedefleri ile kullanılan teknikler arasında doğrudan bir bağlantısı vardır. Örneğin, farklı seçenekler arasında kıyaslamalı bir çalışma yürütülüyorsa, farklılıktan etkilenmeyen sistem bölümleri için daha az ayrıntılı sonuç modellerinin kullanımı kabul edilebilir.
- Karar vericilerin ihtiyaçları. Bazı durumlarda, iyi kararlar alabilmek için yüksek seviyeli bir detaylandırma gereklidir. Diğer durumlarda, daha genel bir anlayış yeterlidir.
- Analiz edilen risklerin türü ve kapsamı.
- Sonuçların potansiyel büyüklüğünün, hangi risk değerlendirmenin gerçekleştirilmesine dair ayrıntılı karar, sonuçların ilk algılamasını yansıtmalıdır (Ön kıyaslama tamamlandıktan sonra tekrar düzenlenmesi gerekebilir).
- İhtiyaç duyulan uzmanlık seviyesi, insan ve diğer kaynaklar. Risk değerlendirmenin kapsam ve hedeflerini karşıladığı sürece, iyi uygulanmış basit bir yöntem, başarısız olarak uygulanmış karmaşık bir prosedürden daha iyi sonuçlar verebilir. Normal olarak, risk değerlendirmeye harcanan çaba, analiz edilen riskin potansiyel seviyesi ile tutarlı olmalıdır.
- Verilerin ve bilginin varlığı. Bazı teknikler diğerlerinden daha fazla bilgi ve veri gerektirir.
- Risk değerlendirmenin güncellenme ve değiştirme ihtiyacı. Değerlendirmenin zamanla, güncellenmesi ve değiştirilmesine ihtiyaç olabilir ve bu açıdan, bazı teknikler diğerlerine göre daha kolay tadil edilebilir.
- Düzenleyici ve sözleşmeye dayalı şartlar.

Kaynakların ulaşılabilirliği, bilgi ve verideki belirsizliğin doğası ve derecesi ve uygulamanın karmaşıklığı gibi çeşitli etkenler risk değerlendirmesinde yaklaşım seçimini etkileyebilir (bk. Çizelge A2).

### 6.2.1 Kaynakların varlığı

Risk değerlendirme tekniklerinin seçimini etkileyebilecek kaynaklar ve yeterlilikler aşağıdakileri içerir:

- Risk değerlendirme ekibinin becerileri, deneyimi, kapasitesi ve yeterliliği,
- Kuruluştaki zaman ve diğer kaynaklarla ilgi kısıtlamalar,
- Dış kaynak gerektiğinde yeterli bütçenin varlığı.

### 6.2.2 Belirsizliğin niteliği ve derecesi

Belirsizliğin niteliği ve derecesi, üzerinde düşünülmekte olan riske ait bilginin, kalitesi, miktarı ve bütünlüğünün anlaşılmasını gerektirir. Bu, risk hakkında yeterli bilgi, kaynakları ve nedenleri ile hedeflere ulaşırken yapabileceği etkilerinin bilinmesini de içerir. Belirsizlik, düşük veri kalitesinden veya gerekli ve güvenilir verinin bulunmamasından kaynaklanabilir. Tanımlanmış riskler için veri toplanması konusu somutlaştırılırsa, yöntemleri değişebilir, kurumun bu yöntemleri kullanım biçimi değişebilir ya da kurumun etkin bir veri toplama yöntemi hiç olmayabilir.

Belirsizliğin niteliği ve derecesi, üzerinde düşünülmekte olan riske ait mevcut bilginin kalitesi, miktarı ve bütünlüğünün anlaşılmasını gerektirir. Bu husus; risk, riskin kaynakları ve nedenleri, hedeflere ulaşma üzerindeki etkilerinin neler olduğuna dair mevcut bilgilerin ne derecede yeterli olduğunu içerir. Belirsizlik, düşük veri kalitesinden veya gerekli ve güvenilir verinin eksikliğinden kaynaklanabilir. Örneğin, belirlenen risk ile ilgili veri toplama için, veri toplama yöntemleri değişebilir, kuruluşun bu tip metotları kullanma yöntemleri değişebilir ya da kuruluşun beklenen riskle ilgili etkin bir veri toplama metodu hiç mevcut olmayabilir.

Belirsizlik, aynı zamanda kuruluşun iç ve dış kapsamının doğasında var olabilir. Mevcut veriler, geleceğin tahmin edilmesinde her zaman güvenilir bir temel sağlamazlar. Benzersiz risk türleri için geçmişte dönük veri mevcut olmayabilir veya farklı paydaşlardan gelen farklı yorumlar mevcut olabilir. Risk değerlendirme yapanlar, belirsizliğin türü ve niteliğini anlamalıdır ve risk değerlendirmenin sonuçlarına ait güvenilirliğinin etkilerini kavramaları gerekir. Bunlar, her zaman karar vericilere aktarılmalıdır.

### 6.2.3 Karmaşıklık

Aralarındaki etkileşimleri göz ardı ederek, her bir parçayı ayrı ele almak yerine, tüm sistem çapında risk değerlendirmesi ihtiyacı bulunan karmaşık sistemler örneğinde olduğu gibi riskler, kendi içlerinde karmaşık olabilirler. Diğer durumlarda, tek bir riski ele almanın, başka yerlerde sonuçları ve diğer faaliyetler üzerine etkisi olabilir. Bir riski yönetirken, başka bir yerde tolere edilemeyecek durumlar oluşturulmadığını güvence altına almak için, etki oluşturan sonuçlar ve risk bağımlılıkları anlaşılmalıdır. Bir veya bir risk portföyünün karmaşıklığının anlaşılması, risk değerlendirmesinde uygun yöntem veya tekniğin seçiminde çok önemlidir.

## 6.3 Risk değerlendirmesinin yaşam döngüsü aşamalarında uygulanması

Birçok faaliyet, proje ve ürünün; ilk kavram ve tanımlama aşamasından, hizmetten çıkarma ve donanımın elden çıkarılmasını içerebilen, son tamamlamanın gerçekleşmesine kadar bir yaşam döngüsüne sahip bulunduğu düşünülebilir.

Risk değerlendirme, yaşam döngüsünün tüm aşamalarında uygulanabilir ve genellikle, her bir aşamada alınması gereken kararlara yardımcı olmak için farklı ayrıntı seviyelerinde birçok defa uygulanır.

Yaşam döngüsü aşamalarının farklı şartları vardır ve farklı tekniklere ihtiyaç duyarlar. Örneğin, kavram ve tanımlama aşamasında bir fırsat belirlendiğinde, devam edip edilmeyeceği konusunda karar vermek için risk değerlendirme kullanılabilir.

Çeşitli alternatiflerin mevcut olduğu durumlarda, olumlu ve olumsuz riskler arasında en iyi dengeyi sağlayan karara yardımcı olmak ve alternatif kavramları kıyaslamak için, risk değerlendirmesi kullanılabilir.

Tasarım ve geliştirme aşamasında, risk değerlendirmesi aşağıdaki alanlarda katkı verir:

- Sistem risklerinin tolere edilebilir seviyede olduğunu güvence altına alma,
- Tasarım iyileştirme prosesi,
- Maliyet etkinlik çalışmaları,
- Takip eden yaşam döngüsü aşamalarına etki eden risklerin belirlenmesi.

Faaliyet devam ettiği sürece, risk değerlendirme; normal ve acil şartlar için prosedürlerin geliştirilmesini destekleme amaçlı bilgi sağlamada kullanılabilir.

## 6.4 Risk değerlendirme tekniklerinin türleri

Risk değerlendirme teknikleri, göreceli olarak güçlü ve zayıf yönlerinin anlaşılabilirliğini artırmak için farklı şekillerde sınıflandırılabilirler. Ek A'daki çizelgelerde, bazı potansiyel teknikler ve bunların kategorileri ile ilgili örnekler verilmiştir.

Her bir teknik, sağladıkları risk değerlendirmesinin doğası ve belirli durumlar için uygulanabilirlikleri ayrıntılı olarak Ek B'de verilmiştir.

## Ek A (Bilgi için)

### Risk değerlendirme tekniklerinin karşılaştırılması

#### A.1 Teknik türleri

İlk sınıflandırma, tekniklerin aşağıda belirtilen risk değerlendirme proses adımlarından her birine nasıl uygulanacağını gösterir.

- Riski belirleme,
- Risk analizi - Sonuç analizi,
- Risk analizi - Kalitatif, yarı kantitatif veya kantitatif olasılık tahmini,
- Risk analizi - Mevcut kontrollerin etkinliğinin değerlendirilmesi,
- Risk analizi - Risk seviyesinin tahmini,
- Risk kıyaslama.

Risk değerlendirme prosesindeki her bir adım için, metodun uygulanışı, kuvvetli uygulanabilir, uygulanabilir, uygulanamaz olarak tarif edilmiştir (bk. Çizelge A.1).

#### A.2 Risk değerlendirme tekniklerinin seçimini etkileyen faktörler

Sonraki adımda, yöntemlerin nitelikleri aşağıdaki açılardan tanımlanır:

- Problemin karmaşıklığı ve problemi analiz etmek için gereken yöntemler,
- Mevcut bilgilerin miktarı ve hedeflerin gerçekleştirilmesi için gereken unsurlara bağlı olarak, risk değerlendirmesi belirsizliğinin niteliği ve derecesi,
- Zaman, uzmanlık seviyesi, veri veya maliyet açısından gerekli olan kaynaklar,
- Yöntemin kantitatif çıktı sağlayıp sağlayamayacağı.

Risk değerlendirme yöntemlerinin türlerine ait örnekler Çizelge A.2'de listelenmiş olup, her yöntem yukarıdaki niteliklere göre, yüksek, orta veya düşük olarak derecelendirilmiştir.

**Çizelge A.1 Risk değerlendirmesinde kullanılan araçların uygulanabilirliği**

Araçlar ve teknikler	Risk değerlendirme prosesi					Bakınız Ek
	Risk belirleme	Risk analizi			Risk kıyaslama	
		Sonuç	Olasılık	Risk Seviyesi		
Beyin fırtınası	KU <sup>1)</sup>	UD <sup>2)</sup>	UD	UD	UD	B 01
Yapılandırılmış veya yarı-yapılandırılmış görüşmeler	KU	UD	UD	UD	UD	B 02
Delphi	KU	UD	UD	UD	UD	B 03
Kontrol listeleri	KU	UD	UD	UD	UD	B 04
Başlangıç tehlike analizi	KU	UD	UD	UD	UD	B 05
Tehlike ve işletilebilme çalışması (HAZOP)	KU	KU	U <sup>3)</sup>	U	U	B 06
Tehlike analizi ve kritik kontrol noktaları (HACCP)	KU	KU	UD	UD	KU	B 07
Çevresel risk değerlendirmesi	KU	KU	KU	KU	KU	B 08
Yapı «olursa ne olur?» (SWIFT)	KU	KU	KU	KU	KU	B 09
Senaryo analizi	KU	KU	U	U	U	B 10
İş etki analizi	U	KU	U	U	U	B 11
Kök neden analizi	UD	KU	KU	KU	KU	B 12
Hata türleri ve etkileri analizi	KU	KU	KU	KU	KU	B 13
Hata ağacı analizi	U	UD	KU	U	U	B 14
Olay ağacı analizi	U	KU	U	U	UD	B 15
Neden ve sonuç analizi	U	KU	KU	U	U	B 16
Neden - etki analizi	KU	KU	UD	UD	UD	B 17
Koruma katmanları analizi (LOPA)	U	KU	U	U	UD	B 18
Karar ağacı	UD	KU	KU	U	U	B 19
İnsan güvenilirlik analizi	KU	KU	KU	KU	U	B 20
Papyon (Bow-tie) analizi	UD	U	KU	KU	U	B 21
Güvenirlilik merkezli bakım (RCM)	KU	KU	KU	KU	KU	B 22
Sızan (Sneak) devre analizi	U	UD	UD	UD	UD	B 23
Markov analizi	U	KU	UD	UD	UD	B 24
Monte Carlo simülasyonu	UD	UD	UD	UD	KU	B 25
Bayes istatistiği ve Bayes ağları	UD	KU	UD	UD	KU	B 26
F-N eğrileri	U	KU	KU	U	KU	B 27
Risk endeksleri	U	KU	KU	U	KU	B 28
Sonuç/olasılık matrisi	KU	KU	KU	KU	U	B 29
Fayda/maliyet analizi	U	KU	U	U	U	B 30
Çok kriterli karar analizi (MDCA)	U	KU	U	KU	U	B 31

- 1) Kuvvetli uygulanabilir KU  
2) Uygulanabilir değil UD  
3) Uygulanabilir U

**Çizelge A.2 - Risk değerlendirmesinde kullanılan araçların uygulanabilirliği**

Risk değerlendirme teknik türü	Tanım	Etkileyen faktörlerin ilişkisi			Sayısal çıktı sağlayabilir mi?
		Kaynaklar ve yetkinlik	Belirsizliğin doğası ve derecesi	Karmaşıklık	
<b>KONTROLLERİ DEĞERLENDİRME</b>					
Kontrol listeleri	Risk belirlemenin basit şeklidir. Dikkate alınması gereken tipik belirsizliklerin listelenmesini sağlayan bir tekniktir. Kullanıcılar, önceden geliştirilmiş listeleri, kodları veya standartları referans alırlar.	Düşük	Düşük	Düşük	Hayır
Başlangıç tehlike analizi	Objektif tehlikeleri ve belirli bir faaliyet, tesis veya sistem için zarara neden olabilecek tehlikeli durumları ve olayları belirlemek için basit bir tümevarım yöntemidir.	Düşük	Yüksek	Orta	Hayır
<b>DESTEKLEYİCİ YÖNTEMLER</b>					
Yapılandırılmış görüşme ve beyin fırtınası	Bir ekip ile farklı görüşleri ve değerlendirmeleri toplama ve bunları sıralama aracıdır. Beyin fırtınası, hızlı cevaplarla veya yüz yüze ve toplu görüşme teknikleriyle tetiklenebilir.	Düşük	Düşük	Düşük	Hayır
Delphi Tekniği	Riskin kaynağını ve etkisinin belirlenmesi, olasılık ve sonuç tahmini ve risk değerlendirmesini destekleyen uzman görüşlerini birleştiren bir araçtır. Uzmanlar arasında görüş birliği sağlanması için ortak çalışma tekniğidir.  Bağımsız analizleri içerir ve uzmanlar tarafından oylanır.	Orta	Orta	Orta	Hayır
SWIFT – Yapılandırılmış “olursa ne olur”	Riskleri belirlemek için bir ekibin harekete geçirildiği sistemdir. Normal olarak kolaylaştırılmış çalıştaylarda kullanılır. Normal olarak, bir risk analizi ve değerlendirme tekniğiyle bağlantılıdır.	Orta	Orta	Az	Hayır
İnsan güvenilirlik analizi (HRA)	İnsan güvenilirlik analizi (HRA), insanların sistem performansları üzerindeki etkilerini ele alır ve insan hatalarının sistem üzerindeki etkilerinin değerlendirilmesinde kullanılabilir.	Orta	Orta	Orta	Evet

<b>SENARYO ANALİZİ</b>					
Kök neden analizi (tek kayıp analizi)	Meydana gelen tek bir kayıp hataya neden olan sebepleri ve ileride oluşabilecek benzer kayıpların önlenmesi için sistem veya prosesin nasıl geliştirilebileceğini anlamak için analiz edilir.  Analiz, kayıp oluştuğunda hangi kontrollerin mevcut olduğunu ve nasıl iyileştirilebileceklerini dikkate almalıdır.	Orta	Düşük	Orta	Hayır
Senaryo analizi	Olası gelecek senaryoları, düşünce gücü ile veya her bir senaryonun gerçekleşeceğini varsayarak mevcut ve farklı risklerin gözden geçirilmesi neticesinde ekstrapolasyon hesaplanması ile tanımlanması. Bu, resmi veya resmi olmayan, kalitatif veya kantitatif şekilde yapılabilir.	Orta	Yüksek	Orta	Hayır
Toksikolojik risk değerlendirmesi	Tehlikeler belirlenir ve belirlenen hedefi tehlikeye maruz bırakabilecek olası yolların belirlenmesi ve analiz edilmesi. Belirlenmiş zararın meydana gelme olasılığının bir ölçüsünü vermek için maruz kalma seviyesine ilişkin bilgi ile maruz kalmanın belirli bir seviyesinin neden olduğu zararın doğası birleştirilir.	Yüksek	Yüksek	Orta	Evet
İş etki analizi	Kuruluşun işletimini nasıl etkileyeceğinin, kilit kesinti risklerinin belirlenmesi ve bunları yönetmek için gerekli olan yetkinliklerin sayısallaştırılmasını içeren analiz.	Orta	Orta	Orta	Hayır
Hata ağacı analizi	İstenmeyen bir olayla (esas olay) başlayan ve gerçekleşebilecek tüm yolların belirlendiği teknik. Bunlar, mantıksal ağaç şekli ile grafik olarak gösterilirler. Hata ağacı oluşturulunca, potansiyel neden ve kaynakların azaltılması veya yok edilmesine yönelik çalışma dikkate alınmalıdır.	Yüksek	Yüksek	Orta	Evet

Olay ağacı analizi	Tümevarım mantığı kullanılarak başlatıcı olayların olasılıklarının muhtemel sonuçlara dönüştürülmesidir	Orta	Orta	Orta	Evet
Neden/sonuç analizi	Zaman gecikmelerinin dâhil edilebildiği hata ve olay ağacı analizlerinin birleşimidir. Başlatıcı olayların hem nedenleri hem de sonuçları göz önünde bulundurulur.	Yüksek	Orta	Yüksek	Evet
Neden ve etki analizi	Bir etki, farklı kategorilerde gruplandırılabilir çok sayıda katkı veren faktörlere sahip olabilir. Katkı veren faktörler genellikle beyin fırtınası ile belirlenir ve ağaç yapısında veya balık kılıcı diyagramı ile gösterilir.	Düşük	Düşük	Orta	Hayır
<b>FONKSİYON ANALİZİ</b>					
FMEA ve FMECA	FMEA (Olası hata ve etki analizi) olası hataları, mekanizmaları ve bunların etkilerini belirleyen bir tekniktir.  FMEA'nın çeşitli tipleri vardır. Tasarım (veya ürün) FMEA bileşenler ürünler için kullanılır. Sistem, FMEA sistemleri, proses FMEA ise imalat ve montaj proseslerinde kullanılır. Servis ve Yazılım FMEA'ları da vardır.  FMEA'yı, her bir olası hatanın önemini kalitatif, yarı-kalitatif veya kantitatif olarak (FMECA) tanımlayan bir kritiklik analiz ile takip edilebilir. Kritiklik analizi, hatanın sistem arızası ile sonuçlanacağı veya hata ile ilişkili riskin seviyesi ya da bir risk öncelik sırasının neden olacağı olasılığa dayalı olabilir.	Orta	Orta	Orta	Evet
Güvenirlilik merkezli bakım	Her türlü donanım için gerekli olan işleyişin güvenlik, kullanılabilirlik ve çalışma ekonomisine etkin ve verimli bir şekilde ulaşmak amacıyla hataları yönetmek için uygulanması gereken politikaları belirlemek için bir yöntemdir.	Orta	Orta	Orta	Evet

Sızıntı analizi (Sızan devre analizi)	Tasarım hatalarının belirlenmesi için kullanılan bir yöntemdir. Sızma durumu, istenmeyen bir olayın meydana gelmesine neden olabilen veya istenilen bir olayı engelleyen görünmeyen yazılım, donanım ya da her ikisinin entegre olduğu bir durumdur ve bileşenin hatasından kaynaklanmaz. Bu koşullar, rastgele doğası ve en titiz standart sistem testleri sırasında bile tespit edilmeme yeteneği ile karakterize edilirler. Sızma durumları, uygunsuz koşullarda çalışma, sistem kullanılabilirliğinin kaybına, program gecikmelerine veya hatta personelin, ölüm veya yaralanma neden olabilir.	Orta	Orta	Orta	Hayır
HAZOP Tehlike ve işletilebilirlik çalışmaları	Beklenen veya planlanan performanstan olası sapmaları tespit etmek için risklerin belirlenmesinin genel bir prosesidir. Bu kılavuz kelimeye dayalı bir sistem kullanır.  Sapmaların kritik noktaları değerlendirilir.	Orta	Yüksek	Yüksek	Hayır
HACCP Tehlike analizi ve kritik kontrol noktaları	Ürün kalitesi, güvenilirlik ve proseslerinin güvenliğini temin etmek için, sistematik, belirlenen sınırlar dahilinde olması gereken spesifik özellikleri ölçme ve izleme yöntemi ile proaktif ve önleyici sistemdir.	Orta	Orta	Orta	Hayır
<b>KONTROLLERİN DEĞERLENDİRİLMESİ</b>					
LOPA (Katmanları koruma analizi)	(Aynı zamanda bariyer analizi olarak da edilebilir). Bu kontrolleri ve kontrollerin etkinliğinin değerlendirilmesini sağlar.	Orta	Orta	Orta	Evet
Papyon analizi	Tehlikelerden sonuçlara kadar bir riskin yollarının basit bir şema yoluyla tanımlanması ve analiz edilmesi ve kontrollerin gözden geçirilmesidir. Hata ağacı analizinin bir olayın nedeni ile (bir papyon düğüm ile temsil edilen) bir olay ağacı analizinin ve sonuçlarının birleşmiş mantığı olarak kabul edilebilir.	Orta	Yüksek	Orta	Evet



<b>İSTATİKSEL YÖNTEMLER</b>					
Markov analizi	Bazen, durum-uzay analizinde denilen Markov analizi, çeşitli indirgenmiş durumlar dâhil, birden fazla durumlarda var olabilen onarılabilen karmaşık sistemlerin analizinde yaygın olarak kullanılmaktadır.	Yüksek	Düşük	Yüksek	Evet
Monte-Carlo analizi	Her bir girdinin tanımlanmış dağılımının olduğu ve girdilerin tanımlanmış ilişkilerle çıktılara bağlandığı birçok girdiler için sistemde, sistemdeki varyasyonlardan kaynaklanan toplu bir varyasyon oluşturmak için Monte Carlo simülasyonu kullanılır. Bu analiz, çeşitli girdilerin etkileşimlerinin matematiksel olarak tanımlandığı, spesifik bir model için kullanılabilir. Gösterilmek istenen belirsizliğin doğasına göre girdiler, dağıtım türlerine dayalı olabilir. Risk değerlendirmesi için, üçgen dağılımları veya beta dağılımları yaygın olarak kullanılır.	Yüksek	Düşük	Yüksek	Evet
Bayes analizi	Bayes analizi, doğru bir sonuç çıkarmak için öncesinde dağılımın doğruluğuna bağlıdır. Bayes görüşü, bir sonuç elde etmek için olasılıklı ilişkileri yakalayarak çeşitli alanlarda model ağları neden-sonuç girdilerinin bağlantısını kurar.	Yüksek	Düşük	Yüksek	Evet

## Ek B (Bilgi için)

### Risk değerlendirme teknikleri

#### B.1 Beyin fırtınası

##### B.1.1 Genel

Beyin fırtınası, olası hata türleri ve bunlarla bağlantılı tehlikeleri, riskleri, karar verme kriterlerini ve/veya iyileştirme seçeneklerini belirlemek amacı ile bir araya gelmiş uzman kişilerin arasında serbest bir şekilde karşılıklı konuşmayı teşvik etmeyi içerir. "Beyin fırtınası" terimi genellikle her tür grup tartışmasını içeren geniş anlamda kullanılır. Bununla birlikte, gerçek bir beyin fırtınası katılımcıların yaratıcı hayal güçlerinin gruptaki diğer kişiler tarafından harekete geçirilmesini güvence altına almaya çalışan özel teknikleri içerir.

Bu teknikte grubun etkin olarak yönlendirilmesi çok önemlidir ve başlangıçta görüşlerin açıklanmasını sağlayıcı teşvikler, grubu düzenli olarak konu ile ilgili diğer alanlara yöneltmek ve genellikle sıcak tartışmalarla ortaya çıkan sorunların belirlenmesini içerir.

##### B.1.2 Kullanım

Beyin fırtınası aşağıda açıklanan diğer risk değerlendirme yöntemleri ile birlikte uygulanabilir ya da, risk yönetimi proseslerinin herhangi bir anında ve bir sistemin yaşam döngüsünün herhangi bir aşamasında yaratıcı düşünceyi teşvik etmek amacı ile yalnız başına kullanılabilir. Beyin fırtınası, sorunların belirlenmesi için gerçekleştirilen üst seviye tartışmalarda, ayrıntılı gözden geçirmelerde veya belirli sorunları daha ayrıntılı vermek için kullanılabilir.

Beyin fırtınası hayal gücünün çalıştırılmasına önem verir. Bu nedenle, özellikle yeni teknoloji risklerinin belirlenmesi gibi yeterli verinin bulunmadığı veya sorunlara bilinen çözümlerin dışında, alışılmadık yöntemler bulunması için çok faydalıdır.

##### B.1.3 Girdiler

Değerlendirilen kuruluş, sistem, proses veya uygulama hakkında bilgi sahibi bir ekip.

##### B.1.4 Proses

Beyin fırtınası yapılandırılmış veya yapılandırılmamış biçimde düzenlenebilir. Yapılandırılmış beyin fırtınası, katılımcıların önceden hazırlandığı, oturumun belirli bir amacı olduğu, ortaya konan fikirlerin değerlendirilerek bir çıktıya dönüştürüldüğü kurallara bağlılığı fazla olan bir beyin fırtınası türüdür. Yapılandırılmamış beyin fırtınası, daha az kuralları olan ve genellikle daha plansız şekilde gerçekleşir.

Yapılandırılmış bir proses içerisinde aşağıdaki özellikler bulunur:

- Oturum yöneticisi, oturumdan önce kapsama uygun olarak konu ile ilgili düşünmeye sevk edecek doğrultuda hazırlık yapar,
- Oturumun hedefi tanımlanır ve kurallar açıklanır,
- Oturum yöneticisi, oturumu bir düşünce zemini oluşturarak başlatır ve katılımcılar olabildiğince çok konuyu açıklayan düşünceleri açığa vurmaya çalışırlar. Bu aşamada, bulguların konu listesine eklenip eklenmemesine ilişkin henüz bir tartışma oluşmaz veya serbest fikir dolaşımını engelleyebileceğinden, belirli bir cümle ile neyin kastedildiği araştırılmaz. Tüm girdiler kabul edilir ve hiçbirini eleştirilmez ve grup yan fikirlerin oluşabilmesi için hızla yeni düşünceleri tetiklemeye yönelir,
- Oturum yöneticisi, bir yöndeki fikir üretimi tükendiği veya tartışma amacından çok uzaklaştığı zaman katılımcıları başka bir alana yönlendirebilir. Ancak asıl amaç, mümkün olduğunca fazla ve farklı fikirleri daha sonra analiz etmek üzere derlemektir.

##### B 1.5 Çıktılar

Çıktılar, uygulandıkları risk yönetim prosesinin adımına bağlıdır. Örneğin, risk belirleme aşamasında çıktılar risklerin ve mevcut kontrollerin listesi olabilir.

##### B 1.6 Güçlü yanlar ve kısıtlar

Beyin fırtınasının güçlü yanları:

- Yeni riskleri belirlemede ve alışılmadık çözümler üretmede yardımcı olan hayal gücünü teşvik eder,
- Başlıca paydaşları içerdiğinden genel iletişimin artırılmasına katkı sağlar,
- Kurgulanması nispeten daha hızlı ve kolaydır.

**Kısıtları:**

- Katılımcılar yetersiz beceri ve bilgi seviyesi nedeni ile etkin katkı yapamayabilirler,
- Göreceli olarak fazla yapılandırılmadığından, konunun tamamen kapsandığının, diğer bir deyişle, tüm risklerin belirlendiğinin gösterimi güç olabilir,
- Bazı grup dinamikleri nedeniyle, değerli fikirlerin sessiz kalabildiği aynı zamanda diğer katılımcıların daha baskın olarak görüş sunmaları ortaya çıkabilir. Sohbet forumu veya nominal grup tekniği aracılığı ile bilgisayar ortamında beyin fırtınası gerçekleştirilerek bunun üstesinden gelmek mümkün olabilir. Bilgisayar ortamında beyin fırtınası hazırlanacak anonim bir şekilde kurgulanabilir böylelikle fikirlerin serbest dolaşımını engelleyebilecek kişisel ve politik konular açığa çıkmadan tartışılabilir. Nominal grup tekniğinde fikirler moderatöre isim verilmeksizin sunulur ve sonradan grup olarak tartışılır.

**B.2 Yapılandırılmış veya yarı-yapılandırılmış görüşmeler****B.2.1 Genel**

Yapılandırılmış görüşmelerde, görüşülen bireylerin duruma farklı bir açıdan bakmalarını teşvik edecek önceden hazırlanmış bir soru seti yöneltilir ve böylece risklerin bu açıdan belirlenmesi sağlanır. Yarı yapılandırılmış görüşmeler de benzer şekildedir ancak, karşılıklı konuşmalara daha fazla serbestlik tanınarak önerilen konuların anlaşılması sağlanır.

**B.2.2 Kullanım**

Bir beyin fırtınası oturumu için insanları bir araya getirmenin zor olduğu veya grup içerisinde serbest görüş açıklamanın uygun olmayacağı kişilerin veya şartların bulunması halinde, yapılandırılmış ve yarı yapılandırılmış görüşmelerin kullanılması faydalıdır. Genellikle yapılandırılmış ve yarı yapılandırılmış görüşmeler, risklerin belirlenmesinde veya risk analizinin bir parçası olarak mevcut kontrollerin etkinliğinin değerlendirilmesi amacıyla kullanılır. Bu görüşmeler, bir projenin veya prosesin herhangi bir aşamasında uygulanabilir. Görüşmeler, risk değerlendirmelerine paydaş katkısı sağlamanın bir aracıdır.

