Fonksiyonel emniyet
S-Safety **I**-Integrity **L**-Level

Safety@Festo

Güvenlik önlemlerinin EN ISO 13849-1/IEC 61508/IEC 61511/IEC 62061 standartlarına göre tespiti ve değerlendirmesi.

Risk değerlendirmesi

Risk analizi → Risk tespiti → Risk azaltımı
- → Tasarımsal önlemler
- → Teknik önlemler
- → Kullanıcı bilgileri

10 güvenlik işlevi

- Basınçlandırma
- Sistem tutma basıncı
- Basınç ve kuvvet düşürme
- Dışarı atma
- Kurcalamaya karşı korumalı, yetkisiz devreye alma önleme
- İki elle kumanda
- Hız düşürme
- Kuvvetlerden bağımsız
- Bir hareketi tersine çevirme
- Bir hareketi durdurma, tutma ve bloke etme

Tetikleyen olay	Girdi	Mantık	Çıktı	Tahrik
Güvenlik önlemini ne tetikler?	Tetikleme durumunu algılayan cihaz	Sinyali güvenli bir şekilde işleyen cihaz	Tehlikeli hareketi kontrol eden cihaz	
Örneğin: • Tehlikeli bir alana yaklaşma • Güvenlik kapısını açma • Proses sınır değeri aşıyor	• Işık perdesi • Güvenlik kapısı • Basınca duyarlı altlık • Acil durdurma • Arıza • Lazer tarayıcı • Kamera • Sıcaklık sensörü • Basınç sensörü • Akış hızı sensörü	• Donanım • Güvenlik rölesi • Güvenlik PLC'si • Pnömatik kumanda sistemi	• Pnömatik • Elektriksel • Hidrolik enerji	

FESTO

www.festo.com.tr

EN ISO 13849-1 Elektrikli, pnömatik, hidrolik ya da mekanik, kullanılan enerji türünden ve teknolojiden bağımsız olarak kontrol sistemlerinin ve her türden makinenin güvenlikle ilgili parçalarına uygulanır.

IEC 61508 Elektrikli/elektronik/programlanabilir elektronik güvenlikle ilgili sistemlerin işlevsel güvenliği.

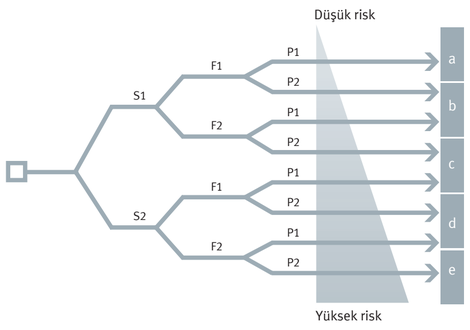
IEC 61511 İşlevsel güvenlik – proses endüstrisi için güvenlik enstrümanlı sistemler.

IEC 62061 Mekanik sistemlerin güvenliği – güvenlikle ilgili elektrikli, elektronik ve programlanabilir elektronik kontrol sistemlerinin işlevsel güvenliği.

Güvenlik önlemlerinin yeterli olup olmadığının değerlendirilmesine yönelik 6 adım

1 Risk değerlendirmesi Gerekli **Performans Seviyesi'nin (PLr)** belirlenmesi

Uygulamaya yönelik değerlendirme



S Yaralanma derecesi
- S1 Hafif (normal şartlarda iyileşen yaralanma)
- S2 Ağır (normal şartlarda iyileşmeyen yaralanma ya da ölüm)

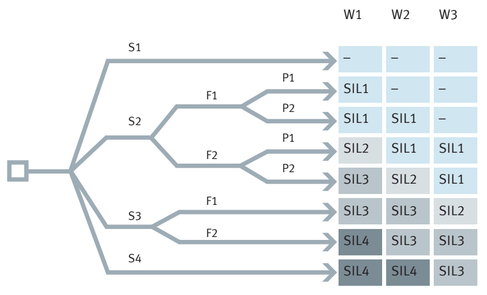
F Riske maruz kalma sıklığı ve/veya süresi
- F1 Nadiren – pek sık değil ve/veya maruz kalma süresi kısa
- F2 Sıklıkla – sürekli ve/veya maruz kalma süresi uzun