**B.2.3 Girdiler**

Girdiler aşağıdakileri içerir:

- Görüşmelerin hedefinin açık tanımı,
- İlgili paydaşlar arasından seçilen katılımcıların bir listesi,
- Önceden hazırlanmış soru seti.

**B.2.4 Proses**

Konu ile alakalı soru seti, katılımcılara yol göstermek amacı ile hazırlanır. Sorular, mümkün olduğu durumlarda açık uçlu olarak hazırlanmalı, basit olmalı, katılımcının lisanına uygun olmalı ve sadece bir sorunu kapsamalıdır. İhtiyaç halinde konunun netleştirilmesi amacı ile ilave takip soruları da hazırlanmalıdır.

Daha sonra sorular ilgili anket katılımcısına yöneltilir. Daha fazla ayrıntı gerektiğinde sorular açık uçlu olarak sorulmalıdır. Katılımcıya yönlendirici etkide bulunmamak için dikkatli olunmalıdır.

Cevaplar, katılımcıya, ilerlemek istediği alanları keşfetme fırsatını vermek için, belirli bir esneklikte ele alınmalıdır.

**B.2.5 Çıktılar**

Çıktılar, anketlerin konusu olan soruna ait katılımcıların görüşünü yansıtır.

**B.2.6 Güçlü yanlar ve kısıtlar**

Yapılandırılmış anketlerin güçlü yanları:

- Yapılandırılmış anketler kişilere bir sorun hakkında dikkatli düşünebilmesi için zaman tanır;
- Birebir görüşmeler, bir sorunun daha ayrıntılı ele alınmasına imkân tanır;
- Yapılandırılmış anketler, gruba nispeten daha az katılımcılı beyin fırtınası toplantılarına kıyasla daha fazla kişinin katılmasına olanak sağlar;

Kısıtlar:

- Farklı görüşleri elde etmek oturum yöneticisi için zaman kaybettirici olur;
- Önyargılar tolere edilir ve grup görüşmelerinde taraflı yargılar ortadan kaldırılamaz,
- Beyin fırtınasının bir özelliği olan hayal gücünün tetiklenmesi mümkün olmayabilir.

## B.3 Delphi tekniđi

### B.3.1 Genel bakış

Delphi tekniđi bir grup uzmanın bir fikir üzerinde uzlařmalarını güvenilir řekilde elde etmek amacı ile uygulanan bir prosedür. Günümüzde daha geniş anlamda beyin fırtınası için kullanılmasına rağmen, Delphi tekniđinin orijinal olarak formüle edilen řekliyle zorunlu özelliđi, proses ilerledikçe, uzmanların kendi görüşlerini bireysel ve anonim olarak açıklarken diđer görüşlere de erişebilmeleridir.

### B.3.2 Kullanım

Delphi tekniđi, risk deđerlendirme prosesinin herhangi bir ařamasında veya sistem yařam döngüsünün herhangi bir safhasında, uzmanların fikir birliđinin gerekli olduđu durumlarda uygulanabilir.

### B.3.3 Girdiler

Fikir birliđine ihtiyaç duyulan farklı görüşler.

### B.3.4 Proses

Bir grup uzmana, yarı-yapılandırılmıř anket soruları yöneltilir. Uzmanlar fikirlerinin bađımsız kalmalarını sađlamak için bir araya gelmezler.

Prosedür ařađıdaki řekildedir:

- Delphi sürecini izlemek ve yönetmek için bir takım oluřturulması,
- Uzman grubunun sečilmesi (bir veya birden fazla uzman paneli oluřturulabilir),
- İlk tur anketinin hazırlanması,
- Anketin denenmesi,
- Panel katılımcılarına soruların bireysel olarak iletilmesi,
- İlk tur cevaplarından gelen bilgilerin analizi edilmesi, derlenmesi ve panel katılımcılarına iletilmesi,
- Katılımcılardan görüşlerin alınması ve bir uzlařma sađlanana kadar prosesin tekrarı řekindedir.

### B.3.5 Çıktılar

Mevcut konu hakkında uzlařma dođrultusunda bir araya gelme.

### B.3.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar:

- Görüşlerin kimlik belirtilmeksizin iletilmesi sayesinde önceden ilgi çekmemiř fikirlerin açıklanması ihtimali artar,
- Tüm görüşler eřit ađırlıktadır, bu da baskın kiřilikler ile ilgili problemini engeller,
- Çıktıların sahiplenilmesi sađlanır,
- Kiřilerin aynı yerde, aynı zamanda bir araya getirilmeleri gerekli deđildir.

Kısıtlar:

- Yođun emek ve zaman gerektirir,
- Katılımcılar, kendilerini yazılı olarak açık bir řekilde ifade edebiliyor olmalıdır.

## B.4 Kontrol listeleri

### B.4.1 Genel

Kontrol listeleri, genellikle geçmiř arızalar sonucunda veya önceki risk deđerlendirmeleri sonucunda ortaya çıkmıř ve deneyimlerle oluřturulmuř tehlikeler, riskler veya kontrol yetersizliklerini içeren listelerdir.

### B.4.2 Kullanım

Kontrol listesi, tehlikeleri ve riskleri belirlemek veya kontrollerin etkinliđini deđerlendirmek için kullanılır. Bir ürün, proses veya sistemin yařam döngüsünün herhangi bir ařamasında kullanılabilir. Diđer risk deđerlendirme tekniklerinin bir parçası olarak kullanılabilir, ancak yeni problemleri tanımlayan daha yaratıcı bir teknikle her türlü çözümün kapsandıđını kontrol amacı ile kullanmak en faydalı olandır.

### B.4.3 Girdiler

İlgili ve tercihan geçerli kılınmıř bir kontrol listesinin seçilebilmesi veya oluřturulabilmesi için ön bilgiler ve konuya iliřkin uzmanlık.

#### B.4.4 Proses

Prosedür aşağıdaki şekildedir:

- Gerçekleştirilecek etkinliğin kapsamının belirlenmesi,
- Kapsamı yeterli derecede içerecek bir kontrol listesi seçilir. Kontrol listeleri ihtiyaca göre dikkatlice seçilmelidir. Örneğin, standart kontrollerin bir listesi, yeni tehlikelerin veya risklerin belirlenmesi için kullanılamaz.
- Kontrol listesini kullanacak kişi veya takım listeyi kullanarak proses veya sistemin her parçasını adım adım takip eder ve listede mevcut olup olmadığını gözden geçirir.

#### B.4.5 Çıktılar

Çıktılar, risk yönetim prosesinin hangi aşamasında uygulandığına bağlıdır. Örneğin, çıktılar yetersiz kontrollerin bir listesi veya risklerin listesi olabilir.

#### B.4.6 Güçlü yanlar ve kısıtlar

Kontrol listelerinin güçlü yanları:

- Uzman olmayan kişiler tarafından kullanılabilir;
- İyi tasarlandığı zaman, geniş çaplı uzman görüşlerini kolay kullanılabilir bir sistem içine dâhil eder;
- Bilinen ortak sorunların unutulmamasını güvence altına alır.

Kısıtlar:

- Risk belirlemede hayal gücünü sınırlandırır,
- Bilinmediği bilinenleri değil, bilindiği bilinenleri kapsamaktadır,
- Kutu işaretleme (dikkatsiz kontrol) davranışını teşvik eder,
- Doğrudan gözlem tabanlı olduğundan kolayca görülemeyenleri gözden geçirir.

### B.5 Başlangıç tehlike analizi (PHA)

#### B.5.1 Genel

PHA; verilen bir faaliyet, yerleşke veya sistem için tehlike veya tehlikeli durum yaratabilecek olayları ve durumları belirleme amacı olan, basit ve tümevarım tabanlı bir analiz metodudur.

#### B.5.2 Kullanım

Genellikle, proje başlangıçları gibi tasarım ayrıntı bilgisinin ya da çalışma prosedürlerinin çok az olduğu projelerin ön geliştirme aşamasında kullanılır. Çoğunlukla, hazırlık çalışması olarak daha ileri düzey çalışmalar veya sistem tasarım özellikleri için gerekli bilgiyi sağlar. Aynı zamanda, mevcut sistemleri tehlikeleri önceliklendirme amacı ile analiz ederken ya da şartların daha geniş bir teknik kullanımına elvermediği zamanlarda kullanışlı olabilir.

#### B.5.3 Girdiler

Girdiler aşağıdakileri içerir:

- Değerlendirilecek sistem hakkında bilgi,
- Mevcut ve ilgili olan sistem tasarım ayrıntıları.

#### B.5.4 Proses

Bir tehlike listesi ve genel tehlike durumları ile birlikte riskler, aşağıdaki ayırt edici özellikler göz önünde bulundurularak formüle edilir:

- Kullanılan veya üretilen malzemeler ve bunların reaktiflikleri,
- Kullanılan donanım,
- İşletme ortamı,
- Yerleşim planı,
- Sistem parçaları arasındaki arayüzler, vb.

Risklerin belirlenmesinde ileri değerlendirme için, istenmeyen bir olayın sonuçlarının kalitatif analizi ve olasılıklarının hesaplanması yapılabilir.

Yeni tehlikelerin belirlenmesi ve gerektiğinde iyileştirmelerin yapılabilmesi için PHA, tasarım, inşaat ve testlerin farklı aşamalarında güncellenmelidir. Elde edilen sonuçlar, tablolar veya ağaç yapıları şeklinde sunulabilir.

**B.5.5 Çıktılar**

Çıktılar aşağıdakileri kapsar:

- Tehlikeleri ve riskleri içeren bir liste,
- Kabul, önerilen kontroller, tasarım özellikleri veya daha ayrıntılı değerlendirme şeklinde yapılacak öneriler.

**B.5.6 Güçlü yanlar ve kısıtlar**

Güçlü yanlar:

- Sınırlı bilgi olduğu zamanda bile kullanılabilir
- Sistem yaşam döngüsünün en erken safhalarında, risklerin göz önünde bulundurulmasını sağlar.

Kısıtlar:

- PHA sadece bir ön bilgi sağlar, kapsamlı olmadığı gibi riskler ve nasıl engellenebilecekleri hakkında ayrıntılı bilgi sağlamaz.

**B.6 HAZOP Tehlike ve işletilebilme****B.6.1 Genel**

HAZOP, **HAZ**ard (tehlike) ve **OP**erability (işletilebilirlik) kelimelerinin kısaltılmış halidir; planlanan ya da mevcut olan ürün, proses, prosedür veya sistemin yapılandırılmış ve sistematik bir incelemesidir. İnsanlar, donanım, çevre ve/veya kurumsal hedefler üzerindeki riskleri belirlemek için kullanılan bir tekniktir. Mümkün olduğu durumlarda, inceleme ekibinden riski iyileştirmek için çözüm sunması beklenir.

HAZOP prosesi, kalitatif bir teknik olup, tasarım, proses, prosedür veya sistemin her aşamasında, tasarım amacının veya işletme koşullarının nasıl sağlanamayacağını sorgulayan rehber kelimeleri temel alarak kullanılan bir tekniktir. Genellikle, farklı disiplinlerden oluşturulmuş bir ekip katılımıyla gerçekleştirilen bir dizi toplantı ile yürütülür.

HAZOP, FMEA'da olduğuna benzer şekilde, proses, sistem veya prosedürlerde bulunabilecek hata türlerinin ve sonuçlarının belirlendiği bir yöntemdir. FMEA'da doğrudan hata türlerinin belirlenmesi ile başlanırken, ekip burada farklı olarak, istenmeyen sonuçları, beklenen sonuçlardan sapmaları ve muhtemel nedenler ve hata türlerinin ardında bulunan koşulları ve faaliyetleri göz önünde bulundurur.

**B.6.2 Kullanım**

HAZOP tekniği ilk olarak kimyasal proses sistemleri için geliştirilmiş olmakla birlikte, daha sonra farklı türlerdeki sistemler ve karmaşık işlemlerde kullanılmak üzere genişletilmiştir. Bu türler; mekanik ve elektronik sistemleri, prosedürleri, yazılım sistemlerini, organizasyon yapısı değişimlerinden, yasal sözleşme tasarımları ve gözden geçirmelere kadar farklı konuları içermektedir.

HAZOP prosesi; tasarımda, parçalarda, planlanmış prosedürlerde ve insan faaliyetlerindeki eksikliklerden kaynaklanabilecek, tasarım amacına ters düşen her tür sapmaya karşı kullanılabilir.

Bu teknik, yazılım tasarımının gözden geçirilmesinde geniş çaplı olarak kullanılır. Kritik güvenlik enstrümanların kontrolü ve bilgisayar sistemlerinde kullanıldığı zaman CHAZOP (**C**ontrol **HA**zards and **OP**erability Analysis or computer hazard and operability analysis) olarak bilinir.

Bir HAZOP çalışması, genellikle ayrıntı tasarım aşamasında, istenen in bütün akış şemasının mevcut olduğu, ancak hala tasarımda değişiklik yapılabilecek aşamada başlatılır. Bununla birlikte, tasarım ayrıntıları belli oldukça farklı aşamalara bölünmüş bir yaklaşımla, her aşamada farklı kılavuz kelimelerle birlikte yürütülebilir. Bir HAZOP çalışması işletim süresince de yürütülebilir ancak gerekli değişiklikleri yapmak çok maliyetli olabilir.

**B.6.3 Girdiler**

HAZOP için gerekli girdiler; sistem hakkında güncel bilgi, gözden geçirilecek proses veya prosedür ve tasarım ve performans şartlarını içerir. Çizimler, şartnameler, akış şemaları, proses kontrol ve mantık diyagramları, yerleşim çizimleri, işletme ve bakım prosedürleri ile acil durum prosedürleri girdi olarak kullanılabilir. Donanım ile ilgili olmayan HAZOP çalışmalarında girdi; fonksiyon ve inceleme altındaki sistemin parçalarını açıklayan herhangi bir belge olabilir. Örneğin, görev tanımları ve organizasyon şemaları, sözleşme tasarımları veya prosedür tasarımları dahi girdi olabilir.

**B.6.4 Proses**

HAZOP, "tasarım" ve incelenecek proses, sistem veya prosedür özelliklerini ele alıp her parçasını gözden geçirerek, ne tür performans sapmalarına yol açabileceğini, bu sapmaların ne tür neden ve muhtemel sonuçları

olabileceğini bulmaya çalışır. Bu da sistemin, prosesin veya prosedürün her bir parçasının anahtar parametrelerdeki değişime nasıl tepki vereceği, uygun anahtar kelimelerin uygulanması ve sistematik olarak incelenmesi ile elde edilir. Anahtar kelimeler belirli bir sistem, proses veya prosedüre uyarlanabilir ya da her türlü farklılaşmayı içerecek genel kelimeler kullanılabilir. Çizelge B.1 teknik sistemlerde genel olarak kullanılan anahtar kelimeleri göstermektedir. Benzer şekilde, “çok erken”, “çok geç”, “çok fazla”, “çok az”, “çok uzun”, “çok kısa”, “yanlış yön”, “hatalı hedef”, “yanlış faaliyet” gibi anahtar kelimeler, insan hatalarını belirlemede kullanılabilir.

HAZOP incelemesinin içerdiği normal adımlar:

- HAZOP çalışmasını yürütecek ve bu çalışmada ortaya çıkabilecek her türlü sorunun çözülmesini güvence altına alacak, yetkili ve sorumlu kişinin aday gösterilmesi,
- İncelemenin kapsam ve hedeflerinin tanımı,
- İnceleme için anahtar ya da rehber kelime setinin hazırlanması,
- HAZOP inceleme ekibinin belirlenmesi ki genellikle bu ekip, mevcut veya istenen tasarımda oluşabilecek sapmaların etkisini değerlendirebilecek yeterli teknik uzmanlığa sahip, farklı uzmanlık alanlarından, tasarım ve işletim personelinin oluşturulur.
- Gerekli belgelerin toplanması.

İnceleme ekibi ile oluşturulan çalıştayda:

- Proses, prosedür veya sistemi daha küçük alt parçalara, alt sistemlere ya da alt proseslere ayırarak, gözden geçirmenin somutlaştırılması,
- Her alt sistem, alt proses veya alt parça için tasarımın amacı üzerinde anlaşmama sağlandıktan sonra, anahtar kelimeleri bir biri ardına alt sistem veya parçaya uygulamak sureti ile istenmeyen sonuçlara neden olabilecek muhtemel sapmaları varsaymak,
- İstenmeyen bir durum belirlendiğinde, her durum için neden ve sonuçlar üzerinde anlaşma sağlanarak oluşmalarını engellemek veya oluştuğlarında zararlı sonuçlarından korunabilmek için nasıl iyileştirileceklerine dair öneri getirmek,
- Görüşmeleri belgelemek ve belirlenen risklere özel iyileştirme çalışmaları üzerinde anlaşma sağlamak.

**Çizelge B.1 - Kullanılabilecek HAZOP anahtar kelimelerine örnekler**

Terimler	Tanımlar
Hayır veya yok	İstenen sonucun hiçbir bölümü elde edilemedi veya istenen şartlar mevcut değil
Daha fazla (daha yüksek)	Çıktıların miktarında veya işletim koşullarında artış
Daha az (daha düşük)	Miktarda azalma
İlaveten	Miktar artışı (Örneğin, ilave malzeme)
Bir parçası/kısmen	Miktarda azalma (Örneğin, bir karışımın bir veya iki bileşeni)
Tersi/zıddı	Karşıt (Örneğin, ters akış)
Farklı şekilde	İstenen sonuç elde edilemedi veya tamamen farklı bir şey gerçekleşti (Örneğin, hatalı akış ya da hatalı malzeme)
Uyumluluk	Malzeme, ortam
Kılavuz kelimeler aşağıdakilere benzer parametrelere uygulanırlar:	
Bir malzeme veya prosesin fiziksel özellikleri	
Isı, hız gibi fiziksel şartlar	
Bir sisteme ait parça hakkında belirlenmiş amaç (örneğin, bilgi transferi)	
İşletim yönleri	

### B.6.5 Çıktılar

Her inceleme noktasına ait bulguların kaydedildiği HAZOP toplantılarının tutanakları. Kullanılan anahtar kelimeler, sapmalar, muhtemel nedenler, tespit edilen problemler için belirlenen faaliyetler ve faaliyetlerden sorumlu kişiler tutanak içeriklerinde yer almalıdır.

Düzeltilenmeyen herhangi bir sapma için bu sapmanın riski değerlendirilmelidir.

### B.6.6 Güçlü yanlar ve kısıtlar

Bir HAZOP analizi aşağıdaki faydaları sağlar:

- Bir sistem, proses ya da prosedürü, bütünsel olarak inceleme imkânı sağlar,
- Gerçek işletim deneyimi olan ve iyileştirme çalışmalarını uygulayacak farklı alanlardaki uzmanların bir araya geldiği ekiplerden oluşur,

- Risk iyileştirme faaliyetleri ve çözümleri üretir,
- Farklı yapılarıdaki sistem, proses ve prosedürlere uygulanabilir,
- İnsan hatalarının nedenleri ve sonuçlarının belirgin şekilde göz önünde bulundurulmasına izin verir,
- Süreçte gerekli özenin gösterildiğini ifade eden yazılı kayıtlar üretir.

#### Kısıtlar:

- Detaylı bir analiz çok zaman alabilir, dolayısı ile pahalı olabilir,
- Detaylı bir analiz, geniş içerikli dokümantasyon, sistem/proses ve prosedür özellikleri gerektirir,
- En temel varsayımların sorgulanması yerine, ayrıntılı çözümler bulmaya odaklanabilir (bununla birlikte, bu kısıt aşamalı yaklaşımla engellenebilir),
- Tartışmalar, daha kapsamlı veya dış sorunlar yerine, önemsiz ayrıntılara odaklanabilir,
- Ekibe verilen hedef ve kapsam ile taslak tasarım ve tasarımın amacı ile sınırlıdır,
- Proses, kendi tasarımlarında sorun bulabilecek yeterli tarafsızlığa sahip bulunmayan tasarımcıların uzmanlığına bağlıdır.

### B.6.7 Referans doküman

*IEC 61882, Tehlike ve işletilebilme çalışmaları (HAZOP çalışmaları) – Uygulama rehberi*

## B.7 Tehlike analizi ve kritik kontrol noktaları (HACCP)

### B.7.1 Genel

Tehlike analizi ve kritik kontrol noktaları (HACCP), bir ürüne ait güvenlik ve güvenilebilir kalitenin devam ettirilebilmesi için tehlikelerin belirlenmesi ve kontrollerin proseslerin gerekli noktalarına konulması için bir yapı sağlar. HACCP, risklerin minimize edilmesi için kontrollerin varlığını, sadece son ürünün incelenmesi yerine, prosesin tamamını kapsayacak şekilde inceler.

### B.7.2 Kullanım

HACCP, NASA uzay programında gıda kalitesi güvencesini sağlamak amacı ile geliştirilmiştir. Günümüzde, gıdalardaki fiziksel, kimyasal veya biyolojik kirleticilerin oluşturacağı riskleri kontrol etmek amacıyla, gıda zincirinin her hangi bir konumunda faaliyet gösteren organizasyonlar tarafından kullanılmaktadır. Aynı zamanda, tıbbi cihazlar ve farmakolojik ürün üreticileri tarafından da kullanılması için genişletilmiştir. Ürün kalitesini etkileyebilecek hususların belirlenmesi ve kritik parametrelerin izlenebileceği noktaların tanımlanması prensibi, başka teknik sistemler için de genelleştirilebilir.

### B.7.3 Girdiler

HACCP, ürünün kalite, güvenlik ya da güvenilirliğini veya proses çıktısını etkileyebilecek tehlikeler hakkında bilginin yanında, temel akış diyagramı veya proses diyagramı ile başlar. Tehlikeler ve tehlikelerden kaynaklı risklerin yanı sıra bunları kontrol edilebilme yöntemleri hakkındaki bilgiler, HACCP'ye girdi teşkil eder.

### B.7.4 Proses

HACCP, aşağıdaki yedi prensipten oluşur:

- Tehlikeleri ve bu tehlikeleri önleyici tedbirleri belirler,
- Proses içinde, tehlikelerin kontrol veya bertaraf edilebileceği noktaları (kritik kontrol noktaları veya CCP) belirler,
- Tehlikelerin kontrol edilmesinde gereken kritik sınırları oluşturur, örneğin her kritik kontrol noktasının, tehlikeyi kontrol edebilmesi için belirli parametreler dâhilinde çalışması gerekir,
- Her bir kritik kontrol noktası için kritik limitleri belirler, başka bir deyişle tanımlanan sınırlar içerisinde bulunduğunu izler,
- Prosesin belirlenen sınırlar dışına çıkması durumları için düzeltici faaliyetler oluşturur,
- Doğrulama prosedürlerini oluşturur,
- Her adım için kayıt altına alma ve dokümantasyon prosedürlerini uygular.

### B.7.5 Çıktılar

HACCP planı ve tehlike analiz çalışma sayfalarını içeren dokümanite edilmiş kayıtlar.

Tehlike analiz çalışma sayfaları, prosesin her adımını listeler:

- Bu adımda oluşabilecek, kontrol edilebilecek ya da artabilecek tehlikeler,
- Tehlikelerin önemli bir riske yol açıp açmayacağı (deneyimler, veriler ve teknik literatür temel alınarak elde edilmiş, sonuçlar ve olasılıklar göz önünde bulundularak),
- Önemli sayılmanın gerekçeleri,
- Her bir tehlike için olası önleyici faaliyetler,
- İzleme ve kontrol önlemlerinin bu aşamada uygulanıp uygulanamayacağı (adımın CCP olup olmadığı)



HACCP planı, belirli bir tasarım, ürün, proses veya prosedüre ait kontrolü güvence altına almak için izlenmesi gereken işlemleri tarif eder. Plan, tüm CCP'lerin bir listesini ve her bir CCP için aşağıdakileri içerir:

- Önleyici tedbirlerin kritik limitlerini,
- İzleme ve sürekli kontrol faaliyetlerini (neyin, nasıl, ne zaman izleneceği ve izlemenin kim tarafından yapılacağı dâhil)
- Kritik limitlerden uzaklaşıldığı tespit edildiğinde gerçekleştirilmesi gereken düzeltici faaliyetler,
- Doğrulama ve kayıt altına alma işlemleri.

### B.7.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar:

- Kalite kontrolü için dokümanite edilmiş kanıt sağlayan, aynı zamanda risklerin belirlenmesini ve azaltılmasını sağlayan yapılandırılmış bir proses,
- Bir proseste risklerin ve tehlikelerin nasıl ve nerede engellenebileceği ve kontrol edilebileceği hakkında uygulamaya odaklanma,
- Son ürün incelemesine güvenmek yerine sürecin tamamında daha iyi risk kontrolü;
- İnsan faaliyetleriyle ortaya çıkan tehlikelerin belirlenmesi ve bunların oluştuğu noktada ve sonrasında nasıl kontrol edilebileceği.

Kısıtlar:

- HACCP; tehlikelerin belirlenmesini, tehlikelerin yol açtığı risklerin tanımlanmasını ve bunların prosese girdi olarak önemini anlaşılmasını gerektirir. Uygun kontrollerin tanımlanması da ayrıca gerekir. Bunlar, kritik kontrol noktalarının ve kontrol parametrelerinin HACCP sürecinde belirlenmesi için gerekir ve sonucun elde edilmesi için bunların başka araçlarla birleştirilmesine ihtiyaç duyulabilir,
- Kontrol parametrelerinin tanımlanmış limitleri geçmesi durumunda uygun faaliyetin gerçekleştirilmesi şeklindeki uygulamada istatistiksel olarak önemli olan kontrol parametrelerindeki tedrici değişim fark edilmeyebilir.

### B.7.7 Kaynak doküman

*ISO 22000, Gıda güvenliği yönetimi sistemi - Gıda zincirindeki tüm kuruluşlar için şartlar*

## B.8 Zehirlilik değerlendirme

### B.8.1 Genel

Bu bölümde, bir dizi çevresel tehlikelere maruz kalma sonucu bitkilere, hayvanlara ve insanlara karşı oluşabilecek risklerin değerlendirilmesi için izlenen prosesi kapsamak üzere çevresel risk değerlendirme kullanılmaktadır. Risk yönetimi; risk kıyaslamayı ve risk iyileştirmeyi de kapsayan karar verme adımlarına atıf yapmaktadır.

Bu yöntem, tehlike veya zarar kaynağını, hedef kitleyi nasıl etkileyeceği ve tehlikeye açık hedef kitleye zararın ulaşabileceği yolların incelenmesini içerir. Elde edilen bu bilgiler daha sonra, zararın olası boyutu ve doğası hakkında bir tahminde bulunmak üzere birleştirilir.

### B.8.2 Kullanım

Bu proses, kimyasallar, mikro-organizmalar ve diğer türler gibi tehlikelere maruz kalma sonucunda, bitkiler, hayvanlar ve insanlara karşı oluşabilecek risklerin değerlendirilmesi için kullanılır.

Patika analizi gibi, bir hedefin maruz kaldığı risk kaynağına ulaşabilecek farklı yolların araştırılması şeklinde yöntemin farklı bakış açıları, insan sağlığı ve çevre dışında, farklı risk alanları için geniş çapta uyarlanıp kullanılabilir ve riski azaltmak için kullanılacak iyileştirmelerin belirlenmesinde kullanışlıdır.

### B.8.3 Girdiler

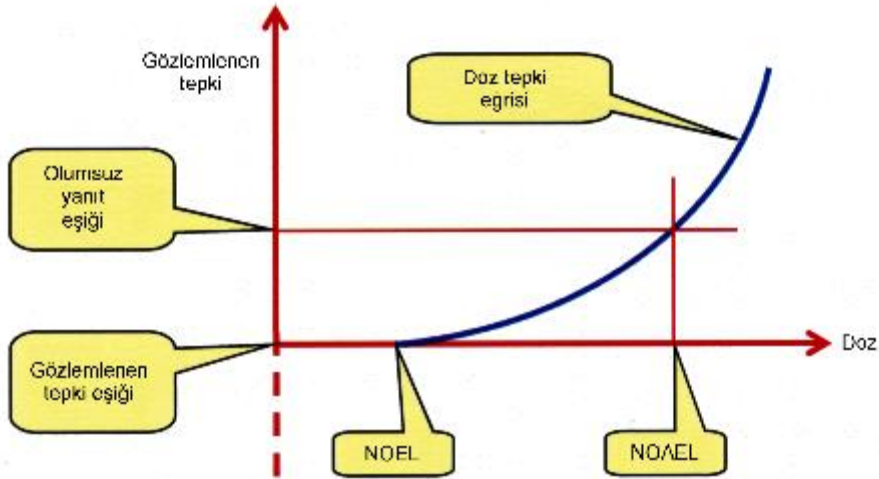
Bu yöntem, tehlikelerin doğası ve özellikleri, hedef kitlenin duyarlılığı ile bu ikisinin nasıl etkileşeceği hakkında doğru veri gerektirir. Bu veri normal olarak, epidemiyolojik girdi veya laboratuvar araştırmalarını temel alır.

### B.8.4 Proses

Prosedür aşağıdaki şekildedir:

- a) Problemin formüle edilmesi - bu adım, ilgi alanındaki hedef kitlenin ve tehlike türlerinin tanımlanmasıyla değerlendirme kapsamının belirlenmesini içerir,

- b) Tehlike tanımlama – bu adım, çalışma kapsamındaki tehlikelerden hedef kitleye gelebilecek her türlü olası zararın kaynağının belirlenmesini içerir. Tehlike tanımlama, genellikle uzman deneyimlerine ve yazılı kaynakların incelenmesine dayanır.
- c) Tehlike analizi – bu adım, tehlikenin doğasının ve hedef ile nasıl bir etkileşimde bulunacağını anlamasını içerir. Örneğin, insanların kimyasal etkilere maruz kalması göz önünde bulundurulurken tehlikenin, akut ve kronik zehirlilik içerebileceği, DNA'lara hasar verme olasılığı veya kansere ya da doğum kusurlarına yol açma ihtimalini de içerir. Her bir tehlike etkisi için, etkinin büyüklüğü (tepki), hedefin maruz kaldığı tehlike (doz) ile karşılaştırılır ve mümkün olan yerlerde, etkinin hangi mekanizmalarla oluşturulduğu belirlenir. Görünür bir etkinin bulunmadığı seviyeler (NOEL) ve görünür istenmeyen bir etkinin bulunmadığı (NOAEL) seviyeler belirlenir. Bunlar bazı durumlarda kabul edilebilir risk kriterleri olarak kullanılır.



**Şekil B.1 - Doz - tepki eğrisi**

Kimyasal etkiler için, Şekil B.1'dekine benzer doz-tepki eğrisini oluşturmak için test sonuçları kullanılır. Bunlar genellikle hayvanlar üzerinde yapılan deney sonuçlarından ya da kültür doku veya hücreler gibi deneysel sistemlerden elde edilir.

Mikro organizmalar veya yerel olmayan türlerle ilgili tehlikelerin etkileri saha verisi ve epidemiolojik çalışmalardan elde edilir. Hastalıkların veya zararlıların belirlenmiş hedef üzerindeki etkileşimi belirlenir ve belirgin bir tehlikeye açıklık nedeni ile oluşabilecek belirli bir zarar seviyesi tahmini yapılır.

- d) Riske maruz kalma (riske açıklık) analizi – bu adımda, zararlı bir maddenin veya kalıntılarının hassas bir hedefe nasıl ve ne miktarda ulaşacağı incelenir. Genellikle, tehlikenin oluşturacağı farklı yollar, hedefe ulaşırken karşılaşacağı engeller ve maruz kalınan risk seviyesini etkileyen kaynakların incelenmesi şeklinde uygulanan iz analizi ile gerçekleştirilir. Örneğin, kimyasal spreyleme ile ilgili riskleri göz önünde bulundururken, riske maruz kalma analizi, ne miktarda kimyasalın püskürtüldüğü, hangi yollarla ve hangi şartlar altında yapıldığı, hayvanların veya insanların bu tehlikeye doğrudan maruz kalıp kalmadıkları, bitkilerin hayatları boyunca üzerlerinde ne kadar kalıntı kalacağı, toprağa karışan zararlı ilaçlarının çevresel etkileri, hayvanlar üzerinde birikip birikmeyeceği, yer altı sularına karışıp karışmayacağı göz önünde bulundurulur. Biyolojik güvenlik için, iz analizi, ülkeye dışardan gelen böceklerin nasıl çoğalıp, çevreye yayılacağı da göz önünde bulundurulabilir.
- e) Risk karakterizasyonu – bu adımda, tehlike analizinden ve riske maruz kalma analizinden elde edilen bilgiler bir araya getirilerek, tüm patikalardan (yol) gelen belirli sonuçlar birleştirilerek olasılıkları tahmin edilmeye çalışılır. Çok fazla tehlike ve patikalar bulunduğu durumlarda, başlangıç aşamasında bir filtreleme gerçekleştirilerek, ayrıntılı tehlike ve riske maruz kalma analizleri daha üst düzey risk senaryolarında ele alınır.

### B.8.5 Çıktılar

Çıktı genellikle, ilgili kapsamda belirli bir hedefin belirli bir tehlikeye maruz kaldığı risk seviyesinin bir göstergesidir. Risk, kalitatif (nitelik yönünden), yarı-kalitatif veya kantitatif (sayısal olarak) olarak ifade edilebilir.

Örneğin, kanser riski genellikle, bir kişide belirli bir zaman aralığı içerisinde, belirli miktarda maruz kalınan kirleticiler nedeni ile kanser oluşabilmesi, olasılık şeklinde kantitatif olarak ifade edilir. Yarı-kantitatif analiz, belirli bir kirletici veya zararlı haşerat için risk endeksi oluşturmak amacı ile kullanılabilir, kalitatif çıktı ise riskin bir seviyesi (yüksek, orta, düşük vb.) veya olası etkilerin gerçekçi verilerle bir tarifi şeklinde olabilir.

### B.8.6 Güçlü yanlar ve kısıtlar

Bu analizin güçlü yanları, problemin doğasının ve riski artıran etkenlerin anlaşılmasını sağlayan bilgiyi çok ayrıntılı olarak sunmasıdır.

Patika analizi; kullanışlı bir yöntem olup genellikle, tüm risk alanları için kontrollerin nerelerde ve nasıl geliştirilebileceği veya yenilerinin tanımlanabileceği konusunda imkân sağlar.

Diğer taraftan bu yöntemde, çoğu zaman mevcut olmayan tam ve doğru veriye ihtiyaç vardır veya ilgili verilerde yüksek seviyede belirsizlik bulunur. Örneğin, yüksek dozda tehlikeye maruz bırakılan hayvanlardan elde edilen doz-tepki eğrilerinin, insanların maruz kalacağı çok düşük dozları tahmin etmek için ekstrapole edilmesi gerekir ve bunu elde etmek için birden fazla model mevcuttur. Etkilenecek hedefin insan yerine çevre olduğu ve tehlikenin kimyasal olmadığı durumlarda, çalışmanın özel koşulları ile doğrudan alakalı veriler sınırlı olabilir.

## B.9 Yapılandırılmış "Olursa Ne Olur" Tekniği (SWIFT)

### B.9.1 Genel

SWIFT tekniği ilk olarak, HAZOP çalışmasına daha basit bir alternatif olarak geliştirilmiştir. SWIFT; katılımcıların riskleri belirlemesini teşvik etmek amacıyla gerçekleştirilen bir çalıştay kapsamında bir yönetici tarafından kullanılan yönlendirici kelime ve ifadeler setinin kullanıldığı sistematik ve ekip çalışması bazlı bir çalışmadır. Yönetici ve ekip; normal işlem ve davranışlardan sapmalar olması halinde bu sapmalardan sistemin, tesisin, kuruluşun veya prosedürün, nasıl etkileneceğini incelemek amacıyla, standart "olursa ne olur" şeklinde ifade türleri kullanılır. SWIFT normalde, HAZOP'tan daha düşük bir ayrıntı seviyesinde, daha çok sistem seviyesinde uygulanır.

### B.9.2 Kullanım

SWIFT ilk olarak kimyasal ve petro-kimyasal tesislerde tehlike çalışması için tasarlanmıştır. Teknik son dönemde sistemler, üretim öğeleri, prosedürler ve kuruluşlara geniş ölçüde uygulanmaktadır. Bu teknik özellikle, değişikliklerin sonuçlarını ve değiştirilmiş veya yeni oluşturulmuş riskleri değerlendirmek için kullanılır.

### B.9.3 Girdiler

Sistem, prosedür, tesis ve/veya değişiklik, çalışma başlamadan önce dikkatli bir şekilde tanımlanmalıdır. İç ve dış içerik, ekip yöneticisinin karşılıklı görüşmeleri, dokümanların, planların ve çizimlerin incelenmesi ile oluşturulur. Normal olarak analiz prosesini kolaylaştırmak amacıyla, üzerinde çalışılacak öğeler, durum veya sistem anahtar elemanlara veya adımlara ayrılır, ancak bu durum nadiren HAZOP için gerekli olan tanımlama seviyesinde meydana gelir.

Diğer bir önemli girdi ise, özenle seçilmiş olması gereken çalışma ekibinin uzmanlığı ve deneyimidir. Tüm paydaşlar mümkünse, benzer öğeler, sistemler veya durumlar hakkında deneyimleri olan kişilerce temsil edilmelidir.

### B.9.4 Proses

Genel proses aşağıdaki şekilde işler:

- Çalışma başlamadan önce yönetici, bir standard setine dayanan veya tehlike ya da risklerin etrafıca gözden geçirilmesini mümkün kılan, uygun yönlendirici kelime ve ifadeler listesi hazırlar.
- Çalıştaylarda işlem, sistem, değişiklik veya duruma ait dış ve iç kaynaklar ve çalışmanın kapsamı tartışılır ve kararlaştırılır.
- Yönetici; katılımcılardan aşağıdakilere ait görüşlerini öne sürmelerini ve tartışmalarını talep eder:
  - Bilinen riskler ve tehlikeler,
  - Önceki deneyim ve olaylar,
  - Bilinen ve var olan kontroller ve tedbirler,
  - Düzenleyici şartlar ve kısıtlamalar.
- Tartışma; "Olursa Ne Olur" sorusu, yönlendirici kelimeler veya konu başlıkları sorularak kolaylaştırılır. "Olursa Ne Olur" ifadesi, "Farz edelim...", "Ya olursa...", "Birisine veya bir şeye... olması mümkün mü" veya "Herhangi biri veya bir şey hiç ... gerçekleştirmiş/ ya da etkilenmiş mi" sorularından

oluşabilir. Amaç çalışma ekibini, muhtemel senaryolar, bu senaryoların nedenleri, sonuçları ve etkilerini keşfetmeye teşvik etmektir.

- e) Riskler özetlenir ve çalışma ekibi yerinde kontrolleri gerçekleştirir.
- f) Riskin tanımı, riskin nedenleri, sonuçları ve beklenen kontroller çalışma ekibi tarafından onaylanır ve kaydedilir.
- g) Çalışma ekibi kontrollerin yeterli ve etkin olup olmadığını göz önünde bulundurur ve risk kontrol etkinliğine ilişkin bir beyan üzerinde mutabık kalır. Eğer bu beyan tatminkâr değilse, çalışma ekibi risk iyileştirme alanları ve mümkün olan kontrollerin tanımlanması üzerinde daha fazla düşünür.
- h) Görüşmeler sırasında, daha fazla "olursa ne olur" gibi sorular sorulmaya devam edilerek daha fazla risk tespit edilmeye çalışılır.
- i) Yönetici, tartışmayı izlemek ve çalışma ekibinin tartışabileceği ilâve konu ile senaryoları önermek için yönlendirici kelime ve ifadeler listesi kullanır.
- j) Öncelik açısından yapılacak faaliyetleri derecelendirmek için kalitatif veya yarı kantitatif risk değerlendirme yöntemleri kullanmak normaldir. Risk değerlendirmesi normalde mevcut kontrolleri ve bu kontrollerin etkinliğini göz önünde bulundurularak gerçekleştirilir.

### B.9.5 Çıktılar

Çıktılar, risk-derecelendirilmiş faaliyetler veya görevleri gösteren bir risk kaydı içerir. Bu görevler daha sonra bir iyileştirme planı için temel oluşturabilir.

### B.9.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar aşağıdaki konular içerir:

- Fiziki tesis veya sistem, durum ya da şartlar, kuruluş veya faaliyetin tüm formlarına geniş ölçüde uygulanabilir,
- Çalışma ekibi tarafından en az ön hazırlığı gerektirir,
- Nispeten süratlidir ve önemli tehlikeler ve riskler çalıştay çerçevesinde hızlıca görünür hale gelir,
- Çalışma "sistem odaklı"dır ve katılımcıların sadece parça arızalarının sonuçlarını incelemesi yerine sapsmalara karşı sistemin tepkilerine bakmalarına izin verir,
- Prosesler ve sistemler için iyileştirme fırsatlarını tanımlamak ve genellikle başarı olasılıklarını artıran faaliyetleri belirlemek amacıyla kullanılabilir,
- Mevcut kontrollerin ve ileri seviye risk iyileştirme faaliyetlerinden sorumlu olanların atölye çalışmasına katılmasını sağlayarak sorumluluklarını pekiştirir,
- Az bir çaba ile risk kayıtları ve risk iyileştirme planlarının oluşturulmasını sağlar,
- Risk değerlendirmesi ve dikkate alınması gereken gerekli faaliyetlerin önceliklendirilmesi için genellikle kalitatif veya yarı-kantitatif yapıda risk derecelendirmesi kullanılmasına rağmen, SWIFT, sayısallaştırılmış bir çalışma için risklerin ve tehlikelerin belirlenmesi amacı ile de kullanılabilir.

SWIFT'in kısıtları:

- Verimli olabilmesi için, deneyimli ve liyakatli bir yöneticiye ihtiyaç vardır,
- Çalıştay ekibinin zamanının boşa harcanmaması için dikkatli bir hazırlık gereklidir,
- Çalıştay ekibi geniş çaplı deneyime sahip değilse veya yönlendirici kelime seti kapsamlı değilse, bazı riskler veya tehlikeler belirlenemeyebilir,
- Tekniğin yüksek-seviye uygulaması; karmaşık, ayrıntılı veya ilişkilendirilmiş sonuçları ortaya çıkarmayabilir.

## B.10 Senaryo analizi

### B.10.1 Genel

Senaryo analizi, gelecekte neler olabileceğini betimlemek amacı ile geliştirilen modellere verilen addır. Gelecekteki olası gelişmeleri göz önünde bulundurarak riskleri belirlemek ve sonuçlarını araştırmak için kullanılır. Riskleri analiz ederken, muhtemel sonuçları ve her senaryo için hassasiyet analizi şeklindeki olasılıkları inceleyebilmek için, "en iyi durum", "en kötü durum" ve "beklenen durum" u yansıtan çeşitli senaryo setleri oluşturulur.

Senaryo analizinin gücü, teknolojiye tüketici tercihlerinde, sosyal davranışlarda geçmiş 50 yılda yaşanan değişimler vb. üzerinden açıklanabilir. Senaryo analizi bu tür değişimlerin olasılıklarını tahmin edemez, ancak sonuçlarını anlamaya ve kurumların öngörülebilir değişikliklere uyum sağlayabilmeleri için ihtiyaç duyacakları dayanıklılık ve gücü geliştirmelerine yardım eder.

**B.10.2 Kullanım**

Mevcut faaliyetleri değerlendirmenin yanı sıra, politika oluşturulması ve gelecek stratejilerin planlanmasına destek vermek amacıyla senaryo analizi kullanılabilir. Risk değerlendirmesinin her üç parçasında da yer alabilir. Belirleme ve analiz aşamasında, “en iyi durum”, “en kötü durum” ve “beklenen durum”u yansıtan senaryo setleri kullanılarak, belirli durumlarda her senaryo için neler oluşabileceği, muhtemel sonuçları ve oluşma ihtimalleri analiz edilebilir.

Senaryo analizi, uzun veya kısa zaman diliminde her tür risk için ve aynı anda hem tehditlerin hem de fırsatların nasıl gelişeceğini öngörmek için kullanılabilir. Kısa vadeli ve iyi veri sayesinde günümüzdeki muhtemel senaryolar geleceğe uyarlanabilir. Daha uzun zaman çerçeveleri için yapılan ya da yetersiz veri ile yapılan senaryo analizleri daha hayale dayalı dönüşür ve geleceğe yönelik analizler olarak adlandırılabilir.

Senaryo analizleri, zaman, mekân ve topluluktaki gruplar arasında ya da kuruluşlarda olumlu sonuçlar ile olumsuz sonuçlar arasındaki dağılımlarda güçlü ayırımlarının olduğu hallerde kullanışlı olabilir.

**B.10.3 Girdiler**

Bir senaryo analizinin ön koşulu, geçmiş veriye bağlı olarak gelecek tahmini yapmaya ihtiyaç duymayan, aralarında ilgili değişikliklerin doğası hakkında yeterli bilgisi bulunan kişilerden oluşan bir ekip bulunmasıdır. Gerçekleşen değişiklikler hakkında veri ve kaynaklara erişim de ayrıca kullanışlıdır.

**B.10.4 Proses**

Senaryo analizi çalışmasının yapısı resmi veya gayri resmi olabilir.

Gerekli ekip ve iletişim kanalları oluşturulduktan, göz önünde bulundurulacak problemin ve sorunların içeriği tanımlandıktan sonraki adım, oluşabilecek değişikliklerin doğasının belirlenmesidir. Bu önemli eğilimlerin ve eğilimlerdeki değişimlerin muhtemel zamanlamasının araştırılmasını ve aynı zamanda gelecek hakkında hayal gücü yüksek düşünmeyi gerektirir.

Düşünülecek değişiklikler aşağıdakileri içerebilir:

- Dış değişiklikler (teknolojik değişiklikler vb.),
- Yakın zamanda alınması gereken ancak, çok çeşitli sonuçları olabilecek kararlar,
- Paydaşların ihtiyaçları ve bunların nasıl değişebileceği,
- Makro çevrede oluşabilecek değişiklikler (mevzuat, demografik vb.). Bazıları kaçınılmaz, bazıları belirsiz olabilir.

Bazı zamanlarda, bir değişiklik başka bir riskin sonucu olarak ortaya çıkabilir. Örneğin, iklim değişikliği riski, tüketici talebi üzerinde gıda yolu ile ilgili değişikliklerle sonuçlanabilir. Bu risk; hangi gıdaların yerel olarak yetiştirileceğinin yanı sıra hangi gıdaların kar edilerek ihraç edilebileceğini de etkiler.

Yerel ve makro etkenler veya eğilimler bundan sonra listelenip, (1) önem derecesi ve (2) belirsizliklerine göre sıralanabilirler. En önemli ve en belirsiz etkenlere özel dikkat gösterilir. Ana etkenler ve eğilimler senaryoların geliştirileceği alanları göstermek için birbirleri ile eşleştirilirler.

Her biri parametrelerde makul değişiklikler içeren bir dizi senaryo önerilir.

Daha sonra, her bir senaryo için bu noktadan hedef senaryoya nasıl ilerlenebileceğini anlatan bir “hikaye” yazılır.

Senaryolar daha sonra orijinal soruyu test etmek veya değerlendirmek için kullanılabilir. Test, her türlü önemli ancak tahmin edilebilir etkenleri (model kullanarak) dikkate alır ve politikanın (aktivitenin) bu yeni senaryoda nasıl “başarılı” olabileceği araştırılır ve çıktıları, modeldeki ön kabulleri temel alan “olursa ne olur” soruları ile “ön test”e tabi tutar.

Öneri veya soru, her bir senaryoya göre değerlendirildiğinde, daha az riskli veya daha güçlü olması için değişiklik yapılması gerektiği ortaya çıkar. Değişiklik oluşmaya başladığı zaman bunu gösterecek bazı öncü göstergeleri de belirlemek mümkün olabilir. İzleme ve öncü göstergelere tepki verme, planlanmış stratejileri değiştirmek için bir fırsat sunabilir.

Senaryolar, muhtemel geleceğe ait sadece ufak bir zaman “dilimi” olduklarından, belirli bir çıktının (senaryo) ihtimalinin dikkate alındığından emin olunması (risk yönetim çerçevesinin uygulanması) çok önemlidir. Örneğin, en iyi, en kötü ve beklenen senaryoların kullanıldığı durumlarda, her senaryonun oluşabilme ihtimalinin belirtilmesi veya ifade edilmeye çalışılması gerekir.

**B.10.5 Çıktılar**

Duruma en iyi uyan senaryo her zaman bulunamasa bile, sonunda, kişi farklı seçenekleri ve göstergelerin işaret ettiği yönde ilerlenecek yönü ve faaliyetleri nasıl değiştirmek gerekeceğini daha açık şekilde görebilmelidir.

**B.10.6 Güçlü yanlar ve kısıtlar**

Senaryo analizi, geçmiş zamana ait veriye dayalı ve gelecekte de aynı eğilimlerin tekrar edeceğini varsayan geleneksel yüksek-orta-düşük tahminleri yerine tercih edilebilecek, bir dizi muhtemel özellikleri göz önünde bulundurur. Bu, özellikle tahminlere temel olacak mevcut bilginin çok az olduğu veya öngörülen risklerin uzun vadeli olduğu durumlar için çok önemlidir.

Bununla birlikte, bu güçlü yan ile birlikte gelen, yüksek belirsizlik olduğu durumlarda senaryoların gerçeklikten uzaklaşması gibi bir zayıflık mevcuttur.

Bir karar verme aracı olarak senaryo analizini kullanmanın tehlikeleri, kullanılan senaryolarda verilerin spekülatif olması ve benzer şekilde sonuçların kabul görmemesine neden olabilecek yeterli altyapı bulunamaması şeklinde ifade edilebilir.

**B.11 İş etki analizi (BIA)****B.11.1 Genel**

Aynı zamanda iş etki değerlendirmesi olarak ta bilinen iş etki analizi, iş kesintilerine yol açabilecek risklerin bir kurumun işleyişini nasıl etkileyeceğini inceler ve bu durumu yönetebilmek için gerekli olan yetkinlikleri belirleyip sayısallaştırır. İş etki analizi özellikle aşağıdakilerin anlaşılmasına olanak sağlar:

- Kurumda bulunan iş proseslerinin, fonksiyonlarının ve bağlı kaynakların ve karşılıklı bağımlılıkların belirlenmesi ve önem seviyelerinin anlaşılması,
- Kesintiye yol açan olayların, önemli iş hedeflerini gerçekleştirme kapasite ve kabiliyetini nasıl etkileyeceği,
- Kesintinin etkisini yönetmek ve kuruluşun istenen işletme seviyesinde çalışmasını sağlamak için ihtiyaç duyulan kapasite ve kabiliyet.

**B.11.2 Kullanım**

İş etki analizi, hedeflere ulaşmadaki devamlılığı sağlamak amacıyla, prosesin ve ilişkili kaynakların (insan, donanım, bilgi teknolojisi) kritikliğini ve geri kazanma zaman aralığını belirlemek için kullanılır. Buna ek olarak BIA; prosesler, iç ve dış taraflar ve tedarik zinciri mekanizmaları arasındaki bağımlılık ve ilişkinin belirlenmesini destekler.

**B.11.3 Girdiler**

Girdiler aşağıdakileri içerir:

- Bir planın analizi ve geliştirilmesi görevini üstlenen bir ekip,
- Kuruluşun hedefleri, çevresi, faaliyetleri ve bağımlılıklarını ilgilendiren bilgiler,
- Kuruluşun; prosesler, destekleyici kaynaklar, diğer kuruluşlarla ilişkiler, dış kaynak kullanılan düzenlemeler, paydaşlar gibi konuları içeren faaliyet ve işlemlerine ilişkin ayrıntılar,
- Kritik proseslerin kaybının meydana getirdiği finansal ve işletimsel sonuçlar,
- Hazırlanan anketler,
- İlgili alanlardaki kuruluşlardan ve/veya ilintili paydaşlardan irtibat kurulacak kişilerin listesi.

**B.11.4 Proses**

Kritik proseslerin, bu proseslerin kayıplarının neden olabileceği etkilerin, gerekli kurtarma zaman aralıklarının ve destekleyici kaynakların anlaşılabilmesi amacıyla; anket, görüşme, yapılandırılmış çalıştay veya bu üçünün kombinasyonu kullanılarak bir BIA gerçekleştirilebilir.

Başlıca adımlar aşağıdakileri içerir:

- Risk ve zafiyet değerlendirmesi temel alınarak, proseslerin kritikliğinin anlaşılması için önemli prosesler ve kuruluşun çıktılarının doğrulanması,
- Tanımlanan periyotlardaki finansal ve/veya işletimsel dönemler için, belirlenen kritik proseslerin aksamamasından kaynaklanan sonuçların tespit edilmesi,
- Başlıca iç ve dış paydaşlarla karşılıklı bağımlılığın belirlenmesi. Bu faaliyet bağımlılıklarının doğasının, tedarik zinciri aracılığıyla belirlenmesini içerebilir,

- Herhangi bir aksama durumunda, kuruluşun kabul edilebilir en düşük seviyede işletilebilmesine devam edilebilmesi için, mevcut uygun kaynakların ve ihtiyaç duyulan kaynakların asıl seviyesinin belirlenmesi,
- Kullanımda olan veya geliştirilmesi planlanan alternatif proses ve seçeneklerin belirlenmesi, kaynaklara veya yetkinliklere erişilemediği veya yetersiz olduğu durumlarda alternatif proses ve seçeneklerin geliştirilmesi gerekebilir,
- Her prosesinin kabul edilebilir en yüksek devre dışı kalma süresi (MAO), belirlenen sonuçlara ve kritik başarı faktörlerine dayanır. Kabul edilebilir en yüksek devre dışı kalma süresi (MAO), kuruluşun tolere edebileceği kapasite kaybına ilişkin en yüksek zaman periyodunu temsil eder,
- Tüm özel donanım veya bilgi teknolojileri için kurtarma zaman hedeflerine (RTO) karar verilmesi. RTO, kurumun özel donanım veya bilgi teknolojileri kabiliyetlerini tekrar kullanılabilir hale getirmeyi hedeflediği süreyi ifade eder,
- Kritik prosesleri kesinti durumunda yönetebilmesi için mevcut hazırlık durumu yeterliğinin doğrulanması. Bu adım, proses içerisindeki yedek seviyesinin (örneğin, yedek donanım) veya alternatif tedarikçilerin değerlendirmesini de içerebilir.

### B.11.5 Çıktılar

Çıktılar aşağıdaki gibidir:

- Kritik proseslerin ve ilişkili bağımlılıkların öncelik listesi,
- Kritik proseslerde meydana gelen kayıplardan kaynaklanan, dokümanede edilmiş finansal ve işletimsel etkiler,
- Belirlenen kritik prosesler için ihtiyaç duyulan destekleyici kaynaklar,
- Kritik prosesler için devre dışı kalma süresi ve ilişkili bilgi teknolojisi kurtarma süresi.

### B.11.6 Güçlü yanlar ve kısıtlar

BIA'nın güçlü yanları:

- Kuruluşa, belirtilen hedeflere ulaşmaya devam etme yeteneği sağlayan kritik prosesleri anlama,
- İhtiyaç duyulan kaynakları anlama,
- Kuruluşun esnekliğini desteklemek için, kuruluşun işletimsel bir prosesinin yeniden tanımlanma fırsatı.

Kısıtları:

- Ankete, görüşmelere veya çalıştaylara katılan katılımcıların bilgi birikimi eksikliği,
- Grup dinamiği kritik proseslerin analizini etkileyebilir,
- Kurtarma şartlarında, basit veya aşırı-iyimser beklentiler,
- Kuruluşun faaliyet ve icraatlarını anlama seviyesini uygun bir seviyeye çekmedeki güçlükler.

## B.12 Kök Neden Analizi (RCA)

### B.12.1 Genel

Önemli bir kaybın tekrar oluşmasını engellemek için gerçekleştirilen analiz; genel olarak Kök Neden Analizi (RCA), Hatanın Kök Neden Analizi (RCFA) ya da kayıp analizi olarak adlandırılır. RCA, farklı türden hatalar nedeni ile ortaya çıkan varlık kayıplarına odaklanırken, kayıp analizi asıl olarak, felaketler veya dış faktörler nedeniyle oluşan finansal ya da ekonomik kayıplarla ilgilidir. Bu yöntem, olayın ilk görünür belirtileri yerine kök ya da temel nedenlerini belirlemeye çalışır. Düzeltici faaliyetlerin her zaman sorunun tamamında etkili olmadığı ve sürekli iyileştirmenin gerekliliği bilinmektedir. RCA, çok sıklıkla önemli bir kaybı değerlendirmek için uygulandığı halde, daha küresel ölçekte temel olarak yaşanan kayıplar için nerelerde iyileştirme yapılabileceğine dair inceleme için de kullanılabilir.

### B.12.2 Kullanım

RCA, farklı içeriklerde geniş çaplı olarak aşağıdaki alanlarda uygulanabilir:

- Güvenlik temelli RCA, kaza incelemeleri ve iş sağlığı ve güvenliği için kullanılır,
- Hata analizi, teknolojik sistemlerde bakım ve güvenilirlikle ilgili çalışmalarda kullanılır,
- Üretim temelli RCA, endüstriyel üretimde kalite kontrol alanında uygulanır,
- Proses temelli RCA iş proseslerine odaklanır,
- Sistem temelli RCA önceki alanların bileşimi olarak, değişiklik yönetimi, risk yönetimi, sistem analizi gibi karmaşık sistemler için geliştirilmiştir.

### B.12.3 Girdiler

RCA için temel girdi, kayıp ve hata sonucunda toplanmış tüm delillerdir. Diğer benzer hatalardan elde edilen veriler de analizde göz önünde bulundurulabilir. Diğer bir tür girdi ise, özel hipotezleri test etmek için kullanılan sonuçlar olabilir.

### B.12.4 Proses

RCA ihtiyacı belirlendiği zaman, bir grup uzman inceleme ve öneri yapmaları için görevlendirilir. Gerekli olan uzmanlık hatayı incelemek için ihtiyaç duyulan özel uzmanlık alanına bağlıdır.

Analizi gerçekleştirmek için pek çok farklı yöntem olsa da, RCA'yı yürütmek için gerekli olan temel adımlar birbirine benzer ve aşağıdakilerini içerir:

- Ekip oluşturulması,
- Kök-neden analizinin kapsam ve hedefinin belirlenmesi,
- Kök-nedenlerin anlaşılması için yapılandırılmış analizin gerçekleştirilmesi,
- Önerilerin yerine getirilmesi,
- Yerine getirilmiş önerilerin başarılı olduğunun doğrulanması.

Yapılandırılmış analiz teknikleri aşağıdakilerin birinden oluşabilir:

- "5 neden" tekniği, arka arkaya "neden?" sorusunun sorulmasıyla, nedenler ve alt nedenlerin ortaya çıkarılması,
- Hata türleri ve etkileri,
- Arıza çözümüleme ağacı,
- Balık-kılçığı veya Ishikawa diyagramları
- Kök neden eşleştirme.

Nedenlerin değerlendirilmesi çoğunlukla, ilk belirgin fiziksel nedenlerle başlayıp, insan kökenli nedenlere ve en son yönetim altyapısı veya temel nedenler şeklinde ilerler. Düzeltici faaliyetin etkin ve uygulamaya değer olabilmesi için, neden olan faktörlerin kontrol edilebilir ya da ortadan kaldırılabilir olması gerekir.

### B.12.5 Çıktılar

RCA'nın çıktıları:

- Elde edilen veri ve delillerin dokümantasyonu,
- Göz önünde bulundurulan hipotezler,
- Kayıp veya hatanın en muhtemel nedenleri,
- Düzeltici faaliyetler için öneriler.

### B.12.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar:

- Ekip halinde çalışan uygun uzmanların bulunması,
- Yapılandırılmış çözümleme,
- İhtimal dâhilindeki tüm hipotezlerin gözden geçirilmesi,
- Sonuçların belgelenmesi,
- Sonuç öneri getirme gerekliliği.

RCA'nın kısıtları:

- Gerekli olan uzmanlar bulunamayabilir,
- Kritik deliller temizlik ya da olay esnasında ortadan kaldırılmış olabilir,
- Durumu değerlendirecek ekibe yeterli zaman veya kaynak sağlanamayabilir,
- Önerilerin hayata geçirilmesi mümkün olmayabilir.

## B.13 Hata türleri ve etkileri analizi (FMEA), hata türleri ve etkileri ve kritiklik analizi (FMECA)

### B.13.1 Genel

Hata türleri ve etkileri analizi (FMEA); bileşenlerin, sistemlerin veya proseslerin kendilerinden beklenen sonuçları tasarlanma amaçlarına uygun olarak yerine getirip getiremediklerini belirlemek için kullanılan bir tekniktir.

FMEA şunları belirler:



- Bir sistemin çeşitli parçalarının tüm muhtemel (bir hata türü; çalışmama veya doğru sonuç üretmeme anlamındadır),
- Bu hataların sistem üzerinde yol açacağı etkiler,
- Hatanın oluş biçimi,
- Hatalar nasıl engellenir ve/veya hatanın sistem üzerindeki etkileri nasıl giderilir.

FMECA; FMEA'nın belirlenen her hata durumunun önemine veya kritikliğine göre derecelendirilmesi şeklinde geliştirilmiş halidir.

Bu kritiklik analizi genellikle kalitatif veya yarı kantitatif, bununla birlikte gerçek hata oranları kullanılarak kantitatif hale getirilebilir.

### B.13.2 Kullanım

FMEA'nın farklı uygulama alanları vardır: Tasarım FMEA (veya ürün) bileşenler ya da ürünler için kullanılır, Sistem FMEA, sistemler için kullanılır, Proses FMEA, üretim ve montaj prosesleri için kullanılır, Servis FMEA ve Yazılım FMEA.

FMEA/FMECA bir fiziksel sistemin tasarım, üretim veya işletim aşamasında uygulanabilir.

Bununla birlikte, değişikliklerin tasarım aşamasında gerçekleştirilmesi güvenilirliği artırır. FMEA ve FMECA aynı zamanda proseslere ve prosedürlere de uygulanabilir. Örneğin, sağlık bakım sistemlerinde tıbbi hata potansiyeli ve bakım prosedürlerindeki hataları belirlemek için kullanılır.

FMEA/FMECA aşağıdaki amaçlarla kullanılabilir:

- Yüksek güvenilirlik içeren tasarım alternatiflerinin seçiminde yardımcı olmak,
- Sistem ve proseslere ait tüm hata durumlarının ve bunların başarılı işletimlerini güvence altına almak,
- İnsan kaynaklı hata türlerini ve etkilerini belirlemek,
- Fiziksel sistemlerin, planlama, test ve bakımı için temel sağlamak,
- Prosedür ve proseslerin tasarımını geliştirmek,
- Hata ağacı analizi gibi analiz teknikleri için kalitatif veya kantitatif bilgi sağlamak.

FMEA ve FMECA; hata ağacı analizi gibi diğer analiz tekniklerine kalitatif veya kantitatif seviyede girdi sağlayabilir.

### B.13.3 Girdiler

FMEA ve FMECA, her bir parçanın ne şekilde hata üretebileceğinin anlamlı bir analizini yapabilmek için, sistemi oluşturan parçalardan yeterli ayrıntı için bilgi alma ihtiyacı duyar. Ayrıntılı bir Tasarım FMEA yürütmek için, öğeler her bir bileşen düzeyinde ayrıntıda tanımlanabilir, daha yüksek seviyede Sistem FMEA için ise, öğeler daha yüksek seviyede tanımlanabilir.

Bilgiler aşağıdakileri içerebilir:

- Analiz edilecek sistemin ve bileşenlerinin veya bir prosesin adımlarının çizimleri veya akış şemaları,
- Bir sistemin bileşenlerinin veya bir proses adımlarının fonksiyonlarının anlaşılması,
- İşletimi etkileyebilecek çevresel ya da diğer parametrelerin ayrıntıları,
- Belirli hatalara ait sonuçlarının anlaşılması,
- Elde edilebildiği durumlarda, arıza oranlarının da bulunduğu hatalara ait geçmişe dönük bilgi.

### B.13.4 Proses

FMEA prosesi şu şekilde işler:

- Çalışmanın hedef ve kapsamının tanımlanması,
- Ekibin oluşturulması,
- FMECA'ya konu olan sistem veya prosesin anlaşılması,
- Sistemin bileşenlerine veya adımlarına ayrıştırılması,
- Her adım veya bileşenin işlevinin tanımlanması,
- Listelenen her parça veya adım için aşağıdakilerin belirlenmesi:
  - Her bir parçada nasıl bir arıza meydana gelebilir?
  - Bu hata durumlarını hangi mekanizmalar üretebilir?
  - Hatanın oluşması halinde etkileri neler olabilir?
  - Arıza zararsız mı yoksa hasar verebilir mi?
  - Arıza nasıl tespit edilir?
- Tasarım içerisinde arızalara karşı alınmış önlemlerin belirlenmesi.

FMECA için, çalışma ekibi belirlenen her hata türünü kritikliklerine göre sınıflandırır. Bunu yapabilmek için çeşitli yollar mevcuttur. Çok kullanılan yöntemler:

- Durum kritiklik indeksi
- Risk seviyesi
- Risk öncelik sayısı.

Model kritikliği, ele alınan durumun, tüm sistemin çökmesi ile sonuçlanacağına dair olasılığın ölçüsüdür ve şu şekilde tanımlanır:

$$\text{Arızanın etki ihtimali} * \text{Arıza durum oranı} * \text{Sistemin işletim süresi}$$

Yukarıdaki tanımlama, her bir değer sayısal olarak belirlendiği ve arıza durumlarının aynı neticeye yol açacağı düşünülen donanım arızalarında en sık uygulanan tanımlamadır.

Risk seviyesi, arıza durumunun oluştuğundan sonraki etkilerinin arıza olasılığı ile birleştirilmesinden elde edilir. Farklı arıza durumlarının sonuçlarının da farklı olduğu zamanlarda, donanım sistemleri veya prosesler için kullanılır. Risk seviyeleri; kalitatif, yarı kantitatif veya kantitatif olarak ifade edilebilir.

Risk öncelik numarası (RPN) derecelendirme ölçümlerinden elde edilmiş, arızanın etkileri, arızanın olasılığı ve sorunu tespit edebilme imkanını yansıtan sayıların (genellikle 1-10 arası) çarpılması ile oluşturulan yarı kantitatif bir kritiklik değeridir (Bir arızanın tespiti zor ise daha fazla öncelik verilir). Bu yöntem en çok kalite güvence uygulamalarında kullanılır.

Arıza durumları ve mekanizmaları belirlendikten sonra, önemli arıza durumları için düzeltici faaliyetler tanımlanabilir ve uygulanabilir.

FMEA aşağıdakileri içeren bir rapor ile doküman edilir:

- Çözümünecek sistemin ayrıntıları,
- İşlemin yürütülme yöntemi,
- Çözümlemede kullanılan varsayımlar,
- Veri kaynakları,
- Sonuçları içeren tamamlanmış çalışma dosyaları,
- Kritiklik (eğer tamamlanmış ise) ve tanımlamakta kullanılan yöntem,
- Daha ileri düzey analiz, tasarım değişiklikleri veya test planlarına dâhil edilmesi gereken özellikler vb. için öneriler.

Gerekli faaliyetler gerçekleştirildikten sonra sistem, diğer bir FMEA döngüsü ile tekrar değerlendirilebilir.

### B.13.5 Çıktılar

FMEA'nın başlıca çıktıları; arıza durumları listesi, arıza mekanizmaları ve bir sistemin veya prosesin (arızanın olabirliği hakkında bilgi de içerebilir) tüm adım veya parçalarına ait etkilerdir. Arızanın nedenleri ve tüm sistem üzerindeki etkileri hakkında bilgi de verilebilir. FMECA'nın çıktıları; sistemin çökme ihtimali, hata durumu nedeni ile oluşan risk veya risk seviyesi ile arıza durumunun "tespit edilebilirlik" seviyesinin birleşimini temel alan önemlilik derecesini içerir.

FMECA, uygun kantitatif sonuçlar ve hata oranları verisi kullanıldığı takdirde sayısal bir çıktı verebilir.

### B.13.6 Güçlü yanlar ve kısıtlar

FMEA/FMECA'nın güçlü yanları aşağıdaki gibidir:

- Geniş çaplı olarak insan, donanım ve sistem hata durumları için ayrıca, donanım, yazılım ve prosedürler için kullanılabilir,
- Bileşenlerin arıza durumlarını, bunların nedenleri ve sistem üzerindeki etkilerini belirler ve bunları kolay okunabilir bir yapıda sunar,
- Tasarım aşamasında erken tespit sayesinde yüksek tamir ve değişiklik maliyetlerine engel olur,
- Tek noktada oluşan hata durumlarını ve yedekleme veya güvenlik sistemleri gereksinimlerini belirler;
- İzlenmesi gereken önemli anahtar özellikleri öne çıkararak izleme programlarının geliştirilmesi için girdi sağlar.

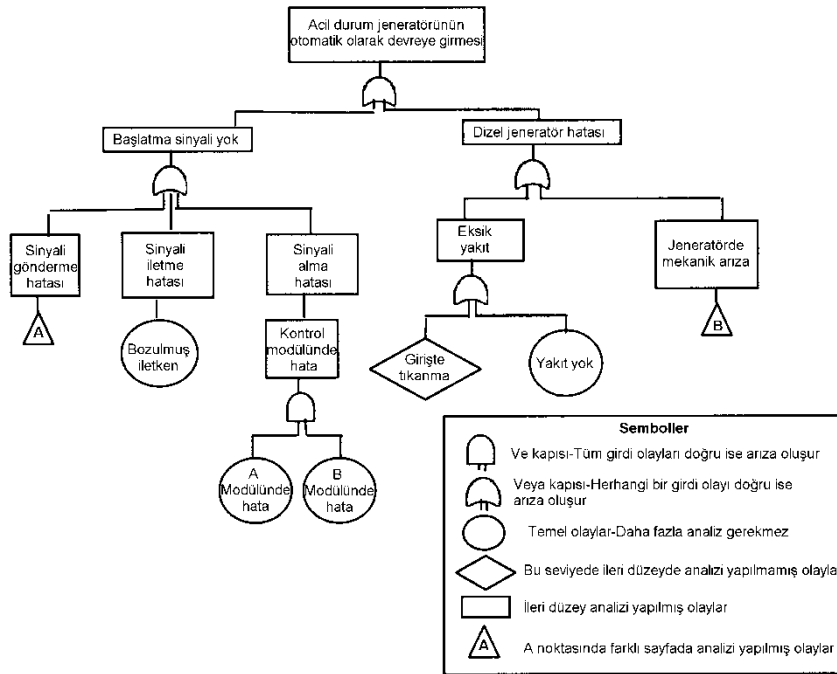
Kısıtlar:

- Tek noktadaki hata durumlarını tespit edebilirler, iç içe geçmiş hata durumlarını tespit edemez;
- Yeterli derecede odaklanıp kontrol edilmez ise, bu tür çalışmalar zaman kaybettirici ve yüksek maliyetli olabilir;
- Çok katmanlı sistemler için karmaşık ve yorucu olabilirler.

**B.13.7 Kaynak doküman**IEC 60812, *Sistem güvenirliliği için analiz teknikleri – Hata durumları ve etki analizi için prosedürler (FMEA)***B.14 Hata Ağacı Analizi (FTA)****B.14.1 Genel**

Hata ağacı analizi, belirli bir istenmeyen olaya ("üst olay" olarak adlandırılır.) neden olan faktörleri tanımlamak ve analiz etmek için kullanılan bir tekniktir. Nedensel faktörler tümdengelimli olarak tanımlanır, mantıksal biçimde organize edilir ve mantıksal faktörler ve bunların üst olayla mantıksal ilişkisi şekilsel olarak bir ağaç diyagramında sunulur.

Hata ağacında tanımlanan faktörler; istenmeyen olaylara sebebiyet veren donanım bileşen hatası, insan hatası veya diğer alakalı olaylar ile ilişkilendirilmiş olaylar olabilir.

**Şekil B.2 - IEC 60300-3-9 dan bir FTA örneği****B.14.2 Kullanım**

Bir hata ağacı, hataya (üst olay) sebebiyet verebilecek potansiyel olayları ve yolları kalitatif olarak tanımlamak için veya nedensel olayların meydana gelme olasılığı ile ilgili verilen bilgi ışığında, üst olayın olasılığını sayısal olarak hesaplamak için kullanılabilir.

Hata ağaçları sistemin tasarımı aşamasında, bir hatanın potansiyel etkilerini tanımlamak ve dolayısıyla farklı tasarım seçenekleri arasında seçim yapmak için kullanılabilir. Ayrıca hata ağaçları, faaliyete geçme aşamasında majör hataların nasıl meydana geldiğini ve farklı yolların üst olay açısından bağlı önemini tanımlamak için kullanılabilir. Bir hata ağacı, birden farklı olayın nasıl bir araya gelerek sorun oluşturduğunu analiz etmek ve şekilsel olarak göstermek için de kullanılabilir.

**B.14.3 Girdiler**

Kalitatif bir analiz için, sistemin nasıl aksadığının teknik olarak anlaşılmasının yanı sıra, sistemin ve hatanın nedenlerinin anlaşılması da gereklidir. Ayrıntılı diyagramların kullanılması, analize yardımcı olmada faydalıdır.

Kantitatif bir analiz için ise, hata ağacındaki tüm temel olaylar için, hata oranları veya başarısız olma olasılığı verilerinin bulunması gerekir.

#### B.14.4 Proses

Bir hata ağacının geliştirilmesi için basamaklar aşağıdaki gibidir:

- Analiz edilecek üst olay tanımlanır. Bu tanımlama bir hata veya hatanın daha geniş bir çıktısı olabilir. Çıktı analiz edildiğinde, hata ağacı gerçek hatanın azaltılmasına ilişkin bölümleri içerebilir.
- Üst olaydan başlamak üzere, üst olaya neden olan olası anlık nedenler veya hata durumları tanımlanır.
- Bu neden/hata durumları, hataların nasıl meydana geldiğini tanımlamak için analiz edilir. Sistemdeki istenmeyen işletim durumları adım adım belirlenerek, daha fazla incelemenin verimsiz olacağı en alt seviyeye kadar devam ettirilir. Bir donanım sisteminde bu seviye, parça arıza seviyesidir. En düşük sistem seviyesinde çözümlenen olaylar ve nedensel faktörler, temel olaylar olarak bilinir.
- Olasılıkların Temel Olay'lara dayandırıldığı yerlerde, esas olayın olasılığı hesaplanabilir. Sayısallaştırmanın geçerli olması için; bu sayısallaştırma, çıktı olayları üretmek amacıyla, tüm girdilerin (her kapı için) hem gerekli hem de yeterli olduğunu gösterebilir olmalıdır. Böyle değilse, hata ağacı olasılık analizi için geçerli değildir ancak nedensel ilişkileri göstermede faydalı bir araç olabilir.

Sayısallaştırmanın bir parçası olarak, hata ağacının Boolean cebir kullanılarak basitleştirilmesine ihtiyaç duyulabilir. Bu basitleştirme, hata modlarının tekrarını dikkate almak amacıyla yapılır.

Esas olayın olasılığının tahmin edilmesinin yanı sıra, esas olaya giden ayrı ayrı bireysel yolları oluşturan minimal kesit setleri ve bu kesit setlerinin hesaplanan esas olay üzerindeki etkisi tanımlanabilir.

Basit hata ağaçları hariç olmak üzere; tekrarlanan olaylar hata ağacının birkaç yerinde meydana geldiğinde, hesaplamaları düzgün bir şekilde ele almak ve minimal kesit setlerini hesaplamak için bir yazılım paketi gerekebilir. Yazılım araçları tutarlılığı, doğruluğu ve onaylanabilirliği sağlamaya yardımcı olur.

#### B.14.5 Çıktılar

Hata ağacı analizinin çıktıları aşağıdaki gibidir:

- İki veya daha fazla eşzamanlı olayın meydana geldiği durumlarda birbirini etkileyen yolları gösteren ve esas olayın nasıl meydana geldiğini şekilsel olarak gösteren sunum,
- Veri olduğunda olma olasılığı olan en az kesit setlerinin (hataya giden bireysel yollar) listesi,
- Üst olayın olma olasılığı.

#### B.14.6 Güçlü yanlar ve kısıtlar

FTA'nın güçlü yanları:

- Yüksek derecede sistematik ancak, aynı zamanda, insan etkileşimleri ve fiziksel olayları içeren faktör çeşitliliğinin analizine müsaade edecek kadar esnek olan, disipline edilmiş bir yaklaşım sağlar.
- Tekniğin içindeki "Yukarı-Aşağı" yaklaşımının uygulaması, üst olayla direkt ilişkili hataların etkisi üzerindeki dikkate odaklanır.
- Hata ağacı analizi, özellikle pek çok ara yüzü ve etkileşimi olan sistemlerin analiz edilmesi için faydalıdır.
- Şekilsel gösterim; sistem davranışını ve dâhil olan faktörleri anlamayı sağlar ancak hata ağaçları çok büyük olduğunda hata ağaçları bilgisayar sistemi gerektirebilir. Bu özellik, ilave edilecek daha kompleks mantıksal ilişkilere olanak sağlar ancak aynı zamanda hata ağacının doğrulamasını güçleştirir.
- Esas olaya neden olan olayların kısmi kombinasyonlarının gözden kaçırılması durumunda, hata ağacının mantıksal analizi ve kesit setlerinin tanımlanması, çok karışık bir sistemde basit hata yollarını belirlemede faydalıdır.

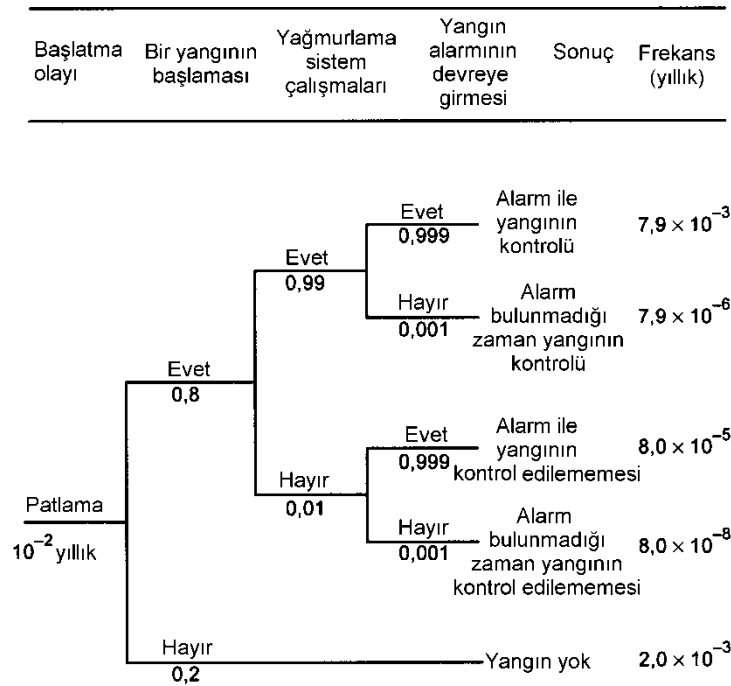
Kısıtlar:

- Temel olayların olasılıklarındaki belirsizlikler, üst olayın olasılığının hesaplanmasına katılır. Bu nedenle temel olayların hataya yol açma olasılıkları hassas olarak bilinmiyorsa yüksek belirsizlik durumları ile sonuçlanabilir. Bununla birlikte, iyi bilinen sistemler için yüksek güvenilirlik derecesi mümkündür.
- Bazı durumlarda, neden olayları bir araya getirilemezler ve bu nedenle üst olaya yol açacak tüm yolların kapsandığı saptanamayabilir. Örneğin, üst olay olarak bir yangın çözümlenmesinde, tüm ateşleme kaynaklarının kapsanmasıdır. Bu durumda olasılık çözümlenmesi imkânsızdır.
- Hata ağacı statik bir modeldir, zaman bağımlılıklarını içermez.
- Hata ağaçları yalnızca ikili durumlarda geçerlidir (hata oluştu/oluşmadı).
- İnsan hatası modlarının kalitatif hata ağacına dâhil edilebilmesine rağmen, insan hatasını niteleyen aşama veya kalitedeki genel hatalar kolayca dâhil edilemez.

Bir hata ağacı, domino etkisine veya kolayca dâhil edilecek koşullu hatalara olanak sağlamaz.

**B.14.7 Kaynak dokümanlar**IEC 61025, *Hata ağacı analizi (FTA)*IEC 60300-3-9, *Bağımlılık yönetimi- 3. Bölüm: Uygulama kılavuzu- 9. Kısım: Teknolojik sistemlerde risk analizi***B.15 Olay ağacı analizi (ETA)****B.15.1 Genel**

ETA, olumsuz sonuçları en aza indirmek için tasarlanan çeşitli sistemlerin çalışma/çalışmama durumlarına göre, başlangıç olayının ardından gelen olayların ayrışık sırasının gösterimi için kullanılan grafiksel bir tekniktir (bk. Şekil 3). Kalitatif ve kantitatif olarak her iki şekilde de uygulanabilir.

**Şekil B.3 - Örnek olay ağacı**

Şekil B.3 Dalların tümünün bağımsız olduğu örnek olay ağacı için basit hesaplamaları göstermektedir.

Ağaca benzer yelpaze şeklindeki açılımı ile ETA, başlangıç olayına tepki olarak oluşan iyileştirici ya da kötüleştirici olayları, ilave sistemleri fonksiyonları veya engelleri de hesaba katarak gösterebilmektedir.

**B.15.2 Kullanım**

Olay ağacı analizi; başlangıç olayını takip eden farklı kaza senaryolarını modellemek, hesaplamak ve derecelendirmek (risk açısından bakıldığında) için kullanılabilir.

ETA bir ürünün veya prosesin yaşam döngüsünün herhangi bir aşamasında kullanılabilir. Olay ağacı analizi; potansiyel senaryolarla ve başlangıç olayının ardından gelen olayların sırası ile ilgili beyin fırtınasına yardımcı olması amacıyla kalitatif olarak kullanılabilir. Bu yöntem aynı zamanda çıktılarını; istenmeyen çıktılarının etkilerinin hafifletilmesinde kullanılan çeşitli davranışlardan, engellerden veya kontrollerden nasıl etkilediğini göstermede kullanılır.

Sayısal analiz, kontrollerin kabul edilebilirliğini dikkate almaya yol açar. Sıklıkla, birden fazla önlemin bulunduğu hataların modellenmesi için kullanılır.

ETA kazanç veya kayıp getiren başlangıç olaylarının modellenmesi için kullanılabilir. Bununla beraber, kazancı optimize edecek yolların arandığı durumlarda, modelleme için daha sıklıkla karar ağacı kullanılır.

**B.15.3 Girdiler**

Girdiler aşağıdakileri içerir:

- Uygun başlangıç olaylarının bir listesi,
- İyileştirmeler, engeller, ve kontroller ve bunların hata olasılıkları hakkında bilgi (sayısal analizler için),
- Başlangıç hatalarının artmaya başladığı proseslerin anlaşılması.

**B.15.4 Proses**

Bir olay ağacı bir başlatıcı olayın seçilmesi ile başlar. Bu olay, bir toz patlaması olabileceği gibi, enerji kesintisi gibi nedensel bir olay da olabilir. Daha sonra, sonuçları en aza indirmek için mevcut bulunan fonksiyonlar ve sistemler sırayla listelenir. Her bir fonksiyon veya sistem için, bu fonksiyon veya sistemlerin başarısını ya da hatasını gösteren bir çizgi çizilir. Uzman görüşü tarafından tahmin edilen koşullu olasılık veya hata ağacı analizi ile birlikte, her çizgiye hatanın kısmi olasılığı atanabilir. Bu yolla, başlangıç olayından çıkan farklı yollar modellenebilir.

Olay ağacındaki olasılıklar koşullu olasılıklardır. Örneğin, otomatik yağmurlama sisteminin çalışma olasılığı; normal şartlarda gerçekleştirilen çalıştırma denemelerinden elde edilen çalışma olasılığı değil, patlamanın sebebiyet verdiği bir yangının meydana gelmesi durumundaki çalışma olasılığıdır.

Olay ağacındaki her yol, bu yollardaki tüm olayların meydana gelme olasılığını temsil eder. Bu nedenle çıktının meydana gelme sıklığı; ayırık koşullu olasılık çıktısı ve başlangıç olayının meydana gelme sıklığı tarafından temsil edilir (çeşitli olayların birbirinden bağımsız olduğu varsayımıyla).

**B.15.5 Çıktılar**

ETA'nın çıktıları aşağıdakileri içerir:

- Başlangıç olayından itibaren, çeşitli tipteki problemleri (çıkıtı kümesini) meydana getiren olay kombinasyonları gibi potansiyel problemlerin niteliksel tanımlamaları,
- Olay sıklığının veya olasılığının sayısal tahminleri ve çeşitli hata dizilerinin ve katkıda bulunan olayların bağlı önemi,
- Riskleri azaltmak için yapılan önerilerin listesi,
- Öneri etkinliğinin sayısal olarak değerlendirilmesi.

**B.15.6 Güçlü yanlar ve kısıtlar**

ETA'nın güçlü yanları aşağıdakileri içerir:

- ETA, bir başlatıcı olaydan sonra oluşabilecek muhtemel senaryoları, bunların analiz edilmesini ve sonuçları en aza indirmek için uygulanan sistemler ya da fonksiyonların başarısının veya hatalarının etkilerini açık bir şekilde şematik olarak gösterir.
- Hata ağaçlarında modellemesi çok güç olan zaman, bağımlılık ve domino etkisini hesaba katar.
- Hata ağaçlarında grafiksel olarak sunulması mümkün olmayan olayların sıralı olarak gösterimini sağlar.

Kısıtlar:

- Kapsamlı bir değerlendirmenin bir parçası olarak ETA'nın kullanılabilmesi için, tüm potansiyel başlangıç olaylarının tanımlanması gerekir.. Bu tanımlama başka bir analiz metodu (örneğin, HAZOP, PHA) kullanılarak yapılabilir. Bununla birlikte bazı başlatıcı olayların her zaman atlanma olasılığı vardır.
- Olay ağaçları aracılığıyla, sistemin sadece başarı ve hata durumları ile ilgilenilir ve bu durumda ertelenen başarı veya atlanan olayları birleştirmek güçtür.
- Yol boyunca tüm olayların oluşması bir önceki dallanma noktasındaki olayın oluşma şartına bağlıdır. Bu sayede, muhtemel yollar boyunca pek çok bağımlılık tanımlanabilir. Bununla birlikte eğer bu analiz dikkatli bir şekilde yapılmazsa, bazı bağımlılıklar (ortak bileşenler, fayda sistemi gibi) gözden kaçırılmış olabilir ve bu gözden kaçırma iyimser risk tahminlerine neden olabilir.

**B.16 Neden-sonuç analizi****B.16.1 Genel**

Neden-sonuç analizi, hata ağacı ve olay ağacı analizlerinin bir kombinasyonudur. Kritik bir olay ile başlar ve olası şartları veya başlatıcı olayın sonuçlarını engellemek için tasarlanmış bir sistemin arızalanmasını gösteren evet/hayır mantık kapılarının bir araya getirilmesi ile oluşturulmuş sonuçları analiz eder. Hataların ya da bu duruma yol açan nedenlerin hata ağacı yoluyla analizleri yapılır (bk. Madde B.15 ).

**B.16.2 Kullanım**

Neden-sonuç analizi ilk olarak kritik güvenlik sistemleri için, sistem hataları hakkında daha fazla bilgi edinmek üzere güvenilirlik aracı olarak geliştirilmiştir. Hata ağacı analizine benzer şekilde, ancak buna ek olarak

sunduğu işlevsellikle, zaman sıralamalı arızaların incelenmesine izin vererek, hatanın kritik olaya yol açma mantığının gösterimi için kullanılır. Bu yöntem, olay ağaçlarında mümkün olmayan gecikme zamanlarının da sıralama analizine dâhil edilmesine izin verir.

Bu yöntem kritik olaydan sonra sistemin çeşitli seçeneklerle nasıl yol alabileceğini ve eğer sayısallaştırılırsa, belirli bir alt sistemin davranışına bağımlı olarak, kritik olaydan sonra oluşabilecek farklı sonuçların olasılık tahminlerini verir.

Diyagramda gösterilen her bir neden-sonuç sıralaması aynı zamanda bir alt hata ağacı olup, neden-sonuç analizi büyük hata ağaçları kurgulamak için kullanılabilir.

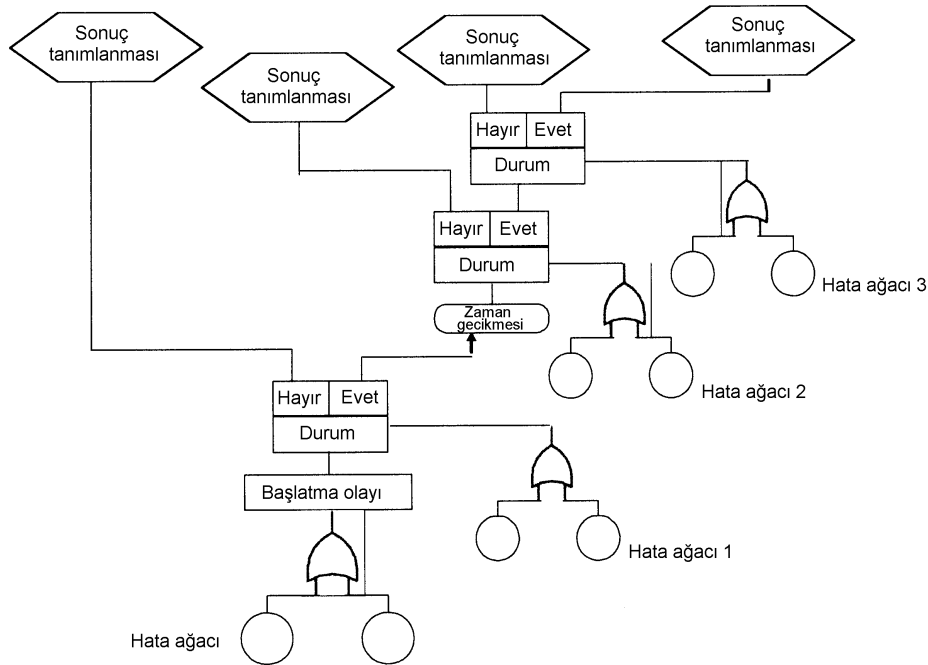
Diyagramların oluşturulmaları ve kullanılmaları karmaşık olduğundan, potansiyel sonuçların büyüklüğünün harcanacak kaynakları karşılayabileceği durumlarda kullanılması eğilimi vardır.

### B.16.3 Girdiler

Sistemin ve hata durumlarının ve hata senaryolarının anlaşılması gerekir.

### B.16.4 Proses

Şekil B.4 tipik bir neden-sonuç analizinin kavramsal bir resmini göstermektedir.



**Şekil B.4 - Neden-sonuç analizi örneği**

Prosedür aşağıdaki şekildedir:

- Kritik (ya da ilk başlatan) olayın tespiti (hata ağacındaki üst olay ve olay ağacındaki başlatıcı olayla aynı).
- Madde B.14'te belirtildiği şekilde başlatıcı olayın nedenleri için hata ağacının geliştirilmesi ve doğrulanması. Geleneksel hata ağacında kullanılan sembollerin aynısı burada da kullanılır.
- Hangi şartların göz önünde bulundurulacağı hakkında karar verme. Bu yapı, oluşma sırası gibi mantıksal bir sıralamada olmalıdır..
- Farklı şartlara bağlı olarak sonuçlar için yolların oluşturulması. Bu yapı, olay ağacındakine benzer şekilde olmasına karşılık yol ayırmaları, üzerlerine bu ayrıma neden olan koşulun yazıldığı kutular şeklinde gösterilir.
- Her koşul kutusu için mevcut olan hatanın bağımsız olduğu kabul edilerek, her sonuç için bir olasılık hesaplanabilir. Bu da, ilk olarak her koşul kutusunun çıkışına bir olasılık tayin edilmesi (ilgili hata ağacının uygun şekilde kullanımı) ile elde edilir. Belirli bir sonuca götüren her hangi bir sıranın olasılığı, bu belirli sonucun içerisinde sonlanan, her bir koşul sırasına ait olasılıkların birbiriyle çarpımından elde edilir. Eğer, birden fazla sıralama aynı sonuç ile sonlanıyorsa, o takdirde olasılıklar birbiriyle toplanır. Bir

sıralamaya ait hata koşulların arasında bağımlılık varsa ( örneğin, bir enerji kesintisi pek çok koşulun da hata üretmesine neden olabilir), bu tür bağımlılıklar, hesaplama öncesi ele alınmalıdır.

### B.16.5 Çıktılar

Neden-sonuç analizinin çıktısı, bir sistemin, nedenlerini ve sonuçlarını göstererek nasıl hataya yol açacağına şekilsel sunumdur. Kritik olayı izleyen, her bir potansiyel sonuca ait belirli şartların oluşma olasılıklarının analizi temel alınarak elde edilen olasılık tahmini yapılır.

### B.16.6 Güçlü yanlar ve kısıtlar

Neden-sonuç analizinin avantajları, olay ağacı ve hata ağacı analizlerinin birleşmiş avantajları ile aynıdır. Bu yöntem ek olarak, zaman içerisinde gelişen olayları analiz edebilmesi ile diğer tekniklerin bazı kısıtlamalarını aşar. Neden-sonuç analizi sisteme kapsamlı bir bakış sağlar.

Bu analizin kısıtları ise, hem oluşturulması hem de sayısallaştırma sırasındaki bağımlılıklarla ilgilenilmesinden ötürü, olay ağacı ve hata ağacından daha karmaşık olmasıdır.

## B.17 Neden-ve-etki analizi

### B.17.1 Genel bakış

Neden-etki analizi istenmeyen olayların veya problemlerin olası nedenlerini belirlemek için yapılandırılmış bir yöntemdir. Olayın oluşmasına katkıda bulunan olası faktörlerini geniş kapsamlı olarak sınıflara ayırır, böylece bütün olası hipotezler dikkate alınabilir. Ancak, yöntemin kendisi, sadece gerçek delil ve hipotezlerin deneysel olarak test edilmesi ile belirlenebileceğinden, asıl nedenleri göstermez. Eldeki bilgi Balık-kılçığı (Ishikawa olarak da adlandırılır) veya ağaç gösterimi şeklinde düzenlenmelidir (bk. Ek B.17.4).

### B.17.2 Kullanım

Neden ve etki analizi, belirli bir etkiye yol açan nedenlerin listesini resimsel olarak, yapılandırılmış bir şekilde gösterimini sağlar. Etki, kapsamına göre olumlu (bir hedef) veya olumsuz (bir problem) olabilir.

Uzmanlardan oluşan bir ekip tarafından üretilen tüm olası senaryolar ve nedenlerin dikkate alınmasını sağlamak için kullanılan ve sonrasında deneysel olarak veya mevcut verilerin değerlendirilmesi ile test edilebilen gerçekleşme olasılığı en yüksek nedenler üzerinde görüş birliğinin oluşturulmasına olanak sağlar. Bir analizin başlangıç aşamasında, olası nedenler hakkında düşünce zeminini genişletmek çok değerli kabul edilir ve sonrasında olası hipotezler oluşturmak daha resmi bir şekilde dikkate alınabilir.

Neden ve etki diyagramı aşağıda belirtildiği şekilde, ihtiyaç duyulan zamanlarda oluşturulur:

- Belirli bir etki, problem veya durum için, olası kök nedenleri ve temel nedenleri belirlemek,
- Belirli bir prosesi etkileyen faktörler arasındaki etkileşimlerin bazılarını sınıflandırmak ve bunlar arasındaki ilişkiyi düzenlemek,
- Düzeltici faaliyetleri gerçekleştirebilmek için, mevcut sorunları analiz etmek.

Neden ve etki diyagramı oluşturmanın faydaları aşağıdakileri içerir:

- Gözden geçirme ekibinin dikkatini belirli bir sorun üzerinde odaklar,
- Yapılandırılmış bir yaklaşım kullanarak, soruna ait kök-nedenlerinin belirlenmesine yardımcı olur,
- Grup katılımlarını teşvik eder ve ürün veya proses için grup bilgisinin kullanımını kolaylaştırır,
- Neden ve etki ilişkilerinin diyagramı için, düzenli, kolay okunabilir bir biçimi kullanılır,
- Bir proses içerisinde oluşabilecek değişimlerin olası nedenlerini gösterir,
- Daha ileri aşama incelemeler için verilerin hangi alanlardan toplanması gerektiğini belirler.

Neden ve etki analizi, kök-neden analizini gerçekleştirmek için bir yöntem olarak kullanılabilir (bk. Madde B.12).

### B.17.3 Girdiler

Bir neden-etki analizinin girdisi, uzmanlık ve katılımcıların deneyiminden veya önceden geliştirilmiş ve geçmişte kullanılmış bir modelden gelebilir.

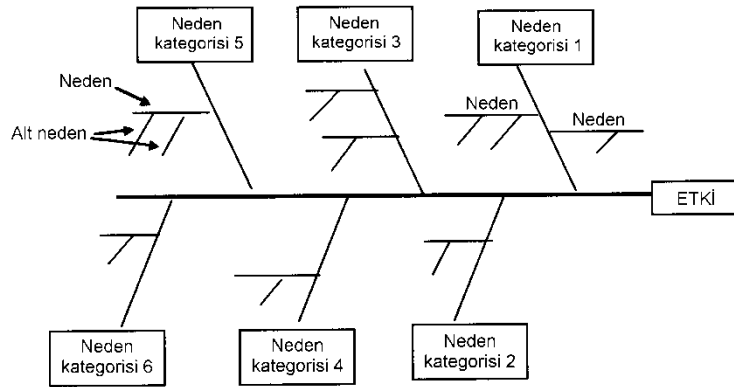
### B.17.4 Proses

Neden ve etki analizi, çözümlenmesi gereken sorun hakkında bilgi sahibi olan bir ekip tarafından yürütülmelidir.

Bir neden-etki analizi yürütülmesinin temel adımları aşağıda gösterilmiştir:

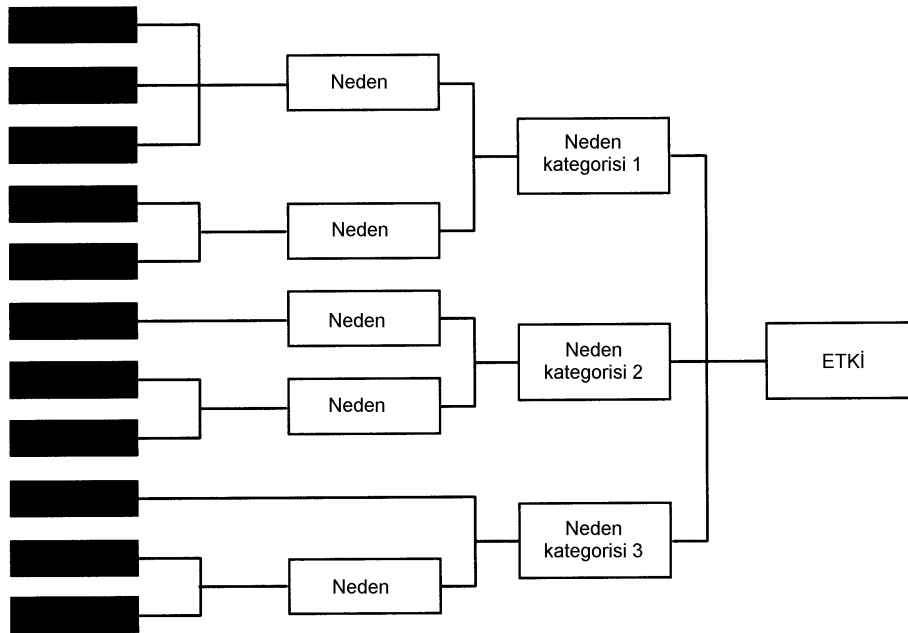


- Analiz edilecek etki belirlenir ve bir kutu içerisine yazılır. Etki koşullara bağlı olarak, olumlu (bir hedef) veya olumsuz (bir sorun) olabilir,
- Nedenlerin ana kategorileri belirlenerek, Balık-kılçığı (Fishbone) diyagramında bulunan kutularla ifade edilir. Tipik olarak, bir sistem sorunu için, kategoriler, insan, donanım, çevre, proses vb. olabilir. Bununla birlikte, kategoriler her kapsama uygun, özgün olarak seçilir,
- Aralarındaki ilişkiyi göstermek için, her ana kategoriye ait olası nedenler, dallar ve alt dallar şeklinde doldurulur,
- Niçin?" veya "buna ne neden oldu?" soruları üst üste sorularak, nedenler arası bağlantılar kurulur,
- Bütün dallar gözden geçirilerek, tutarlılık ve tamlığı doğrulanır ve elde edilen nedenlerin asıl etkiye yol açacağı güvence altına alınır,
- Mevcut deliller ve ekibin düşüncesi temel alınarak en muhtemel nedenler belirlenir.



**Şekil B.5 - Ishikawa veya Balık-kılçığı diyagramı**

Ağaç gösterimi, hata ağacına görünürde benzer şekildedir, ancak, genellikle yukardan aşağı yerine soldan sağa doğru ilerleyen yapıda geliştirilir. Bununla beraber, meydana gelme olasılıklarıyla bilinen hatalar yerine, nedenler, muhtemelen katkı sağladıkları tepe olayın olasılığını üretebilmek için sayısallaştırılmazlar.



**Şekil B.6 - Neden-ve-Etki analizi örnek ağaç formülasyonu**

Neden-ve-etki diyagramları genellikle niteliksel olarak kullanılır. Sorunun oluşma ihtimali 1 olarak kabul edilerek, genel nedenlere olasılıklar ve sonrasında, ne derecede ilgili olduklarına göre alt nedenlere tayin edilebilir. Ancak, katkıda bulunan öğeler sık sık karmaşık yapılarda etkileşim içerisinde girerek sayısallaştırmayı geçersiz hale getirir.

### B.17.5 Çıktılar

Neden-ve-etki analizini çıktısı olası ve muhtemel nedenleri gösteren Balık-kılıçığı ya da ağaç diyagramıdır. Bu yapı, öneriler yapılmadan önce deneysel olarak doğrulanabilir.

### B.17.6 Güçlü yönler ve kısıtlar

Güçlü yönler aşağıdakileri içerir:

- Uygun uzmanların ekip ortamında çalışmaya katılması,
- Yapılandırılmış analizi,
- Olası tüm hipotezlerin dikkate alınması,
- Sonuçların okunması kolay grafiksel olarak gösterimi,
- Daha fazla verinin ihtiyaç olduğu alanların belirlenmesi,
- İstenen etkiye olduğu kadar istenmeyen etkiye de katkı veren öğelerin belirlenmesi için kullanılabilir. Bir sorun hakkında olumlu şekilde odaklanılması daha fazla sahiplenme ve katılımı teşvik edebilir.

Kısıtlar aşağıdakileri içerir:

- Ekip yeterli uzmanlığa sahip olmayabilir;
- Tek başına tam bir proses olmadığı için, öneriler oluşturabilmek için kök-neden analizinin bir parçası olması gerekir,
- Ayır bir analiz tekniğinden ziyade beyin fırtınası için kullanılan gösterim tekniğidir,
- Analizin başlangıcında, nedensel faktörlerin kategorilere ayrılması, kategoriler arasındaki etkileşimlerin yeterli derecede dikkate alınmadığı anlamına gelebilir, örneğin insan hatası nedeni ile oluşan donanım hatası veya yetersiz tasarım nedeniyle oluşan insan sorunlarından kaynaklanır.

## B.18 Koruma katmanları analizi (LOPA)

### B.18.1 Genel bakış

Koruma katmanları analizi (LOPA), istenilmeyen bir olay veya senaryo ile ilişkili risklerin tahmininde kullanılan yarı-sayısal bir yöntemdir. Bu riski kontrol etmek veya riskini azaltmak için yeterli önlemlerin olup olmadığını analiz eder.

Neden-sonuç ilişki çifti seçilir ve istenmeyen sonuçlara yol açan nedenlerden korumayı sağlayan katmanları tanımlanır. Riskin tolere edilebilir seviyeye indirmek için uygun korumanın bulunup bulunmadığını belirlemek amacıyla büyüklük sırası hesaplaması gerçekleştirilir.

### B.18.2 Kullanım

LOPA basitçe tehlike veya olay ile sonuç arasında koruma katmanlarını niteliksel olarak gözden geçirmek için kullanılabilir. Normal olarak, yarı-sayısal yaklaşım kullanılarak, örneğin HAZOP veya PHA sonrasında gerçekleştirilecek inceleme sürecine daha fazla kesinlik kazandırılabilir.

LOPA, IEC 61508 serisinde ve IEC 61511'de açıklandığı gibi, aletli sistemler için bağımsız koruma katmanları (IPLs) ve güvenlik bütünlüğü seviyelerinin (SIL) şartlarını belirlemek için bir temel sağlar. LOPA, her bir koruyucu katman tarafından üretilen risk azaltmasını analiz ederek, risk azaltma kaynaklarını etkili bir şekilde dağıtmaya yardımcı olması için kullanılabilir.

### B.18.3 Girdiler

LOPA için girdiler aşağıdakileri içerir:

- PHA tarafından sağlanana benzer şekilde, tehlikelerin, nedenlerin ve sonuçların da dâhil olduğu riskler hakkında temel bilgi,
- Mevcut ya teklif edilen kontroller hakkında bilgi,
- Tesadüfi olay sıklıkları, koruma katmanı hata olasılıkları, sonuç ölçümleri ve tolere edilebilir riskin tanımı,
- Başlatan nedenlerin sıklıkları, koruma katmanı hata olasılıkları, sonuç ölçümleri ve tolere edilebilir riskin tanımı.

### B.18.4 Proses

LOPA, aşağıdaki prosedürü uygulayan uzman bir ekip tarafından yürütülür:

- İstenmeyen bir sonucu başlatan nedenlerin belirlenmesi ve bu nedenlerin oluşma sıklıkları ve sonuçları ile ilgili verilerin toplanması,
- Bir neden-sonuç çiftinin seçilmesi,
- Nedenlerin istenmeyen sonuçlara götürmesini engelleyen koruma katmanlarının belirlenmesi ve etkinliğinin analiz edilmesi,
- Her bir IPL için hata olasılığının tahmin edilmesi,
- Her bir IPL için belirlenen hata olasılığı, başlatıcı nedenin oluşma sıklığı ile ve koşullu değişticiler (koşullu değiştirici, örneğin bir kişinin o anda bulunup bulunmayacağına göre etkilenip etkilenmeyeceği) birleştirilerek, istenmeyen sonucun oluşabilme sıklığı belirlenir. Büyüklük sıraları, sıklıklar ve olasılıklar için kullanılır,
- Daha fazla korumanın gerekli olup olmadığını belirlemek amacıyla, hesaplanan risk seviyesi risk toleransı seviyesi ile karşılaştırılır.

Soruna yol açan olaydan ve diğer koruma katmanlarından bağımsız olarak IPL, bir senaryonun istenmeyen sonuçlara ilerlemesini engelleme yeteneği bulunan cihaz, sistem veya bir faaliyettir.

Bağımsız koruma katmanları (IPLs) aşağıdakileri içerir:

- Tasarım özellikleri,
- Fiziksel koruma cihazları,
- Güvenlik kilidi ve kapatma sistemleri,
- Kritik alarmlar ve manuel müdahaleler,
- Olay sonrası fiziksel koruma,
- Acil durum müdahale sistemleri (prosedürler ve incelemeler IPL değildir).

### B.18.5 Çıktılar

Alınması gereken ek kontroller ve riskleri azaltmak için bu kontrollerin etkinliğini hakkında öneriler verilmeli. LOPA, güvenlikle ilişkili/aletli sistemleri ilgilendiren, SIL değerlendirmesi için kullanılan bir tekniktir.

### B.18.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar aşağıdakileri içerir:

- Hata ağacı analizinde veya tamamen sayısal risk değerlendirmesine göre daha az zaman ve kaynak gerektirir, ancak niteliksel sübjektif yargılamaya göre daha kesindir,
- En kritik koruma katmanları üzerindeki kaynakların belirlenmesine ve bu kaynaklara odaklanılmasına yardımcı olur,
- Yetersiz önlemlerin bulunduğu yerlerde, işletimleri, sistemleri ve prosesleri belirler,
- En ciddi sonuçlar üzerinde odaklanır.

Kısıtlar:

- LOPA neden-sonuç çiftine ve her seferde bir senaryo üzerine odaklanır. Riskler veya kontroller arasındaki karmaşık etkileşimler kapsamaz,
- Sayısallaştırılmış riskler, alışılmış hata durumlarını içermeyebilir,
- Ortak mod hataları için sayısallaştırılmış riskler dikkate alınmaz,
- LOPA, çok fazla neden-sonuç çiftinin veya farklı paydaşları etkileyen çeşitli sonuçların bulunduğu durumlar gibi çok karmaşık senaryolarda uygulanamaz.

### B.18.7 Kaynak dokümanlar

IEC 61508 (tüm bölümleri), *Güvenlikle ilgili elektrikli veya elektronik veya programlanabilir elektronik sistemlerde fonksiyonel güvenlik*

IEC 61511, Fonksiyonel güvenlik - Proses sanayi sektörü için güvenlik enstrümanlı sistemler

## B.19 Karar ağacı analizi

### B.19.1 Genel bakış

Bir karar ağacı, belirsizlik sonuçlarını da dikkate alarak, karar seçeneklerini ve sonuçlarını sıralı bir biçimde temsil eder. Olay ağacındakine benzer şekilde başlatıcı bir olay veya ilk karar ile başlayıp, oluşabilecek farklı olayları ve verilebilecek farklı kararlara ulaştıran yolları sonuç olarak modeller.

**B.19.2 Kullanım**

Karar ağacı, proje risklerini yönetmek için ve belirsizliğin bulunduğu diğer durumlarda en iyi hareket yönünü seçmeye yardımcı olmak için kullanılır. Grafik gösterimi de verilen kararların nedenleri hakkında bilgilendirme yapmak için yardımcı olabilir.

**B.19.3 Girdiler**

Karar verme noktalarını içeren bir proje planı. Kararların muhtemel sonuçları ve kararları etkileyebilecek olasılık dâhilindeki olaylar hakkında bilgi.

**B.19.4 Proses**

Karar ağacı ilk alınan kararlar başlar, örneğin, proje B yerine proje A ile devam edilmesi. Her iki projenin hayali olarak ilerletilmesi ile farklı olaylar oluşacak ve farklı öngörülebilir kararlar verilmesi gerekecektir. Bu yapı, olay ağacına benzer ağaç şeklinde gösterilir. Olayların oluşma ihtimalleri, sonuç çıktısının maliyeti veya kullanımı ile birlikte yol boyunca tahmin edilebilir.

Her iki proje varsayımına dayalı olarak ilerledikçe farklı olaylar meydana gelecek ve farklı öngörülebilir kararlar verilmesi gerekecektir. Bu yapı, olay ağacına benzer ağaç şeklinde gösterilir. Olayların meydana gelme ihtimalleri, sonuç çıktısının maliyeti veya kullanımı ile birlikte izlenen yol boyunca tahmin edilebilir.

En iyi karar yolu ile ilgili bilgiler, mantıksal yolun ve sonuç değeri boyunca bütün koşullu olasılıkların ürünü olarak hesaplanan en yüksek beklenen değeri üretmesidir.

**B.19.5 Çıktılar**

Çıktılar aşağıdakileri içerir:

- Tercih edilebilecek farklı seçeneklerin sunulmasından oluşacak riskin mantıksal analizi,
- Her bir muhtemel yol için beklenen değer hesaplaması.

**B.19.6 Güçlü yanlar ve kısıtlar**

Güçlü yanlar aşağıdaki gibidir:

- Karar sorununa ait ayrıntıların grafiksel gösterimini sağlar,
- Karar verilmesi gereken soruna ait ayrıntıların net bir grafiksel gösterimini sağlar,
- Bir duruma ait en iyi yolun hesaplanmasına imkân verir.

Kısıtlara dâhil olanlar:

- Büyük karar ağaçları, diğer kişileri kolayca bilgilendirmek için çok karmaşık hale gelebilir,
- Bir ağaç diyagramı olarak gösterebilmek için, durumu aşırı basitleştirme eğilimi olabilir.

**B.20 İnsan güvenirlilik değerlendirme (HRA)****B.20.1 Genel bakış**

İnsan güvenirlilik değerlendirme (HRA), sistem performansı üzerindeki insan etkisi ile ilgilendirir ve sistem üzerindeki insan hatası etkilerini kıyaslamak için kullanılabilir.

Pek çok proses, özellikle işletimcinin karar vermesi için gerekli zamanın az olduğu durumlarda, insan hatası ihtimali taşır. Sorunların büyüyerek ciddi duruma gelmesi ihtimali az düşük olabilir. Ancak bazen, bir başlangıç hatasının büyüyerek kaza halini almasını engellemek için insan faaliyeti, tek savunma çeşidi olabilir.

HRA'nın önemi, kritik insan hatalarının felaketler zincirine nasıl katkıda bulunduğu çeşitli kazalarda kazaların örneklendirilmesiyle gösterilmektedir.

Bu tür kazalar, bir sistemde sadece donanım ve yazılım üzerinde odaklanan risk değerlendirmeleri için uyarı niteliğindedir. Bu kazalar, insan hatası katkısının göz ardı edilmesinin tehlikelerini gösterir. Bu kazalar, insan hatası katkı olasılığının göz ardı edilmesinin doğuracağı tehlikeleri gösterir. İlave olarak, HRA'lar verimliliği azaltacak hataların vurgulanması için kullanılırken, bu ve diğer hataların (donanım ve yazılım), işletimcileri ve bakım personeli tarafından nasıl "düzeltilebileceğini" de açığa çıkarır.

**B.20.2 Kullanım**

HRA, niteliksel olarak da sayısal olarak da kullanılabilir. Niteliksel olarak, insan hatası olasılığı ve nedenlerinin belirlenmesi ile hata olasılığı azaltılabilir. Sayısal olarak kullanıldığında ise, HRA insan hataları hakkında FTA veya diğer tekniklere veri sağlar.

**B.20.3 Girdiler**

İnsan güvenilirlik değerlendirmesinin (HRA) girdileri aşağıdakileri içerir:

- İnsanların gerçekleştirilmesi gereken görevlerin tanımlanması için bilgi,
- Uygulamada meydana gelen hata çeşitleri ve hata potansiyeli ile ilgili deneyim,
- İnsan hataları ve bu hataların sayısal değeri hakkında uzmanlık.

**B.20.4 Proses**

İnsan güvenilirlik analizi, aşağıdaki şekilde gerçekleştirilir:

- **Problem tanımlama:** Araştırılması/değerlendirilmesi gereken insan etkisi tipleri nelerdir?
- **Görev analizi:** Görev nasıl gerçekleştirilir ve performansı desteklemek için ne tür yardımlara ihtiyaç duyulur?
- **İnsan hatası analizi:** Görev performansı nasıl hata verir: ne tür hatalar meydana gelebilir ve bu hatalar ve nasıl düzeltilebilirler?
- **Sunum:** Bu hatalar veya görev performans hataları; bütün sistem hata olasılıklarının hesaplanmasını mümkün kılmak amacıyla diğer donanım, yazılım ve çevresel olaylarla nasıl entegre edilir?
- **Görüntüleme:** Ayrıntılı sayısallaştırma gerektirmeyen herhangi bir hata veya görevleri var mı?
- **Sayısallaştırma:** Görevlere ait bireysel hatalar ve bu hatalara bağlı başarısızlıkların olasılıkları nelerdir?
- **Etki Değerlendirme:** Hangi hatalar veya görevler en önemlidir? Yani güvenilirlik veya riske en büyük katkıyı hangisi verir?
- **Hata azaltma:** Daha fazla insan güvenirliliği nasıl elde edilebilir?
- **Dokümantasyon:** HRA'nın hangi ayrıntıları dokümante edilmelidir?

Uygulamada, bazen parçalar (örneğin, görev analizleri ve hata belirlenmesi) birbiri ile paralel olarak ilerlemesine rağmen, HRA prosesi adım adım ilerler.

**B.20.5 Çıktılar**

Çıktılar aşağıdakileri içerir:

- Meydana gelebilecek hataların ve bu hataları azaltabilecek yöntemlerin listesi - tercihen sistemin yeniden tasarlanması aracılığıyla,
- Hata modları, hata türleri, nedenleri ve sonuçları,
- Hatalar sonucu ortaya çıkan risklerin niteliksel veya sayısal değerlendirilmesi.

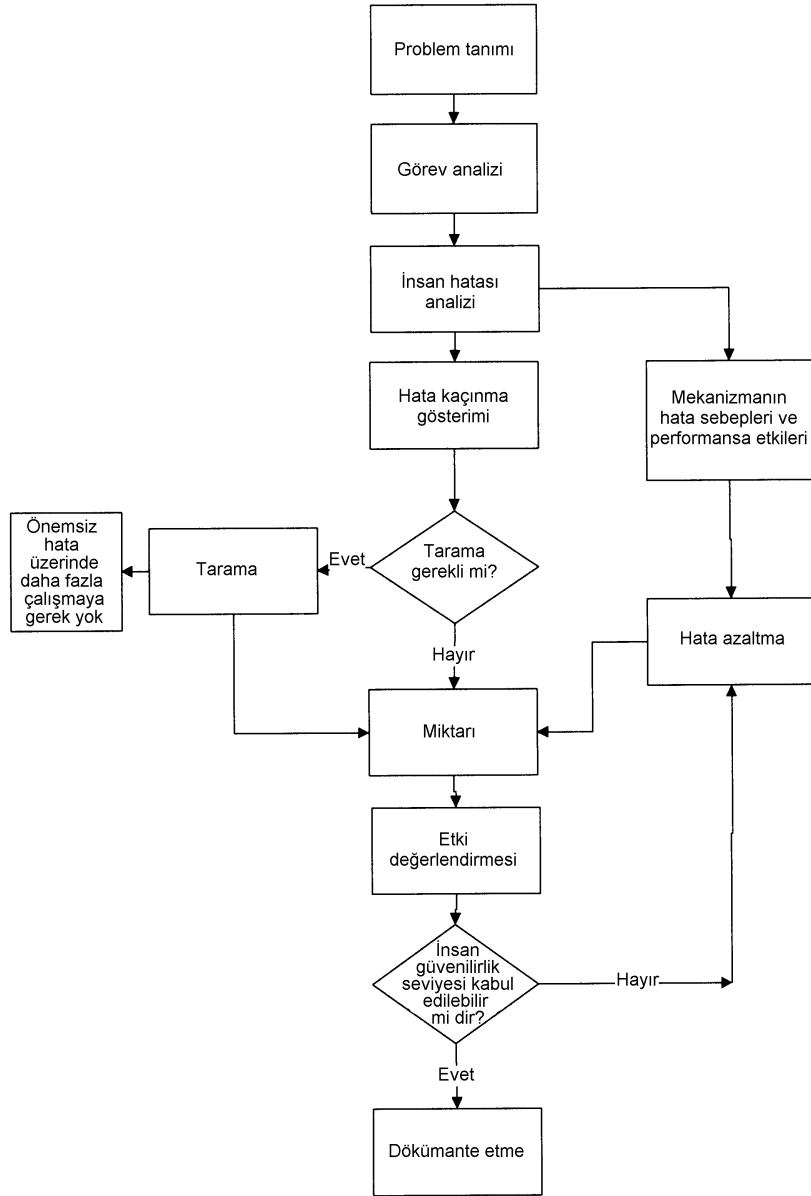
**B.20.6 Güçlü yanlar ve kısıtlar**

HRA'nın güçlü yanları aşağıdaki gibidir:

- İnsanların önemli rol oynadığı yerlerde, sistemle bağlantılı risklerin göz önünde bulundurulmasında HRA, meydana gelen insan hatasını kapsamaya yönelik uygun bir mekanizma sağlar.
- İnsan hata modlarının ve mekanizmalarının uygun olarak göz önünde bulundurulması hata nedeniyle oluşacak arıza olasılığını azaltmaya yardımcı olabilir.

Kısıtlar aşağıdakileri içerir:

- İnsanların değişkenliği ve karmaşıklığı, basit hata modlarını ve olasılıklarını tanımlamayı zorlaştırır,
- İnsanların pek çok faaliyeti basit bir başarı/hata moduna sahip değildir. İnsan güvenilirlik analizi, kalite hatası veya karar vermede meydana gelen kısmi hatalar veya hataları belirlemede güçlük çeker.



Şekil B.7 - İnsan güvenilirlik değerlendirme örneği

## B.21 Papyon analizi

### B.21.1 Genel bakış

Papyon analizi, nedenlerden sonuçlara kadar bir riskin yollarının tanımlanması ve analiz edilmesi için basit şekilsel bir gösterim yöntemidir. Bir olayın (papyonun düğümü ile gösterilen) nedenlerini analiz eden hata ağacı ile sonuçları analiz eden olay ağacının birleşimi olarak düşünülebilir. Ancak, papyon analizi; nedenler-risk ve risk-riskin sonuçları arasındaki engellere odaklanır. Papyon diyagramları hata ve olay ağacından başlayarak oluşturulabilir, ancak çoğunlukla yapılan bir beyin fırtınası sonrasında doğrudan çizilir.

### B.21.2 Kullanım

Papyon analizi, olası nedenleri ve sonuçların sıralamasını gösteren bir riski görüntülemek için kullanılır. Papyon analizi, tam bir hata ağacı analizinin karmaşıklığına izin vermediği durumlarda veya her hata yolu üzerinde bir engel veya kontrolün bulunmasını güvence altına almaya odaklanılması gerektiği durumlarda kullanılır. Hataya yol açan belirgin bağımsız yolların bulunduğu yerlerde daha kullanışlıdır.

Papyon analizi, genellikle hata ağacı ve olay ağacına göre anlaşılması daha kolaydır ve dolayısıyla daha karmaşık teknikler kullanılarak elde edilen analizlerde faydalı bir iletişim aracı olabilir.

### B.21.3 Girdiler

Bir risk ve engellerin nedenleri ve sonuçları ve bu risk ve engelleri önleyebilen, azaltabilen veya harekete geçirebilen kontroller ile ilgili bilgilerin anlaşılması gereklidir.

### B.21.4 Proses

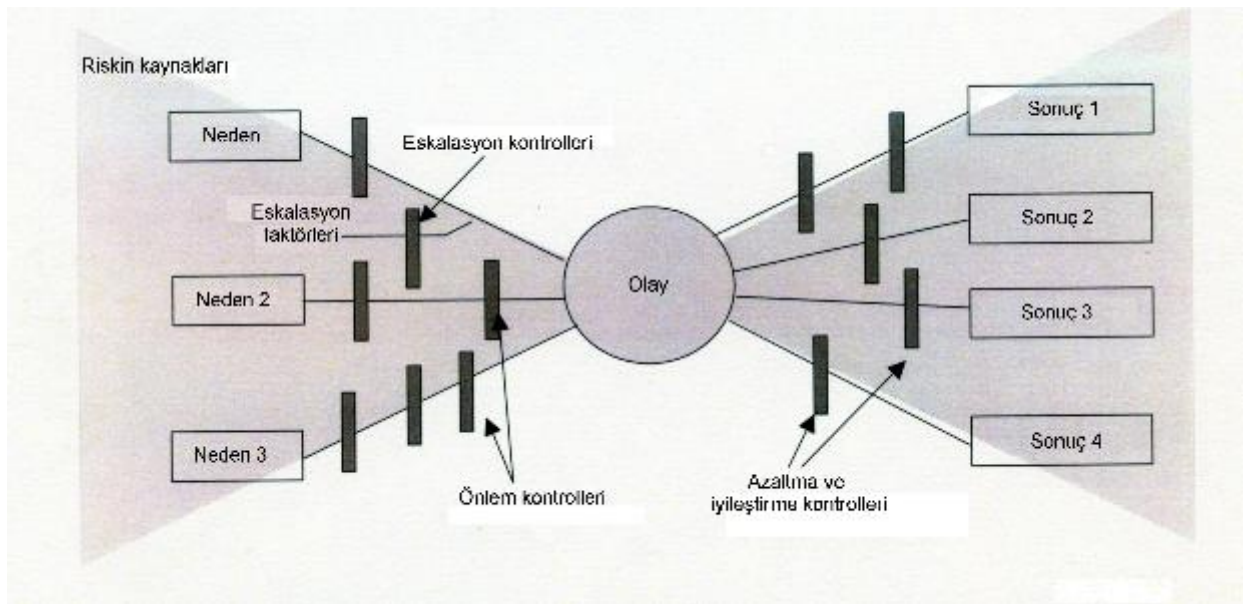
Papyon diyagramı aşağıdaki şekilde çizilir:

- Belirli bir risk, bir papyon merkez düğümü olarak temsil ve analiz edilmek üzere tanımlanır.
- Olayların nedenleri, risk kaynakları (veya güvenlik kapsamındaki tehlikeler) göz önünde bulundurularak listelenir.
- Risk kaynağının kritik olaya yol açan mekanizması belirlenir.
- Papyonun sol tarafını oluşturmak için her bir neden ve olay arasına bir çizgi çizilir. Artmasına yol açacak faktörler (eskalasyon faktörleri) belirlenebilir ve diyagrama dâhil edilebilir. Bu yaklaşım; çubukların olayın oluşumunu harekete geçiren "kontrolleri" yansıtması durumunda, olumlu sonuçlar için kullanılabilir.
- Papyonun sağ tarafında, riske ait farklı potansiyel sonuçları belirlenir ve risk olayından her bir potansiyel sonuca gidecek şekilde bir çizgi çekilir.
- Sonuç engelleri, radyal çizgileri boyunca dikey çubuklar olarak tasvir edilir. Bu yaklaşım; çubukların, olayın oluşumunu destekleyen kontrolleri yansıtması durumunda, olumlu sonuçlar için kullanılabilir.
- Kontrolleri destekleyen yönetim fonksiyonları (örneğin, eğitim ve muayene) papyonun altında gösterilebilir ve ilgili kontrol ile bağlantılı olabilir.

Papyon diyagramına ait bazı sayısalştırma seviyelerinde, yolların birbirinden bağımsız olduğu yerlerde, belirli bir sonuç veya çıktının olasılığının bilinmesi mümkün olabilir ve kontrolün etkinliğinin tahmin edilebilmesi için bir figür kullanılabilir. Bununla birlikte, pek çok durumda, yollar ve engeller birbirinden bağımsız değildir ve kontroller bir prosedür şeklinde olabilir ve bu nedenle de etkinlikleri belirsizdir. Sayısalştırma daha uygun bir şekilde Hata Ağacı Analizi (FTA) ve Olay Ağacı Analizi (ETA) kullanılarak gerçekleştirilir.

### B.21.5 Çıktı

Çıktı, istenmeyen sonuçları önlemek veya azaltmak veya istenilen sonuçları teşvik etmek ve desteklemek amacıyla, ana risk yollarını ve engellerin yerlerini gösteren basit bir diyagramdır.



Şekil B.8 - İstenmeyen sonuçlar için kullanılan Papyon (Bow tie) diyagramı

**B.21.6 Güçlü yanlar ve kısıtlar**

Papyon analizinin güçlü yanları aşağıdaki gibidir:

- Anlaşılması kolaydır ve problem ile ilgili açık resimsel bir sunum sağlar,
- Dikkati, engelleme ve azaltma amaçlı kurgulanan kontrollere ve bunların etkinliği üzerine odaklanır,
- İstenilen sonuçlar için kullanılabilir,
- Kullanımı yüksek bir uzmanlık seviyesi gerektirmez.

Kısıtlar aşağıdakileri içerir:

- Eşzamanlı olarak çoklu nedenlerin meydana geldiği yerlerde, sonuçların nedenlerini gösteremez (örneğin, papyonun sol tarafını tasvir eden, hata ağacındaki Ve Kapıları'nın bulunduğu yerlerde),
- Özellikle sayısallaştırmanın denendiği karmaşık durumları fazlaca basitleştirebilir.

**B.22 Güvenirlilik merkezli bakım****B.22.1 Genel bakış**

Güvenirlilik merkezli bakım (RCM), gerekli olan güvenliği, erişebilirliği ve her türlü donanım için işletim ekonomisini, etkin ve verimli bir şekilde tesis edebilmek için hataları yönetmek amacıyla uygulanması gereken politikaları belirlemeyi sağlayan bir yöntemdir.

RCM günümüzde, çok çeşitli endüstriyel alanda kullanılan, ispatlanmış ve kabul edilmiş bir yöntemdir.

RCM, donanım için, belirlenebilir hataların güvenlik, işletimsel ve ekonomik sonuçlarına ve bu hataların sorumlu olduğu bozulma mekanizması ile uyumlu olarak, donanım için uygulanabilir ve etkin önleyici bakım şartlarını belirlemek için bir karar verme süreci sağlar. Proses boyunca yapılan çalışmaların sonucu, bir bakım görevi veya işletim değişiklikleri gibi bir başka faaliyetin gerekli olup olmadığı hakkında görüş oluşturulmasıdır. Proses boyunca yapılan çalışmaların sonucu, bir bakım görevi veya işletimsel değişiklikler gibi diğer faaliyetler ile gerçekleştirme gerekliliği ilgili olarak verilen nihai karardır.

RCM'in kullanımı ve uygulama ile ilgili ayrıntılar IEC 60300-3-11'de sunulmuştur.

**B.22.2 Kullanım**

Bütün görevler, personel ve çevreye ilişkin güvenlik hususuna ve işletimsel veya ekonomik gerekçelere dayanır. Bununla birlikte göz önünde bulundurulacak kriterler ürünün doğasına ve bu ürün/hizmetin uygulanmasına bağlıdır. Örneğin, bir üretim süreci ekonomik olarak uygulanabilir ve katı çevresel kurallara karşı hassas olabilir, diğer taraftan, daha az bağlayıcı güvenlik, ekonomik ve çevresel kriterlere sahip olmalıdır. En büyük fayda, hataların nerede ciddi bir güvenlik, çevresel, ekonomik veya işletimsel etkiye sahip olduğunun analiz edilmesi hedeflendiğinde elde edilir.

RCM uygulanabilir ve efektif bir bakım gerçekleştirildiğinin garantiye alınması için kullanılabilir ve bu yöntemde genelde tasarım ve geliştirme aşamasında başvurulur ve sonrasında da işletim ve bakım boyunca uygulanır.

**B.22.3 Girdiler**

Başarılı bir RCM uygulaması, donanımın ve yapısının, işletimsel çevrenin ve ilişkili sistemlerin, alt sistemlerin ve olası hatalar ve bu hataların sonuçları ile birlikte donanımın iyi bir şekilde anlaşılmasını gerektirir.

**B.22.4 Proses**

Güvenirlilik merkezli bakım (RCM) programının temel adımları aşağıdaki gibidir:

- Başlama ve planlama,
- Fonksiyonel hata analizi,
- Görev seçimi,
- Uygulama,
- Sürekli gelişme.

RCM risk tabanlı olup, risk değerlendirmesinin temel adımlarını takip eder. Risk değerlendirme türü, hata modu, etki ve kritiklik analizidir (FMECA) ancak, bu bağlamda kullanıldığı zaman özel bir yaklaşım gerektirir.

Risk belirleme, bakım görevlerinin gerçekleştirilmesi ile etkinin ve/veya oluşma sıklığını sonuç açısından ortadan kaldıracak veya azaltılabilecek potansiyel hataların bulunduğu durumlara odaklanır. Gerekli fonksiyonları ve performans standartları ile donanım hataları ve bu donanımların fonksiyonlarını kesintiye uğratabilecek bileşen hatalarının belirlenmesi ile uygulanır.



Risk analizi; bakım gerçekleştirilmeksizin her bir hatanın oluşabilme sıklığını tahmin etmeyi içerir. Sonuçlar, hata etkilerinin tanımlanması aracılığıyla oluşturulur. Hata sıklığı ile hata sonuçlarını birleştiren bir risk matrisi, risk seviyesi kategorilerinin oluşturulması sağlar.

Sonraki adımda, her bir hata durumu için, gerekli hata yönetimi politikasının seçilmesi ile risk değerlendirmesi gerçekleştirilir.

Risk kıyaslama, her bir hata modu için uygun hata yönetimi politikası seçilerek gerçekleştirilir.

Bütün RCM süreci, ileride başvurmak ve gözden geçirmek üzere kapsamlı olarak dokümanite edilir. Hata ve bakımla ilişkili verilerin toplanması, sonuçların izlenmesini ve gelişmelerin uygulanmasını sağlar.

### **B.22.5 Çıktı**

RCM, mevcut durumu izleme, planlı onarım, planlı değişim, hata-bulma veya önleyici olmayan bakım görevlerinin tanımlanmasını sağlar. Analizden kaynaklanan diğer muhtemel faaliyetler; yeniden tasarım, işletim veya bakım prosedürleri değişiklikleri veya ilave eğitimler gibi faaliyetleri içerebilir. Görev aralıkları ve gerekli kaynaklar ayrıca belirlenir.

### **B.22.6 Kaynak dokümanlar**

IEC 60300-3-11, *Güvenilirlik yönetimi - Bölüm 3: Uygulama kılavuzu - Kısım 11: Güvenilirlik merkezli bakım*

## **B.23 Sızıntı analizi (SA) ve Devre sızıntı analizi (SCI)**

### **B.23.1 Genel bakış**

Sızıntı analizi (SA) tasarım hatalarını belirlemek için kullanılan bir yöntemdir. Sızıntı durumu; istenmeyen bir olayın meydana gelmesine neden olabilen veya istenilen bir olayı baskılayabilen; bileşen hatasından kaynaklanmayan gizlenmiş (saklı) bir donanım, yazılım veya her ikisinin bütünleşik bir durumdur. Bu durumlar, rastgele doğaları ve en ayrıntılı standart sistem testleri sırasında bile tespit edilememeleri yeteneği ile nitelendirilirler. Sızma durumları, yanlış işleyiş, sisteme erişebilirlik kaybı, program gecikmelerine hatta personelin ölümüne veya yaralanmasına neden olabilir.

### **B.23.2 Kullanım**

Devre sızıntı analizi (SCA), tasarımların bütünlüğünü ve fonksiyonelliğini doğrulamak için NASA tarafından 1960'ların sonunda geliştirilmiştir. Elektriksel devre yollardaki istenilmeyen gizli hatları keşfetmek için faydalı bir araçtır ve her bir fonksiyonun izole edilmesinde kullanılan çözümleri üretmeye yardımcı olmuştur. Ancak, teknoloji geliştikçe, aynı zamanda devre sızıntı analizinde kullanılacak araçlar da geliştirilmek zorunda kalmıştır. Sızıntı analizinin, devre sızıntı analizini de içine alan ancak bundan çok daha fazla gelişmiş bir kapsamı vardır. Herhangi bir teknolojiyle üretilen hem donanım hem de yazılımlardaki sorunları belirleyebilir. Sızıntı analizi araçları; hata ağaçları, hata modları ve etki analizi (FMEA), güvenilirlik tahminleri vs. gibi birden çok farklı analizi, zaman ve proje maliyetinden tasarruf sağlamak amacıyla tek bir analizle birleştirilebilir.

### **B.23.3 Girdiler**

Sızıntı analizi; belirli bir tipteki problemi bulmak amacıyla, farklı araçları (örneğin, ağ ağaçları, ormanlar ve sızıntı durumunu belirlemek için analiste yardımcı olan ipuçları veya sorular) kullanması bakımından, tasarım prosesinin benzersiz formudur. Ağ ağaçları ve ormanlar, gerçek bir sistemin topolojik gruplamasıdır. Her ağ ağacı, bir alt fonksiyonu temsil eder ve fonksiyonun çıktılarını etkileyebilecek bütün girdileri gösterir. Ormanlar, belirli bir sistem çıktısına katkı sağlamak amacıyla, ağ ağaçlarının birleştirilmesi ile oluşur. Uygun bir orman, ilgili bütün girdiler açısından sistem çıktısını gösterir. Bunlar, diğerleri ile birlikte analize girdi oluşturur.

### **B.23.4 Proses**

Bir sızıntı analizinin temel adımları aşağıdakilerden oluşur:

- Veri hazırlama,
- Ağ ağacının yapılandırılması,
- Ağ yollarının kıyaslanması,
- Nihai tavsiyeler ve rapor.

### **B.23.5 Çıktı**

Bir sızıntı devresi, belirli koşullar altında, istenmeyen bir fonksiyonu başlatabilecek veya istenen bir fonksiyonu engelleyebilecek, sistem içerisindeki beklenmeyen bir yol veya mantık akışıdır. Bu yol; donanım, yazılım, işletim

faaliyetleri veya bunların birleşimi olabilir. Sızıntı devreleri donanım hatasının sonucu değil, ancak sistemin dikkatsizce tasarlanmış, yazılım programı içine kodlanmış veya insan hatası tarafından tetiklenen gizli durumlardır. Sızıntı devrelerinin dört türü bulunur:

- Sızıntı yolları: İstenmeyen bir yöne giden, akım, enerji veya mantıklı sıralama akışları boyunca beklenmeyen yollar,
- Sızıntı zamanlaması: Beklenmeyen veya çakışan şekilde meydana gelen olaylar,
- Sızıntı göstergeleri: Sistemi veya operatörü istenmeyen bir faaliyete götüren işletim koşullarına neden olacak, sistemin belirsiz veya yanlış gösterimi,
- Sızıntı etiketleri: Sistem fonksiyonlarının yanlış veya kesin olmayacak şekilde etiketlenmesi, örneğin; sistem girdileri, kontrolleri veya işletimcinin sisteme yanlış uyarı girmesine neden olan görüntüleme araçları.

### B.23.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar aşağıdaki gibidir:

- Sızıntı analizi tasarım hatalarının tespiti için uygun bir yöntemdir,
- HAZOP analizi ile birlikte uygulandığında en iyi şekilde çalışır,
- Toplu ve yarı toplu tesis gibi birden fazla çalışma durumuna sahip olan sistemler ile ilgilenmek için çok uygundur.

Kısıtlar aşağıdakileri içerir:

- Proses; elektrik devrelerine, üretim tesislerine, mekanik donanıma veya yazılım gibi uygulanıp uygulanmadığı alana bağlı olarak, değişiklikler içerir,
- Yöntemin doğru çalışması, doğru ağ ağaçlarının oluşturulmasına bağlıdır.

### B.24 Markov analizi

#### B.24.1 Genel bakış

Markov analizi, bir sistemin gelecekteki durumu sadece şu andaki durumuna bağlı ise kullanılır. Genellikle birden çok halde bulunabilen, tamir edilebilir sistemlerin analizi için ve güvenilirlik blok analizinin sistemi yeterli derecede analiz etmeye uygun olmadığı durumlarda kullanılır. Bu yöntem, daha karmaşık sistemler için ileri derecede Markov proseslerine genişletilebilir ve sadece model, matematiksel hesaplamalar ve varsayımlar ile sınırlıdır.

Markov analizi prosesi sayısal bir tekniktir ve ayırık (durumlar arasındaki değişiklik olasılıklarını kullanarak) veya sürekli (durumlar arası değişiklik oranını kullanarak) olabilir.

Markov analizi el ile hesaplamaya uygun olmasına rağmen, tekniğin doğası gereği birçoğu piyasada bulunan bilgisayar programlarının kullanımında kendisine daha fazla yer bulur.

#### B.24.2 Kullanım

Markov analizi, onarım olsun veya olmasın, çeşitli sistem yapılarında kullanılabilecek bir analiz tekniğidir, bazıları:

- Paralel çalışan bağımsız bileşenler,
- Seri çalışan bağımsız bileşenler,
- Yük-paylaşım sistemleri,
- Aktarım hatalarının meydana gelebileceği durumları içeren askı (stand-by) sistemleri,
- Bozulmuş sistemler.

Markov analiz tekniği, onarım için kullanılan yedek parçaları dikkate alınması dâhil erişilebilirliği hesaplamak için de kullanılabilir.

#### B.24.3 Girdiler

Markov analizi için gerekli olan girdiler aşağıdaki gibidir:

- Sistem, alt sistem veya bileşenlerin içinde bulunabileceği çeşitli durumların listesi (tam işletimsel, kısmı

- işletimsel (bozulmuş durum), hata durumu vs. gibi),
- Modellenmesi için gerekli olan olası geçişlerin açıkça anlaşılması. Örneğin, bir araba lastiğinin arızasında, yedek lastiğin mevcut durumunun ve dolayısıyla muayene sıklığının göz önünde bulundurulmasını gerektirir,
- Bir durumdan diğer duruma değişim oranı; ya kesikli olaylar için durumlar arasındaki değişiklik olasılığı ile veya sürekli olaylar için hata oranı ( $\lambda$ ) ve/veya onarım oranı ( $\mu$ ) ile temsil edilir.

#### B.24.4 Proses

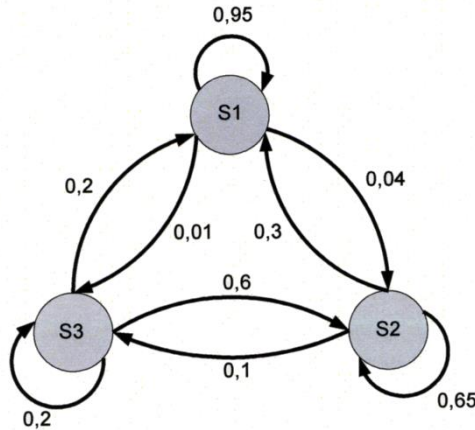
Markov analizi, “durumlar” şartı, örneğin “erişilebilir” ve “hata” kavramı etrafında odaklıdır ve zamanla bu iki durum arasındaki geçiş, sürekli bir değişim olasılığı temeli üzerine kurgulanmış bir tekniktir. Bir rastgele geçişli olasılık matrisi, çeşitli çıktılarının hesaplanmasına izin veren durumların her biri arasındaki geçişi tanımlamak için kullanılır.

Markov analizi tekniğini açıklamak için, sadece çalışma, azaltma ve hata gibi 3 durumda olabilen ve sırasıyla S1, S2, S3 olarak adlandırılan karmaşık bir sistem düşünün. Her gün sistem bu 3 durumdan birini içersin. Aşağıdaki çizelge; sistem Si durumunda iken yarının (sonraki gün)olasılığını gösterir (i değişkeni 1, 2 veya 3 olabilir).

**Çizelge B.2** Markov matrisi

		Bugünkü durum		
		S1	S2	S3
Yarınki durum	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

Bu olasılıklar dizisi Markov matrisi olarak veya geçiş matrisi olarak adlandırılır. Her bir sütunun toplamının, her durumda oluşabilecek bütün olası çıktılarının 1 olduğuna dikkat edin. Sistem aynı zamanda, dairelerin durumları temsil ettiği yerlerde bir Markov diyagramı olarak da sunulabilir ve oklar beraberindeki olasılık ile birlikte geçişleri gösterir.



**Şekil B.9 - Markov sistem örneği diyagramı**

Oklar bir durumdan kendisine geçiş durumu genelde gösterilmez, ancak bu örneklerde bütünlüğü sağlamak için gösterilmiştir.

$P_i$ ,  $i = 1, 2, 3$  için, sistemi “i” halinde bulma olasılığını gösterebilir, aynı anda çözülmesi gereken eşitlikler şunlardır:

$$P_1 = 0,95 P_1 + 0,30 P_2 + 0,20 P_3 \quad (B.1)$$

$$P_2 = 0,04 P_1 + 0,65 P_2 + 0,60 P_3 \quad (B.2)$$

$$P_3 = 0,01 P_1 + 0,05 P_2 + 0,20 P_3 \quad (B.3)$$

Bu eşitlikler bağımsız değildir ve üç bilinmeyeni çözmezler. Aşağıdaki eşitlik kullanılarak yukarıdaki bir eşitlik iptal edilir.

$$1 = P_1 + P_2 + P_3 \quad (B.4)$$

Ayrık durumlar olan 1, 2, 3 için çözüm 0.85, 0.13 ve 0.02'dir. Sistem zamanın %85'inde tam olarak çalışmakta, zamanın %13'ünde aksamalı durumda çalışmakta ve zamanın %2'sinde hata vermektedir.

Aynı cihazdan iki tane paralel olarak açık ancak, sistemin işlevini yerine getirebilmesi için en az birinin çalışır durumda olması gerektiğini düşünün. Sistemin çalışması için faaliyete geçmesi gereken her iki öğenin paralel çalıştığını varsayalım.

Öğeler işletimsel veya hata verme durumunda olabilir ve sistemin elverişliliği bu öğelerin durumuna bağlıdır.

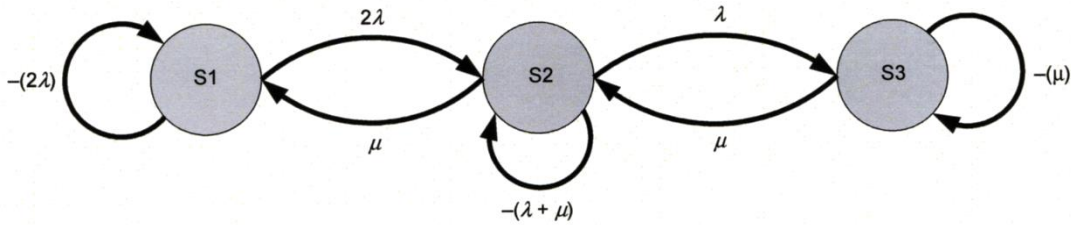
Durum'lar aşağıdaki gibi göz önüne alınabilir:

Durum 1: Her iki öğe de düzgün olarak çalışıyor.

Durum 2: Bir öğe hata verdi ve onarımı sürüyor, diğer öğe çalışıyor.

Durum 3: Her iki öğe de hata verdi ve onarımı sürüyor.

Eğer her öğe için sürekli hata oranı  $\lambda$  olarak ve onarım oranı  $\mu$  olarak farz edilirse, bu durumda durum geçiş diyagramı aşağıdaki gibidir:



Şekil B.10 - Durum geçişi örnek diyagramı

Her iki öğenin de hata vermesi sistemi Durum 2'ye götüreceğinden; Durum 1'den Durum 2'ye geçişin,  $2\lambda$  olduğunu varsayalım.

Geçiş olasılık matrisi aşağıdaki şekilde oluşur:

$P_i(t)$ 'yi  $t$  zamanında, durum  $i$  başlangıç halinde bulunma olasılığını gösterebilir, ve  $P_i(t + \delta t)$   $i$ ,  $t + \delta t$  zamanında son durumun olasılığını gösterebilir.

### Çizelge B.3 Sonuç Markov matrisi

		Bugünkü durum		
		$P_1(t)$	$P_2(t)$	$P_3(t)$
Son Durum	$P_1(t + \delta t)$	$-2\lambda$	$\mu$	$0$
	$P_2(t + \delta t)$	$2\lambda$	$-(\lambda + \mu)$	$\mu$
	$P_3(t + \delta t)$	$0$	$\lambda$	$-\mu$

Durum 1'den Durum 3'e veya Durum 3'den Durum 1'e geçiş mümkün olmadığında, sıfır değerleri ortaya çıkabilir. Aynı zamanda, oranlar tanımlandığında sütunların toplamı sıfır olur.

Eşzamanlı eşitlikler aşağıdaki gibidir:

$$dP_1/dt = -2\lambda P_1(t) + \mu P_2(t) \quad (B.5)$$

$$dP_2/dt = 2\lambda P_1(t) + -(\lambda + \mu) P_2(t) + \mu P_3(t) \quad (B.6)$$

$$dP_3/dt = \lambda P_2(t) + -\mu P_3(t) \quad (B.7)$$

Basitleştirmek için, gerekli olan uygunluk, kararlı durum uygunluğu olarak kabul edilir.

$\delta t$  değeri sonsuzluk eğiliminde ise,  $dP_i/dt$  değeri sıfır olma eğilimindedir ve denklemler çözülmesi daha kolay bir hale gelir.

Aynı zamanda, (B.4)'de gösterilen ilave eşitlik de kullanılmalıdır:

Bu durumda;  $A(t) = P1(t) + P2(t)$  eşitliği aşağıdaki gibi ifade edilebilir:

$$A = P1 + P2$$

Böylece,  $A = (\mu^2 + 2 \lambda \mu) / (\mu^2 + 2 \lambda \mu + \lambda^2)$  olur.

#### B.24.5 Çıktılar

Bir Markov analizinin çıktısı, çeşitli durumlarda olma olasılıklarıdır ve bu nedenle hata olasılığının ve/veya mevcudiyetinin tahmini önemli sistem bileşenlerinden biridir.

#### B.24.6 Güçlü yanlar ve kısıtlar

Markov analizinin güçlü yanları aşağıdakileri içerir:

- Onarım kapasitesine ve çoklu aksayan durumlarına sahip sistemler için olasılıkları hesaplayabilme kabiliyeti.

Markov analizinin kısıtları aşağıdakileri içerir

- Hata veya onarım durumu hal değişikliklerinde sabit olasılıkların varsayılması,
- Durumun öncelikli olma durumu haricinde; gelecek olayları geçmiş olaylardan bağımsız olduğu için, tüm olaylar istatistiksel olarak birbirinden bağımsızdır,
- Bütün durum değişikliği olasılıklarının bilinmesi gerekliliği,
- Matris işlemlerinin bilinmesi gerekliliği,
- Sonuçların teknik bilgisi olmayan personele aktarılması zordur.

#### B.24.7 Karşılaştırmalar

Markov analizi, sistem hallerini izleme ve takip imkanı sağlaması açısından Petri-Net analizine benzer, ancak farklı şekilde Petri-Net aynı anda birden fazla halde bulunabilir.

#### B.24.8 Kaynak dokümanlar

IEC 61078, *Uyumluluk için analiz teknikleri - Blok diyagram ve mantıksal metot güvenilirliği*

IEC 61165, Markov tekniklerinin uygulanması

ISO/IEC 15909 (tüm bölümler), *Yazılım ve sistem mühendisliği – Yüksek-seviye Petri ağları*

### B.25 Monte Carlo simülasyonu

#### B.25.1 Genel bakış

Pek çok sistem, üzerlerindeki belirsizlik etkisini analitik tekniklerle modelleyebilmek için çok karmaşıktır, ancak girdileri rastgele değişkenler olarak ele alıp, istenen sonuçlardan N tane muhtemel çıktı elde etmek için, girdileri örnekleyerek N defa hesaplama yapmak (simülasyonlar) şeklinde değerlendirilir.

Pek çok sistem, analitik teknikler kullanarak üzerlerindeki belirsizlik etkisinin modellenmesi için çok karmaşıktır, ancak girdileri rastgele değişkenler olarak ele alıp, istenen sonuçlardan N tane muhtemel çıktı elde etmek için, girdileri örnekleme ile N defa hesaplama yapmak (simülasyonlar) şeklinde değerlendirilir.

Bu yöntem, anlaşılması ve analitik yöntemlerle çözülmesi çok zor karmaşık durumları ifade edebilir. Sistemler hesap çizelgeleri ve diğer alışılmış araçlarla geliştirilebilir, Sistemler, hesap çizelgesi ve diğer alışılmış araçlar kullanılarak geliştirilebilir, ancak günümüzde, nispeten pahalı olmayan daha gelişmiş araçlar karmaşık gereksinimlerde yardımcı olmak için erişilebilir durumdadır. Teknik ilk geliştirildiğinde, Monte Carlo simülasyonunu gerçekleştirmek için gerekli olan hesaplama tekrar adedi, süreci prosesi yavaş ve vakit kaybettirici hale getirmiştir, ancak bilgisayar alanındaki ilerleme ve Latin-hypercube örnekleme gibi teorideki teorik gelişmeler, pek çok uygulama için işleme zamanını proses süresini neredeyse önemsiz hale getirmiştir.

#### B.25.2 Kullanım

Monte Carlo simülasyonu geniş bir aralıktaki durumlardaki sistemler üzerindeki belirsizlik etkisini değerlendirmek için bir araç sağlar. Genellikle, olası çıktı aralığını ve bir sisteme ait bulunan maliyet, devam

süresi, verimlilik, talep ve benzer ölçümler gibi bir sistemin sayısal ölçümlerinin bu aralıktaki değerlerin bağlı frekansını hesaplamak için kullanılır. Monte Carlo simülasyonu iki farklı amaç için kullanılabilir:

- Geleneksel analitik modeller üzerindeki belirsizliğin yayılması,
- Analitik teknikler çalışmadığı durumlarda olasılığa bağlı hesaplamalar.

### B.25.3 Girdiler

Monte Carlo simülasyonuna ait girdi; iyi bir sistem modeli ve girdi tipleri hakkında bilgi, temsil edilen belirsizlik kaynakları ve gereken çıktıdır. Belirsizlik içeren veri; belirsizlik seviyesine göre, daha fazla veya daha az yayılan dağılımlar şeklinde rastgele değişkenler olarak temsil edilir. Tekdüze, üçgen, normal ve log normal dağılımlar genellikle bu amaç için kullanılırlar.

### B.25.4 Proses

Proses aşağıdaki gibidir:

- Çalışılan sistemin davranışını mümkün olduğunca yakın bir şekilde ifade eden bir model veya algoritma tanımlanır.
- Model, rastgele rakamlar kullanılarak modelin çıktılarını üretmek amacıyla birçok kez çalıştırılır (sistem simülasyonu). Uygulamanın, belirsizlik etkilerinin modellemek olduğu yerlerde, model girdi parametreleri ve bir çıktı arasındaki ilişkiyi sağlayan bir eşitlik şeklindedir. Girdiler için seçilen değerler, bu parametrelerin belirsizlik doğasını temsil eden uygun olasılık dağılımlarından elde edilir.
- Her iki durumda da bilgisayar programı, modeli değişik girdilerle birden çok kez çalıştırır (genelde 10.000 adede kadar) ve çoklu çıktılar oluşturur. Bunlar; ortalama değerler, standart sapma, güven aralığı gibi bilgileri sağlamak amacıyla, geleneksel istatistikler kullanılarak işlenebilir.

Bir simülasyon örneği aşağıda verilmiştir.

Her iki ögenin paralel çalıştığı ve sistemin işlemesi için sadece bir ögenin gerektiğini varsayalım. İlk ögenin güvenilirliği 0,9 ve diğerinininki 0,8'dir.

Aşağıdaki sütunlara sahip bir hesap çizelgesi oluşturmak mümkündür.

### Çizelge B.4 - Monte Carlo simülasyonuna bir örnek

Durum Numarası	ÖGE 1		ÖGE 2		Sistem
	Rastgele Sayı	Fonksiyon?	Rastgele Sayı	Fonksiyon?	
1	0,577 243	EVET	0,059 355	EVET	1
2	0,746 909	EVET	0,311 324	EVET	1
3	0,541 728	EVET	0,919 765	HAYIR	1
4	0,423 274	EVET	0,643 514	EVET	1
5	0,917 776	HAYIR	0,539 349	EVET	1
6	0,994 043	HAYIR	0,972 506	HAYIR	0
7	0,082 574	EVET	0,950 241	HAYIR	1
8	0,661 418	EVET	0,919 868	HAYIR	1
9	0,213 376	EVET	0,367 555	EVET	1
10	0,565 657	EVET	0,119 215	EVET	1

Rastgele sayı üretici, sistemin işletimsel olup olmadığını belirlemek için her ögenin olasılığı ile karşılaştırmak üzere, 0 ile 1 arasında bir sayı üretir. Sadece 10 kez çalıştırma ile 0.9 sonucundan hassasiyet beklememek gerekir. Genel yaklaşım, simülasyonun gerekli hassasiyet seviyesine ulaşması için toplam sonuçları karşılaştırmak için bir hesap cetveli oluşturulmasıdır. Bu örnekte, 0.979 9 sonucuna 20.000 tekrar sonrasında ulaşılmıştır.

Yukarıdaki model farklı yollarla genişletilebilir. Örneğin:

- Modelin kendisini genişleterek (örneğin, birinci ögenin hata vermesi durumunda, ikinci ögenin acilen işletimsel hale getirilmesi),
- Olasılık tam olarak tanımlanamadığında, sabit olasılığı değişken olasılıkla değiştirerek (buna iyi bir örnek üçgen dağılımdır),
- Hata oranlarının rastgele sayı üreticiyle birleştirilerek arıza zamanlarını türetilmesi (üstel, Weibull veya diğer uygun bir dağılım) ve onarım sürelerinin belirlenmesi.

Uygulamalar; diğerlerinin yanında, finansal tahminler, yatırım performansı, proje maliyetleri, planlanan tahminler, iş proses kesintileri ve istihdam şartlarındaki belirsizliğin değerlendirilmesini içerir.

Analitik teknikler, ilgili sonuçları sağlamanın mümkün olmadığı durumlarda veya girdi verisinde belirsizlik olduğunda ve dolayısı ile çıktılarda belirsizlik olduğu durumlarda kullanılır.

### B.25.5 Çıktılar

Çıktı, tek bir değer olabilir. Bu çıktı, yukarıdaki örnekte belirtildiği gibi, olasılık veya sıklık dağılımı olarak ifade edilebilen sonuçları olabilir veya çıktı üzerinde en büyük etkisi olan model içinde bulunan ana fonksiyonların tanımlanması da olabilir.

Genel olarak Monte Carlo simülasyonu, ya meydana gelebilecek bütün çıktıların dağılımını veya dağılımdan gelen aşağıdaki anahtar ölçüleri değerlendirmek için kullanılır:

- Tanımlanan bir çıktının oluşabilme olasılığı,
- Problem sahibi aşılacak veya yenilemeyecek belirli bir güven seviyesine sahip olduğunda %10'dan daha az ihtimalde bir maliyet veya %80'i aşan belirli bir bekleme süresi gibi bir çıktı değeri.

Girdiler ve çıktılar arasındaki ilişkinin analizi; işteki etkenlerin bağıl önemini aydınlatılabilir ve çıktıdaki belirsizliği etkileme girişimleri için faydalı hedefleri tanımlayabilir.

### B.25.6 Güçlü yanlar ve kısıtlar

Monte Carlo analizinin güçlü yanları aşağıdaki gibidir:

Yöntem prensip olarak; ilgili sistemlerin gözlemlerinden elde edilen ampirik dağılımlar dahil olmak üzere bir girdi değişkeninde herhangi bir dağılımı içerebilir,

- Modellerin geliştirilmesi nispeten basittir ve ihtiyaç durumunda genişletilebilir,
- Şartlı bağımlılıklar gibi çözümü zor etkileri içeren, gerçek hayatta meydana gelen herhangi bir etki veya ilişkiyi temsil edilebilir,
- Hassasiyet analizi güçlü ve zayıf etkileri belirlemek için uygulanabilir,
- Girdiler ve çıktılar arasındaki ilişki şeffaf olduğunda, modeller kolayca anlaşılabilir,
- Monte Carlo simülasyon amaçları için çok verimli olduğu kanıtlayan Petri Ağları (gelecekteki IEC 62551) gibi verimli davranış modelleri mevcuttur,
- Sonucun doğruluğu ile ilgili bir ölçüt sağlar,
- Yazılım erişilebilir ve nispeten pahalı değildir.

Kısıtlar aşağıdaki konuları içerir:

- Çözümlerin doğruluğu, gerçekleştirilebilen simülasyonların sayısına bağlıdır (bu kısıtlama bilgisayar hızları arttıkça daha az önemli hale gelmektedir),
- Bu analiz, geçerli bir dağılım aracılığıyla parametrelerdeki belirsizliklerin temsil edilmesi üzerine dayanır,
- Büyük ve karmaşık modeller; modelleyici için zorlayıcı olabilir ve paydaşlar için bu karmaşık modelleri proses ile ilişkilendirmek zor olabilir,
- Teknik yeterli şekilde, yüksek-önem/düşük olasılıklı olaylar olarak tartamayabilir ve dolayısıyla bir kuruluşun risk iştahı analize yansıtılamayabilir.

### B.25.7 Kaynak dokümanlar

IEC 61649, *Weibull analysis*

IEC 62551, *Bağımsızlık analizi teknikleri - Petri net teknikleri (çalışma aşamasında)*

*Belirsizlik ölçümü - Bölüm 3: Ölçüm belirsizliği kılavuzu*

## B.26 Bayes İstatistiği ve Bayes Ağı

### B.26.1 Genel

Bayes istatistiği Reverend Thomas Bayes'e atfedilmiştir. Bu istatistiğin önermesi; hâlihazırda bilinen herhangi bir bilginin (önbilgi), genel bir olasılık oluşturabilmek için müteakip ölçümlerle (çıkarım) birleştirilebilir olmasıdır. Bayes teoreminin genel ifadesi aşağıdaki şekilde sunulabilir:

Burada,

$P(X)$ : X'in oluşma olasılığını,

$P(X|Y)$ : Y koşulu oluştuktan sonra, X'in oluşma olasılığını, ve

$E_i$ : i'nci olayı

ifade eder.

En basit gösterimi ile  $P(A|B) = \{P(A) P(B|A)\} / P(B)$  şekline indirgenir.

Bayes istatistiği, klasik istatistikten farklı olarak tüm dağılım parametrelerinin sabit olduğunu varsaymaz, ancak bu parametrelerin rastgele değişkenler olduğu kabul eder. Bir Bayes olasılığı, fiziksel deliller temelinde elde edilen klasik anlayışın zıddı olarak eğer bir kişinin inanış derecesi olarak görülürse daha iyi anlaşılabilir.

Bir Bayes dağılımı; fiziksel kanıta dayanan klasik yaklaşımın aksine, bir kişinin belli bir olaydaki inanç derecesi olarak kabul edilirse çok daha kolay anlaşılabilir. Bayes yaklaşımı, olasılığın sübjektif yorumuna dayanır ve bu yaklaşım karar vermeye yarayan fikirler ve Bayes ağlarının (veya İnanç ağları, İnanç şebekeleri veya Bayes ağları) geliştirilebilmesi için bir temel oluşturur.

Bayes ağları, değişkenler kümesini ve bu değişkenler kümesinin olasılık ilişkilerini temsil edecek grafiksel bir model kullanır. Ağ yapısı, rastgele bir değişkeni ve ana düğümle yavru düğümü (ana düğüm değişkeni, diğer (yavru) düğüm değişkenini doğrudan etkileyen değişken olduğu yerlerde) birbirine bağlayan okları temsil eden düğümlerin oluşumudur.

### B.26.2 Kullanım

Son yıllarda, Bayes teorisinin ve Bayes ağlarının kullanımı; kısmen anlaşılması ve kullanılması kolay, kısmen de yazılımın bilgi işlem araçlarının kullanılabilirliğinden dolayı yaygın hale gelmiştir. Bayes ağları çok kapsamlı bir kullanım aralığına sahiptir: tıbbi teşhis, görüntü modellemesi, genetik, ses tanıma, ekonomi, uzay araştırma ve günümüzde kullanılan güçlü internet arama motorları. Bu teori ve ağlar; yapısal ilişkiler ve verilerin kullanımı ile bilinmeyen değişkenlerin tespit edilmesi gerekli olduğu her alanda çok değerli olabilir.

Bayes ağları, bir sorunun etki alanı hakkında bilgi sahibi olabilmek ve müdahale sonuçlarını tahmin ederek nedensel ilişkileri öğrenmek için kullanılabilir.

### B.26.3 Girdiler

Girdiler, Monte Carlo modelindeki girdilerle benzerlik gösterir. Bir Bayes ağı için atılması gereken adımların örnekleri aşağıdakileri içerir:

- Sistem değişkenlerini tanımlamak,
- Değişkenler arasındaki neden-sonuç ilişkilerini tanımlamak,
- Şartlı veya öncelikli olasılıkları belirlemek,
- Ağa delil eklemek,
- İnanış güncellenmesini gerçekleştirmek,
- Sonuç inanışlarının çıkarımı.

### B.26.4 Proses

Bayes teorisi çeşitli şekillerde uygulanabilir. Bu örnek; bir kişinin hastalığa sahip olup olmadığını belirlenmesi için kullanılan tıbbi deneylerin kullanıldığı yerlerde, Bayes çizelgesinin oluşturulmasını dikkate alır. Deney yapılmadan önceki inanç popülasyonun %99'unun bu hastalığa sahip olmadığı ve %1'inin ise bu hastalığa sahip olduğu yönündedir (örneğin, ön bilgi). Deneyin doğruluğu kişinin hastalığa sahip olup olmadığını gösterir, deney sonucu %98 oranında pozitifdir. Aynı zamanda eğer kişi hastalığa sahip değilse, deney sonucunun %10 oranında pozitif olma olasılığı da vardır. Bayes çizelgesi aşağıdaki bilgileri sağlar:

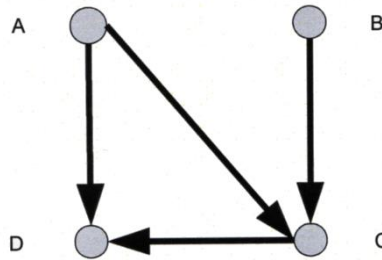


**Çizelge B.5 Bayes çizelgesi verisi**

	Önbilgi	Olasılık	Çarpım	Çıkarım
Hastalık var	0,01	0,98	0,009 8	0,0901
Hastalık yok	0,99	0,10	0,099 0	0,909 9
TOPLAM	1		0,108 8	1

Bayes kuralı kullanılarak; çarpım, ön bilgi ve olasılık birleştirilerek belirlenir. Çıkarım ise çarpım değerinin ürün toplamına bölünmesiyle bulunur. Çıktı; pozitif bir deney sonucunun, ön bilgi olan %1'den %9'a çıktığının belirtisi olduğunu gösterir. Daha önemlisi, tahlilin pozitif çıkmasına rağmen güçlü bir ihtimal daha vardır, bu da hastalığa sahip olmanın beklenilmeyen bir durum olmasıdır.  $(0,01 \times 0,98) / ((0,01 \times 0,98) + (0,99 \times 0,1))$  eşitliği incelendiğinde "hastalık yok - pozitif sonuç" değeri çıkarım sonuçları için önemli rol oynar.

Aşağıdaki Bayes ağını dikkate alırsak:

**Şekil B.11 - Örnek Bayes Ağı**

Aşağıdaki çizelgelerde tanımlanan Şartlı Ön bilgi Olasılıklar ile birlikte ve Y'nin pozitif, N'nin ise negatif gösterdiği bir formül kullanıldığında, Pozitif yukarıdaki gibi "Hastalık var" veya Yüksek olabilir ve N Düşük olabilir.

**Çizelge B.6 - A ve B düğümleri için ön bilgi olasılıkları**

P(A = Y)	P(A = N)	P(B = Y)	P(B = N)
0.9	0.1	0.6	0.4

**Çizelge B.7 - A ve B'nin tanımlı olduğu, C düğümü için şartlı olasılıklar**

A	B	P(C = Y)	P(C = N)
Y	Y	0.5	0.5
Y	N	0.9	0.1
N	Y	0.2	0.8
N	N	0.7	0.3

**Çizelge B.8 - A ve C'nin tanımlı olduğu, D için şartlı olasılıklar**

A	C	P(D = Y)	P(D = N)
Y	Y	0.6	0.4
Y	N	1.0	0.0
N	Y	0.2	0.8
N	N	0.6	0.4

Çıkarım olasılığı  $P(A|D=N, C=Y)$ 'yı belirlemek için, öncelikle  $P(A, B|D=N, C=Y)$  eşitliğini hesaplamak gerekir.

Bayes kuralını kullanarak,  $P(D|A, C)P(C|A, B)P(A)P(B)$  değeri aşağıda gösterildiği şekilde belirlenir ve son sütun önceki örneklerden elde edilen ve toplamı 1 olan normalleştirilmiş olasılıkları gösterir (sonuçlar yuvarlanmıştır).

**Çizelge B.9 – D ve C düğümlerinin tanımlı olduğu, A ve B düğümleri için çıkarım olasılıkları**

A	B	$P(D A,C)P(C A,B)P(A)P(B)$	$P(A,B D=N,C=Y)$
Y	Y	$0,4 \times 0,5 \times 0,9 \times 0,6 = 0,110$	0.4
Y	N	$0,4 \times 0,9 \times 0,9 \times 0,4 = 0,130$	0.48
N	Y	$0,8 \times 0,2 \times 0,1 \times 0,6 = 0,010$	0.04
N	N	$0,8 \times 0,7 \times 0,1 \times 0,4 = 0,022$	0.08

$P(A|D=N,C=Y)$ 'yi türetmek için B nin tüm değerleri toplanmalı:

**Çizelge B.10 – D ve C düğümleri tanımlı olduğu, A düğümünün çıkarım olasılıkları**

$P(A=Y D=N,C=Y)$	$P(A=N D=N,C=Y)$
0.88	0.12

Bu,  $P(A=N)$  eşitliği için ön bilgisi olasılığının 0,1'den, çıkarımına 0,12'ye arttığını gösterir. Öte yandan  $P(B=N|D=N,C=Y)$  eşitliği 0,4'den, daha önemli değişimle 0,56'ya artar.

### B.26.5 Çıktılar

Bayes yaklaşımı; çıktıları geniş bir yelpazede, (örneğin, nokta tahminlerinden ve güven aralıklarından elde edilecek veri analizi gibi) klasik istatistiklerle aynı kapsamda uygulanabilir. Bayes yaklaşımının son zamanlardaki popülerliği, çıkarım dağılımlardan elde edilen Bayes ağırları ile ilişkilidir. Grafikselleştirilmiş çıktı, kolay anlaşılabilir bir model sağlar ve veri korelasyon ve parametrelerin hassasiyetini dikkate almak için kolayca değiştirilebilir.

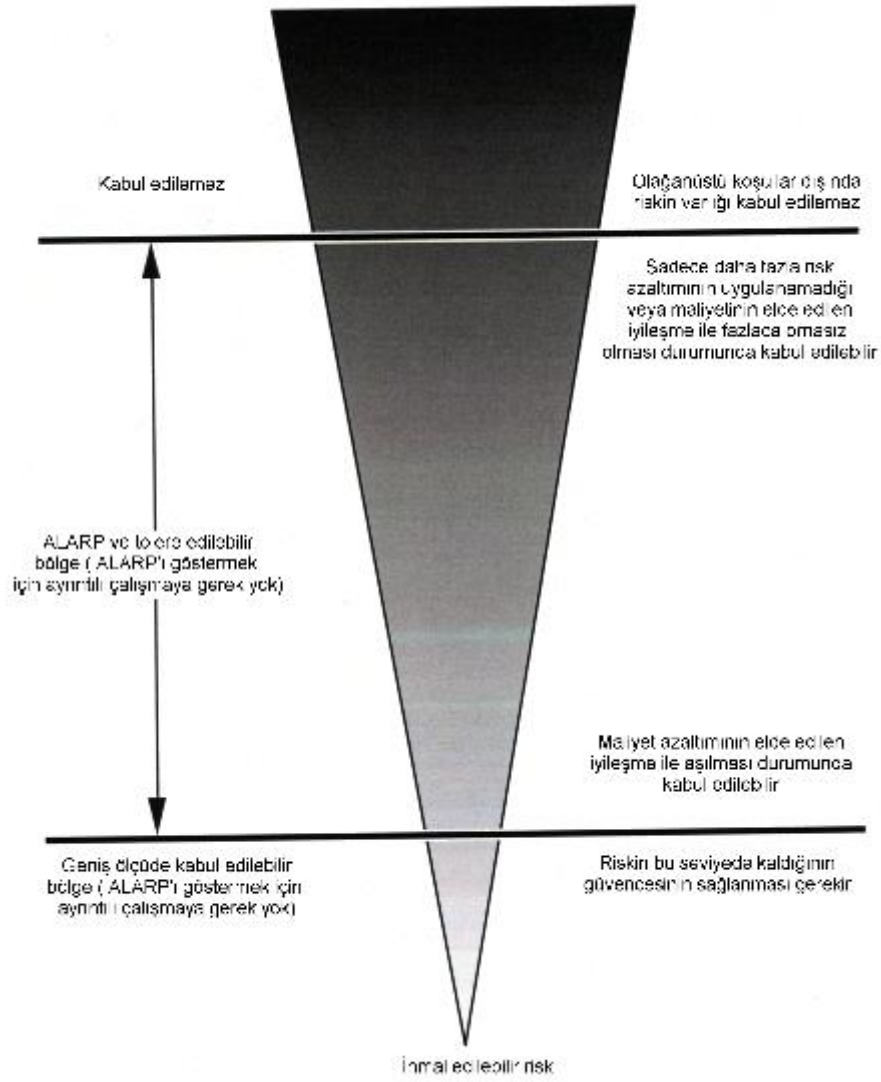
### B.26.6 Güçlü yanlar ve kısıtlar

Güçlü yanları aşağıdaki gibidir:

- Tek ihtiyaç duyulan ön bilgi hakkındaki bilgidir,
- Çıkarımsal ifadeler kolay anlaşılabilir,
- Bayes kuralı tek gereksinimdir,
- Bir problemde sübjektif inanışları kullanmak için bir mekanizma sağlar.

Kısıtlar aşağıdakileri içerir:

- Karmaşık sistemler için Bayes ağırlarındaki bütün etkileşimleri tanımlamak problemlidir,
- Bayes yaklaşımı; genellikle uzman görüşü ile sağlanan koşullu olasılıkların çoklu bilgisine ihtiyaç duymaktadır. Yazılım araçları yalnızca bu varsayımlara dayanan cevaplar sağlayabilir.



Şekil B.12 - ALARP konsepti

## B.27 FN Eğrileri

### B.27.1 Genel bakış

FN eğrileri, belirli bir popülasyona belirli bir seviyede zarara neden olan olayların olasılığının grafiksel gösterimi için kullanılan eğrilerdir. Bu eğriler çoğu kez, belli bir sayıda meydana gelen kayıp frekansına işaret eder.

FN eğrileri; popülasyonun N veya daha fazla sayıda üyesinin etkilendiği noktada, kümülatif frekansı (F) gösterir. Yüksek frekansta F durumu ile birlikte meydana gelebilen yüksek değerdeki N değerleri, sosyal ve politik olarak kabul edilemeyecekleri için dikkate değer öneme sahiptir.

### B.27.2 Kullanım

FN eğrileri, risk analizinin çıktılarını gösterme yöntemidir. Pek çok olay, yüksek olasılıkta düşük sonuçlu çıktıya ve düşük olasılıkta yüksek sonuçlu çıktıya sahip olabilir. FN eğrileri; bir sonuç-olasılık çiftini temsil eden tek bir nokta yerine, bu aralığı tarif eden bir risk seviye çizgisinin gösterimini sağlar.

FN eğrileri riskleri karşılaştırmada kullanılabilir; örneğin tahmin edilen riskleri, FN eğrisinde tanımlanan kriterlerle karşılaştırmak için veya tahmin edilen riskleri, geçmişte olan olaylardan veya karar kriterlerinden (F/N eğrisi olarak da ifade edilir.) elde edilen verilerle karşılaştırmak için kullanılabilir.

FN eğrileri ya sistem veya proses tasarımı için veya mevcut sistemlerin yönetilmesi için kullanılabilir.

### B.27.3 Girdiler

Girdiler aşağıdakilerden biri olabilir:

- Verilen bir zaman aralığındaki olasılık sonuç çifti setleri,
- Belirli sayıdaki olay için tahmin edilen olasılıkları veren sayısal bir risk analizinden elde edilen veri çıktısı,
- Hem geçmiş olaylardan elde edilen kayıtlardan hem de sayısal risk analizinden elde edilen veriler.

### B.27.4 Proses

Uygun veriler; dikey eksenini oluşturan N veya daha fazla sayıda kayıp olasılığı ve yatay eksenini oluşturan kayıp (belirli bir zarar seviyesi, örneğin, ölüm) sayısı ile birlikte grafiğe çizilir. Değerlerin geniş aralığından dolayı, her iki eksen de doğal olarak logaritmik ölçektedir.

FN eğrileri, istatistiksel olarak geçmiş kayıplardan elde edilen "gerçek" sayılar kullanılarak yapılabilir veya model tahmini simülasyonu aracılığı ile hesaplanabilir. Kullanılan veriler ve yapılan tahminler; bu iki tipteki FN eğrisinin farklı bilgi verebildiği ve bu eğrilerin farklı amaçlara yönelik olarak ayrı ayrı kullanılabilirdiği anlamına gelebilir. Genel olarak, teorik FN eğrileri sistem tasarımı için çok kullanışlıdır ve istatistiksel FN eğrileri kısmen var olan bir sistemin yönetimi için çok kullanışlıdır.

Her iki türetme yaklaşımı da zaman alıcı olabilir bu yüzden her ikisinin karışımını kullanmak sıradışı bir yol değildir. Ampirik veri daha sonrasında; belirli bir zaman aralığında bilinen kaza/olaylar sırasında meydana gelmiş kesin olarak bilinen kayıplara ilişkin sabit noktaları ve diğer noktaların ekstrapolasyon veya interpolasyon yoluyla elde edilmesini sağlayan sayısal risk analizine ilişkin sabit noktaları oluşturur.

Düşük frekanslı yüksek etkili kazaları göz önünde bulundurma ihtiyacı; düzgün bir analiz için gerekli veriyi bir araya getirmek için uzun zaman periyodu gerektirebilir. Bu sıra, başlangıç olaylarının zamanla değişmesi durumunda mevcut veriyi şüpheli hale getirebilir.

### B.27.5 Çıktılar

Çalışılan popülasyon ve belirlenen zarar seviyesi için uygun kriterler ile karşılaştırılabilir sonuçların değer aralığı boyunca olan riski ifade eden bir çizgi.

### B.27.6 Güçlü yanlar ve kısıtlar

FN eğrileri, risk ve güvenlik seviyeleri hakkında karar vermelerine yardımcı olması amacıyla yöneticiler ve sistem tasarımcıları tarafından kullanılabilen risk bilgisini sunmada faydalı bir yoldur. Hem frekans hem de sonuç bilgisini kabul erişilebilir bir formatta sunmak için kullanışlı bir yoldur.

FN eğrileri, yeterli verinin bulunduğu benzer durumlara ait risklerin karşılaştırılması için de uygundur. Veri kalite ve miktarının farklılık gösterdiği, koşulların değişken karakteristiklerinin bulunduğu durumlarda, farklı türden risklerin karşılaştırması için kullanılmamalıdır.

FN eğrilerinin bir kısıtı ise, etkilenen insan sayısı haricinde, olayların sonuçları ve etkilerin çeşitleri hakkında hiçbir bilgi vermemesidir ve zararın olduğu seviyelere hangi farklı yolların neden olduğunu belirleyebilecek bir imkân bulunmamaktadır. Genellikle, insanların maruz kaldığı zarar gibi belirli bir etki çeşidine göre eşleştirilirler. FN eğrileri, risk değerlendirme yöntemi olmayıp, risk değerlendirme sonuçlarının gösterimi için kullanılan bir yöntemdir.

Bu eğriler, risk değerlendirme sonuçlarının sunumu için iyi kurgulanmış bir yöntemdir ancak, yetkin bir analist tarafından yapılacak bir hazırlığı gerektirir ve genellikle uzman olmayan kişiler için yorumlaması ve değerlendirmesi zordur.

## **B.28 Risk endeksleri**

### **B.28.1 Genel**

Bir risk endeksi, sıralamalı ölçek kullanılarak gerçekleştirilen puanlama yaklaşımı aracılığıyla elde edilen bir tahmin değeri olan riskin yarı-kantitatif ölçümüdür. Risk endeksleri, risklerin karşılaştırılabilmesini sağlamak amacıyla, benzer kriterleri kullanarak bir risk serisini oranlamak için kullanılabilir. Puanlar riskin her bileşenine uygulanır, örneğin kirlenme nitelikleri (kaynaklar), olası maruziyet yollarına ait aralık ve alıcı üzerindeki etki.

Risk endeksleri aslında, riskleri derecelendirmek ve kıyaslamak amaçlı kalitatif bir yaklaşımdır. Sayılar kullanıldığında, işlenmesi kolaylaşır. Pek çok olayda, önde gelen model veya sistemin iyi bilinmediği veya temsil edilmediği durumlarda, daha açık kalitatif bir yaklaşımı kullanmak daha iyi olur.

### **B.28.2 Kullanım**

Endeksler, sistemin iyi anlaşılabilirdiği durumlarda, bir faaliyet ile bağlantılı farklı risklerin sınıflandırılması için kullanılabilir. Endeksler, risk seviyesi üzerinde etkiye sahip olan bir faktör aralığının tek bir sayısal skor ile belirtilen risk seviyeleri üzerine entegrasyonuna imkân sağlar.

Endeksler, genelde risk seviyelerine göre risklerin sınıflandırılması amaçlı kapsam belirleme aracı olarak pek çok farklı tipteki riskler için kullanılabilirler. Bunlar, hangi risklerin daha etraflı ve olası sayısal değerlendirme ihtiyacının olduğunu belirlemek için kullanılabilir.

### **B.28.3 Girdiler**

Girdiler, sistemin analizi sonucunda veya durumun geniş çerçevede tanımlanmasından. Bu, tüm risk kaynaklarının, muhtemel geçiş yollarının ve nelerin etkilenebileceğinin iyi anlaşılmasını gerektirir, Hata ağacı analizi, olay ağacı analizi ve genel karar verme analizleri gibi araçlar risk endekslerinin geliştirilmesini desteklemek için kullanılabilir.

Sıralama sayılarının seçimi bir yere kadar tercihe bağlı olduğundan, indisin geçerli kılınmasını sağlamak için yeterli verinin bulunması gerekir.

### **B.28.4 Proses**

İlk adım sistemi anlamak ve tarif etmektir. Sistem tanımlandığında, bileşik endeksi elde etmek için, her bir bileşenin birleştirebileceği bir yol seçilerek her bileşen için puanlar geliştirilir. Örneğin çevresel açıdan; kaynaklar, yollar ve alıcı/alıcılar puanlandırılır, ancak bazı olaylarda her kaynak için çoklu yollar ve alıcılar olabilir. Bireysel puanlar, sistemin fiziksel gerçekliğini dikkate alan bir şemaya göre birleştirilir. Sistemin her parçası (kaynaklar, yollar ve alıcılar) için puanların istikrarlı olması ve doğru ilişkilerin devam ettirilmesi önemlidir. Risk bileşenleri (örneğin, olasılık, maruziyet, sonuç) veya riski artıran risk faktörleri için puanlar verilebilir.

Puanlar bu yüksek seviye modele göre toplanabilir, çıkartılabilir, çarpılabilir ve/veya bölünebilirler. Kümülatif etkiler puanların toplanmasıyla dikkate alınabilir (örneğin, farklı yollar için puanların toplanması). Sıralamalı ölçeklere matematiksel bir formülün uygulanması kesinlikle geçerli değildir. Bu nedenle puanlama sistemi bir kez geliştirildiğinde, model bilinen bir sistem aracılığıyla geçerli kılınmalıdır. Bir endeks geliştirmek yinelenmeli bir yaklaşımdır ve analistin geçerli kılmadan emin olması amacıyla, puanların birleştirilmesi için birkaç farklı sistem denenmelidir.

Hangi parametrelerin en hassas olduğunu bulmak amacıyla; belirsizlik, hassasiyet analiziyle ve çeşitli puanlarla belirlenebilir.

**B.28.5 Çıktılar**

Çıktı, belirli bir kaynakla bağlantı kuran bir sayılar serisidir (bileşik endeksler) ve bu sayılar serisi, aynı sistem içindeki diğer kaynaklar için geliştirilen endekslerle ile karşılaştırılabilir veya aynı şekilde modellenir.

**B.28.6 Güçlü yanlar ve kısıtlar**

Güçlü yanlar:

- Endeksler farklı riskleri derecelendirmek için iyi bir araç sağlayabilir,
- Endeksler, risk seviyesinin belirlenmesi amacıyla tek bir nümerik puanla birleştirilmiş risk seviyesini etkileyen çoklu faktörlere izin verir.

Kısıtlar:

- Eğer proses (model) ve bu prosesin çıktıları düzgün bir şekilde geçerli kılınmazsa, sonuçlar anlamsız olabilir. Çıktının risk için sayısal bir değer olması gerçeğinden, risk yanlış yorumlanabilir ve yanlış kullanılabilir, örneğin risk analizini izleyen maliyet/fayda analizinde,
- Endekslerin kullanıldığı çoğu durumda, risk faktörlerine ait bireysel ölçeklerin lineer, logaritmik veya bazı diğer formlarda olup olmadığını tanımlamak için temel model yoktur ve faktörlerin nasıl birleştirilmesi gerektiğini tanımlayan hiçbir model yoktur. Bu tür durumlarda, oranlama doğal olarak güvenilir ve gerçek veriye karşı geçerli kılma özellikle önemli hale gelir.

**B.29 Sonuç/Olasılık matrisi****B.29.1 Genel**

Sonuç/olasılık matrisi; bir risk seviyesi veya risk oranı üretebilmek amacıyla, sonuç ve olasılıkların niteliksel ve yarı-sayısal oranlarını birleştirme aracıdır.

Matrisin formatı ve tanımlamalar kullanılan içeriğe bağlı olarak uygulanır ve koşullar için uygun bir tasarımın kullanılması önemlidir.

**B.29.2 Kullanım**

Bir sonuç/olasılık matrisi; riskleri, risk kaynaklarını veya risk seviyesi temelindeki risk davranışlarını sıralamak için kullanılır. Bu matris genellikle, pek çok riskin tanımlandığı yerlerde görüntüleme aracı olarak kullanılır. Örneğin; hangi risklerin daha fazla sayıda ve daha ayrıntılı bir analiz gerektirdiğini belirlemek, hangi risklerin öncelikli olarak ele alınmasının gerektiğini belirlemek veya daha yüksek yönetim seviyelerinde atfedilen ihtiyaçları belirlemek için kullanılır. Bu matris aynı zamanda, hangi risklerin o anda daha fazla dikkate alınmasına gerek olmadığını belirlemek için kullanılır. Bu tarz bir risk matrisi aynı zamanda, verilen bir riskin matris üzerinde konumlandırılan bölgeye göre, geniş çapta kabul edilebilir olup olmadığını belirlemek için yaygın bir şekilde kullanılabilir.

Sonuç/olasılık matrisi ayrıca, kuruluş içerisindeki niteliksel risk seviyeleri için ortak bir anlayış oluşturmaya yardım etmek amacıyla kullanılabilir. Risk seviyelerinin belirlenme yolu ve bunlara ilişkin karar verme kuralları, kuruluşun risk iştahı aracılığıyla sıraya konulabilir.

Sonuç/olasılık matrisinin bir şekli FMECA'nın (hata türleri, etkileri ve kritiklik analizi) kritiklik analizi için veya HAZOP'un (tehlike ve işletilebilirlik analizi) önceliklerini belirlemek için kullanılır. Bu matris aynı zamanda, ayrıntılı bir analiz için yetersiz verinin olduğu yerlerde veya durumun daha sayısal bir analiz yapabilmek için gerekli olan zaman ve çabaya izin vermediği durumlarda kullanılabilir.

**B.29.3 Girdiler**

Proses girdileri, sonuç ve olasılık için özelleştirilmiş ölçekler ve bu ikisini birleştiren matrislerdir.

Sonuç ölçeği (veya ölçekleri), göz önünde bulundurulması gereken değişik tiplerdeki sonuç aralıklarını (örneğin, finansal kayıp, güvenlik, çevre veya diğer parametreler) kapsmalıdır ve bu aralık en güvenilir sonuçtan ilgilenilen en düşük sonuca kadar uzanmalıdır. Kısmi bir örnek aşağıda Şekil B.6'da gösterilmiştir.

Bu ölçek herhangi bir puan sayısına sahip olabilir. 3, 4 veya 5 puanları en yaygın olanlarıdır.

Olasılık ölçeği de aynı zamanda herhangi bir puan sayısına sahip olabilir. Seçilmesi gereken olasılık tanımlamaları mümkün olduğunca belirsizliğe yer vermeyen bir şekilde olmalıdır. Farklı olasılıkları tanımlamak için nümerik kılavuzlar kullanılırsa birimler verilmelidir. Olasılık ölçeği; en düşük olasılığın, en yüksek tanımlı sonuç açısından kabul edilebilir olması gerektiğini unutmadan, eldeki çalışma ile ilgili aralığı ölçmeye ihtiyaç duyar. Aksi takdirde, en yüksek sonuca sahip tüm faaliyetler tolere edilemez şeklinde tanımlanır. Kısmi bir örnek aşağıda Şekil B.7'de gösterilmiştir.

Bir matris bir ekseninde sonuç, diğer ekseninde ise olasılık olacak şekilde çizilir. Aşağıda Şekil B.8'de, 6 noktada sonuç - 5 noktada olasılık ölçekli kısmi bir matris örneği gösterilmektedir.

Çizelgedeki hücrelere atanan risk seviyeleri, olasılık/sonuç ölçekleri için yapılan tanımlamalara bağlıdır. Matris, yukarıda gösterildiği gibi sonuçlara veya olasılıklara ekstra ağırlık verecek şekilde ayarlanabilir veya uygulamasına bağlı olarak simetrik olabilir. Risk seviyeleri ihtiyaç duyulan cevaplar vasıtasıyla, yönetimin dikkat seviyesi veya zaman ölçeği gibi karar vermede kullanılan kurallar ile ilişkilendirilebilir.

Rating	Financial Impact AU\$ EBITDA	Investment Return AU\$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	\$100m+ loss or gain	\$300+ loss or gain	<ul style="list-style-type: none"> <li>Multiple fatalities, or</li> <li>Significant irreversible effects to 10's of people</li> </ul>	<ul style="list-style-type: none"> <li>Irreversible long term environmental impact.</li> <li>Community outrage- potential large-scale case action.</li> </ul>	<ul style="list-style-type: none"> <li>International press reporting over several days.</li> <li>Total loss of shareholder support who act to divest.</li> <li>CEO departs and team is restructured.</li> </ul>	<ul style="list-style-type: none"> <li>Major litigation or prosecution with damages of \$50m+ plus significant costs.</li> <li>Customs sentence for company Executive.</li> <li>Prolonged closure of operations by authorities.</li> </ul>
5	\$10m - \$50m loss or gain	\$30m - \$250m loss or gain	<ul style="list-style-type: none"> <li>Single fatality and/or</li> <li>Severe irreversible disability to one or more persons</li> </ul>	<ul style="list-style-type: none"> <li>Prolonged environmental impact.</li> <li>High-profile community concerns raised - requiring significant remediation measures.</li> </ul>	<ul style="list-style-type: none"> <li>National press reporting over several days.</li> <li>Sustained impact on the reputation of shareholders.</li> <li>Loss of shareholder support for growth.</li> <li>Press...</li> </ul>	<ul style="list-style-type: none"> <li>Major litigation costing \$10m+.</li> <li>Investigation by regulatory body resulting in interruption of...</li> </ul>
4	\$1m - \$10m loss or gain	\$3m - \$20m loss or gain	<ul style="list-style-type: none"> <li>Extensive injuries or illnesses</li> </ul>	<ul style="list-style-type: none"> <li>Major spill</li> </ul>		
3	\$100k - \$100m loss or gain					
2	\$10k - 100k loss or gain					
1						

Şekil B.13 - Etki kriteri çizelgesi kısmi örneği

Rating	Criteria
Likely	<ul style="list-style-type: none"> <li>balance of probability will occur, or</li> <li>could occur within "weeks to months"</li> </ul>
Possible	<ul style="list-style-type: none"> <li>may occur shortly but a distinct possibility</li> <li>could occur within "months"</li> </ul>
Unlikely	<ul style="list-style-type: none"> <li>may occur but not for a foreseeable period</li> <li>could occur in "years"</li> </ul>
Rare	<ul style="list-style-type: none"> <li>occurrence requires exceptional circumstances</li> <li>only occur once in a long period</li> </ul>
Remote	<ul style="list-style-type: none"> <li>theoretical possibility</li> <li>fringe possibility</li> </ul>

Şekil B.14 Risk olasılık ölçeği kısmi örneği

Olabilirlik derecelendirmesi	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		Sonuç derecelendirmesi					

**Şekil B.15 - Risk derecelendirme matrisi kısmi örneği**

Derecelendirme ölçekleri ve matris, sayısal ölçekler için de kurgulanabilir. Örneğin, güvenilirlik alanında olasılık ölçeği arıza oranlarını gösterirken, etki ölçeği arızanın dolar cinsinden maliyetini gösterebilir.

Bu aracın kullanımı, uygun uzmanlık seviyesi ile insan kaynağına (ideal olarak bir ekip) ihtiyacın yanı sıra etki ve olasılık hakkında karar verebilmeye yardımcı olacak verileri gerektirir.

#### B.29.4 Proses

Kullanıcı riskleri sıralamak için, duruma en uygun olan sonuç tanımla ifadesini bulur, sonra oluşacak sonuçlar ile birlikte olasılığı tanımlar. Daha sonra, risk seviyesi matristen okunur.

Pek çok risk olayı, farklı ilintili olasılıklı çıktı aralığına sahip olabilir. Genelde minör problemlere, felaketlerden daha sık rastlanılır. Bu nedenle; en yaygın veya en ciddi çıktıların sıralanıp sıralanmadığı ile ilgili seçenek vardır. Pek çok olayda; en büyük tehlide neden olan en ciddi inanırlıktaki çıktıları odaklanmak uygundur. Bazı durumlarda, hem ortak problemleri hem de münferit riskler gibi alışılmadık afetleri sıralamak uygun olabilir. Seçilen sonuç ile ilgili olasılığın kullanılması önemlidir, ancak bu olasılık bütün olayın olma olasılığı değildir.

Matris tarafından tanımlanan risk seviyesi, riskin iyileştirilmesi veya iyileştirilmemesi gibi bir karar ile bağlantılandırılabilir.

#### B.29.5 Çıktı

Çıktı, her riskin sıralanması veya belirlenen önemli risk seviyelerine ait sıralama listesidir.

#### B.29.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar:

- Kullanımı nispeten kolaydır;
- Farklı önem seviyelerindeki riskler için hızlı bir sıralama sağlar.

Kısıtlar:

- Şartlar için uygun olabilmesi amacıyla bir matris tasarlanabilir, ancak kuruluşla ilgili bir dizi şartlar uygulayan ortak bir sisteme sahip olmak zordur,
- Ölçekleri açık bir şekilde tanımlamak zordur,
- Kullanımı sübjektiftir ve değerlendiriciler arasında önemli farklar olma eğilimi vardır,
- Riskler kümelenemez (örneğin, belli sayıdaki düşük riskleri tanımlanamaz veya belli bir sayıda tanımlanan düşük bir risk orta derecede bir risktir.),
- Farklı kategorilerdeki sonuçlara ait risk seviyelerini birleştirmek veya karşılaştırmak zordur.

Sonuçlar analizinin ayrıntı seviyesine bağlıdır, örneğin düşük olasılığa sahip daha ayrıntılı analizler, daha fazla sayıda senaryo gibi. Bu durum gerçek risk seviyesinin eksik değerlendirilmesine neden olur. Risklerin tanımlanmasında senaryoların gruplandırma şekli tutarlı olmalı ve çalışmanın başlangıcında tanımlanmalıdır.



## B.30 Maliyet/Fayda analizi (CBA)

### B.30.1 Genel

Maliyet/Fayda analizi, en iyi ya da en kârlı seçeneği tercih etmek için, beklenen toplam maliyet, toplam beklenen fayda ile tartılarak risk değerlendirme amacıyla kullanılabilir. Bu analiz, pek çok risk değerlendirme sisteminin dolaylı parçasıdır. Kalitatif veya kantitatif olabilir ya da kalitatif ve kantitatif parçaların birleşiminden oluşabilir. Sayısal CBA, tüm maliyeti ve kapsamda belirlenen paydaşlar için faydayı oluşturan parasal değerlerin toplamını alarak maliyetlerin ve faydanın gerçekleşeceği farklı zaman dilimlerine göre ayarlama yapar. Üretilen net bugünkü değer (NPV) bu risk hakkındaki karar için girdiyi oluşturur. Pozitif NPV ile ilişkilendirilmiş faaliyet, normal bu faaliyetin gerçekleştirilmesi gerektiği anlamına gelir. Bununla birlikte, bazı negatif risklerde, özellikle insan hayatı veya çevreye verilecek zarar konu olduğunda, ALARP prensibi uygulanabilir. Bu, riski üç bölgeye ayırır: olağanüstü durumlar hariç negatif risklerin tolere edilmediği ve kabul edilmemesi gereken bir üst seviye; risklerin sadece izleme ile takip edildiği ve düşük seviyede kaldıklarının güvence altına alındığı bir alt seviye; ve risklerin makul olduğunca aza indirgeneceği (ALARP) merkez bandı. Bu bölgenin düşük seviye sonuna doğru, katı bir maliyet/fayda analizi kullanılır ancak risklerin tolere edilmediği bölgeye yaklaştıkça, iyileştirme maliyetlerinin çok fazla şekilde oranları bozulmadıkça ALARP prensibinin çalışarak iyileştirmenin gerçekleşmesi beklenir.

### B.30.2 Kullanım

Maliyet/Fayda analizi, risk içeren seçenekler arasında karar vermek için kullanılabilir.

Örneğin:

- Bir riskin iyileştirmesi hakkında karar vermek için girdi olarak,
- Risk iyileştirme şekillerini farklılaştırma ve hangisinin daha iyi olduğu hakkında karar verme,
- Farklı hareket yolları hakkında karar verme.

### B.30.3 Girdiler

Girdiler içerisinde, maliyet ve ilgili paydaşlara fayda bilgisi ile bu maliyet ve fayda içerisindeki belirsizlik hakkında bilgi bulunur. Maddi ve maddi olmayan maliyet ve faydalar da düşünülmelidir. Maliyetler; harcanacak kaynakları ve negatif çıktıları, faydalar ise pozitif çıktıları, engellenen negatif çıktıları ve tasarruf edilen kaynakları içerir.

### B.30.4 Proses

Maliyetlere katlanan veya faydalardan yararlanan paydaşlar belirlenir. Tam maliyet/fayda analizinde tüm paydaşlar dâhil edilir.

Seçeneklerin ilgili paydaşlara getirdiği doğrudan ve dolaylı fayda ve maliyetler belirlenir. Doğrudan faydalar, gerçekleştirilen faaliyet sonucunda ortaya çıkan, dolaylı fayda ise rastlantısal ancak kâra önemli ölçüde katkı verenlerdir. Dolaylı fayda örneğine itibar gelişimi, çalışan memnuniyeti ve vicdani rahatlık sayılabilir (Bunlar karar verme aşamasında sıklıkla ağırlık kazanırlar).

Doğrudan maliyetler, gerçekleşen faaliyetlerle ilintili olanlardır. Dolaylı maliyetler, bir alt yapı hizmetinin kesintisi, bu işe ayrılan yönetim zamanı ya da sermayenin potansiyel yatırım alanlarından uzaklaşması gibi ilave, yardımcı ve gizli maliyetlerdir. Bir riski iyileştirme hakkında karar vermek için kullanılan maliyet fayda analizinde, riski iyileştirmek ya da kabul etmek için gerekli maliyet ve fayda bilgisi de dâhil edilmelidir.

Sayısal maliyet/fayda analizinde, tüm maddi ve maddi olmayan maliyet ve faydalar belirlendiğinde, tüm maliyet ve faydalara parasal bir büyüklük atanır (maddi olmayan maliyet ve faydalar da dâhil olmak üzere). Bunu yapabilmek için, içerisinde "ödemeye isteklilik" yaklaşımı ve "yerine geçmenin" de bulunduğu çeşitli standart yöntemler bulunmaktadır. Eğer gerçekleşirse, ödenecek maliyetler genellikle kısa vadede, elde edilecek faydalar ise daha uzun vadede gerçekleşir, bu nedenle geçerli bir karşılaştırma yapabilmek için fayda değerlerini "bugünkü değere" getirecek iskonto yapılmak gerekir. Tüm maliyet ve faydalar bugünkü değerle ifade edilir. Paydaşlar için tüm maliyet ve faydaların toplamı net bugünkü değeri (NPV) verir. Pozitif NPV, hareketin faydalı olacağı anlamına gelir. Fayda maliyet oranları da ayrıca kullanılabilir (bk. Ek B 30.5)

Eğer fayda veya maliyetlerin seviyesinin her ikisinde ya da birinde belirsizlik varsa, biri ya da her ikisinin olasılıklarına göre karşılaştırılır.

Kantitatif maliyet/fayda analizinde maddi olmayan maliyet ve faydalar için parasal değer atanmaya çalışılmaz, maliyet ve faydayı özetleyen tek bir parasal ifade yerine, ilişkiler, farklı fayda ve maliyetler arası getiri dengesi kalitatif olarak ifade edilir.

Bununla ilgili bir teknik ise maliyet-etkinlik analizidir. Bu yöntem, belirli bir fayda ya da çıktının istendiği ve bunu elde etmenin çeşitli yolları olduğu var sayılır. Analiz, sadece maliyetlere bakarak hangi faydanın en ucuz maliyetle elde edilebileceğine bakar.

### B.30.5 Çıktı

Maliyet/fayda analizinin çıktısı, farklı seçenekler veya faaliyetlerin görece maliyet ve faydaları hakkında bilgidir. Bu, sayısal olarak Net Bugünkü Değer olarak (NPV), iç getiri oranı (IRR) veya faydaların bugünkü değerinin, maliyetlerin bugünkü değerine oranı şeklinde ifade edilir. Kalitatif olarak, çıktı genellikle karşılığında neyin verildiğine dikkat çeken, maliyet ve faydaların farklı çeşitlerini karşılaştıran tablo şeklindedir.

### B.30.6 Güçlü yanlar ve kısıtlar

Güçlü yanlar:

- Maliyet ve faydaların tek bir ölçüt ile (para) karşılaştırılmasını sağlar,
- Karar vermede şeffaflık sağlar,
- Kararın tüm boyutları ile ilgili ayrıntılı bilgi toplanmasını gerekli kılar. Bu sayede bilgisizliği ortaya çıkardığı kadar bilginin iletişimini sağladığı için değerli kabul edilir.

Kısıtlar:

- Sayısal CBA, ekonomik olmayan faydalara ekonomik değer atama yöntemine bağlı olarak farklı çok sayılar ortaya çıkarılabilir,
- Bazı uygulamalarda, gelecekteki maliyet ve faydaların bugünkü değeri için gerekli olan iskonto değerini tanımlamak güç olabilir,
- Özellikle piyasada alım satımı bulunmayan kamu yararı ile ilgili alanlarda, büyük kitlelere sağlayacağı faydanın tahmini güçtür,
- İskonto uygulaması, uzun vadede kazanılacak faydaların, seçilen iskonto oranına göre verilecek kararlarda çok az bir etkisi olabileceği anlamına gelir. Gelecek nesilleri etkileyebilecek riskler üzerinde düşünülürken, iskonto oranı sıfır ya da sıfıra yakın bir değer kabul edilmediği takdirde bu yöntemi kullanmak uygun olmayacaktır.

## B.31 Çok kriterli karar analizi (MDCA)

### B.31.1 Genel

Burada amaç, bir kriter yelpazesi kullanarak, bir grup seçeneğin uygulamaya değer olup olmadığını objektif ve şeffaf olarak değerlendirmektir. Genellikle, asıl amaç eldeki seçenekler arasında bir tercihler sıralaması oluşturabilmektir. Analiz, her bir seçenek için genel bir puanlama üretebilmek amacıyla, sıralanmış ve toplulaştırılmış seçenekler ve kriterlerle bir matris yapısı oluşturulmasına dayanır.

### B.31.2 Kullanım

MCDA aşağıdakiler için kullanılabilir:

- Birden fazla seçeneğin karşılaştırılması ile analizin ilk taramasında, hangi seçeneklerin muhtemelen tercih edilebileceğini hangilerinin ise uygun olmadığını belirlenmesi.
- Birden fazla ve bazen çakışan kriterlerin bulunduğu yerlerde seçeneklerin karşılaştırılması.
- Farklı paydaşların birbiri ile çakışan hedefleri veya değerleri olduğu durumlarda bir karar hakkında uzlaşmaya varılması.

### B.31.3 Girdiler

Analizler için bir dizi seçenek sağlar. Seçenekleri birbirinden ayırt edebilmek için, tüm seçenekleri eşit olarak değerlendirebilecek hedeflerin temelinde oluşturulmuş kriterler.

### B.31.4 proses

Genellikle, bir grup bilgili paydaş aşağıdaki prosesi yürütür:

- a) Hedef/hedeflerin tanımlanması,
- b) Her hedef için niteliklerin (kriter veya performans ölçütleri) belirlenmesi,
- c) Bu niteliklerin bir hiyerarşi halinde yapılandırılması,
- d) Kriterlere karşı değerlendirmede kullanmak için seçeneklerin geliştirilmesi,
- e) Kriterlerin önem derecesinin belirlenmesi ve ilgili ağırlıkların bunlara atanması,
- f) Kriterler için alternatiflerin değerlendirilmesi. Bu, bir skorlar matrisi olarak sunulabilir,
- g) Birden fazla tek nitelikli skorun, çok nitelikli tek skora birleştirilmesi,
- h) Sonuçların değerlendirilmesi.

Her bir kritere ait ağırlığın elde edilmesi ve her seçenek için kriter puanlarının birleştirilerek çok nitelikli tek puanlama elde etmek için farklı yöntemler bulunmaktadır. Örneğin, puanlar ağırlıklandırılmış toplamlar veya ağırlıklandırılmış çarpımlar ya da ikili karşılaştırmalarla ağırlık ve puan tanımlanmasını sağlayan analitik hiyerarşi prosesi ile gerçekleştirilebilir. Tüm bu yöntemler, bir kriter için yapılan tercihin başka bir kriterin değerine bağlı olmadığını varsayar. Bu varsayımın geçerli olmadığı durumlarda başka modeller kullanılır.

Puanlamanın sübjektif olması nedeniyle, atanan ağırlık ve skorların seçenekler arası genel tercihleri nasıl etkilediğini incelemek için hassasiyet analizi faydalı olur.

### **B.31.5 Çıktılar**

En çok tercih edilenden en az tercih edilene göre sıralanmış seçeneklerin sunumu. Eğer proses, bir ekseni ağırlıklandırılmış kriter ve diğer ekseni her seçenek için atanmış skordan oluşmuş bir matris üretiyorsa, yüksek ağırlıklı kriteri geçemeyen seçenekler de elenebilir.

### **B.31.6 Güçlü yanlar ve kısıtlar**

Güçlü yanlar:

- Verimli bir karar verme prosesi ile varsayım ve sonuçları sunmak için basit bir yapı sunar,
- Maliyet/fayda analizi ile çözülemeyen karmaşık karar problemlerini yönetilebilir hale getirir,
- Tavizlerin verilmesi gerektiği durumlarda, problemleri rasyonel olarak ele almaya yardımcı olur,
- Paydaşların farklı hedefleri ve kriterleri olduğu durumlarda uzlaşma sağlamaya yardımcı olur,

Kısıtlar:

- Zayıf karar kriterleri ve ön yargılar nedeni ile etkilenebilirler,
- Pek çok MCDA probleminin tek bir ya da bağlayıcı bir çözümü yoktur,
- Kriter ağırlıklarını belirtilen tercihlerden toplayan algoritmalar veya farklı görüşlerin birleştirilmesi, kararın gerçek temelini anlaşılmaz hale getirebilir.

## Kaynaklar

- IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*
- IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*
- IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*
- ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*
- ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*
- IEC 60300-3-11, *Dependability management–Part 3-11: Application guide–Reliability centred maintenance*
- IEC 61649, *Weibull analysis*
- IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*
- IEC 61165, *Application of Markov techniques*
- ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*
- IEC 62551, *Analysis techniques for dependability – Petri net techniques<sup>2)</sup>*
- IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

---

<sup>2)</sup> Tasarım aşamasındadır.