P Tehlikeden kaçma imkanı
- P1 Belli şartlar altında mümkün
- P2 Nadiren mümkün

a – e Performans seviyesi (PL_r)

Kaynak: DIN EN ISO 13849-1 EK 1.2.3

Gerekli **Güvenlik Bütünlük Seviyesi'nin (SILr)** belirlenmesi



- **SIL (Güvenlik Bütünlük Seviyesi)**
  4 adet somut adım (SIL1'den SIL4'e kadar). Güvenlikle ilgili sistemin SIL değeri ne kadar yüksek olursa, sistemin gerekli güvenlik işlevlerini yerine getirebilme imkanı o kadar düşüktür.

S Sonuç
- S1 Tek kişide önemsiz yaralanma
- S2 Çok sayıda kişide ciddi yaralanma ile bir kişinin ölümü
- S3 Çok sayıda ölüm
- S4 Çok sayıda ölüm içeren felaket etkisi

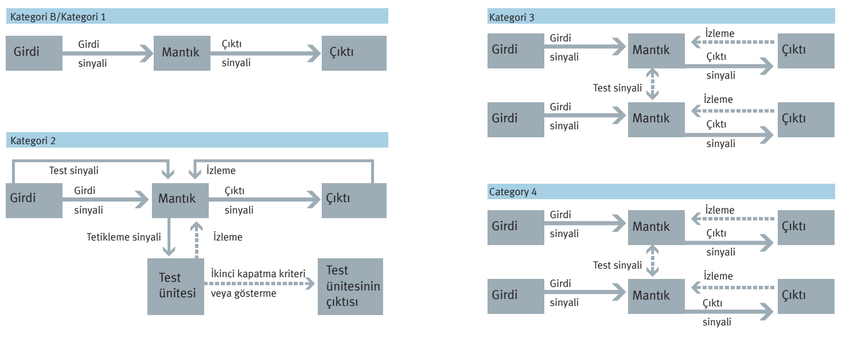
F Sıklık
- F1 Nadiren – Oldukça sık
- F2 Sık – Sürekli

P Kaçınma olasılığı
- P1 Belli koşullar altında mümkün
- P2 Nadiren mümkün

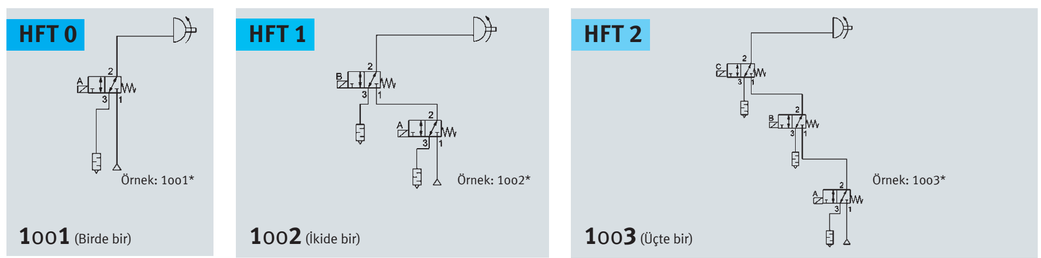
W Meydana gelme olasılığı
- W1 Oldukça yüksek
- W2 Düşük
- W3 Çok düşük

2 Belirlenmiş mimariler **Kategorilerin** özellikleri

Güvenlik önlemlerinin değerlendirimesi



HFT Donanım Arıza Toleransı'nın belirlenmesi



Tek bir arızada güvenlik kaybı gerçekleşir

Güvenlik kaybının gerçekleşmesi için en 2 arızanın aynı anda meydana gelmesi gerekir.

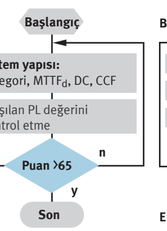
Güvenlik kaybının gerçekleşmesi için en 3 arızanın aynı anda meydana gelmesi gerekir.

- **HFT (Donanım Arıza Toleransı)**
  Gerekli işlevin arıza ya da sapma durumunda bile gerçekleştirilebilmesi durumu

*Güvenlik konumu kapalı (tükendi)

3 CCF Ortak Nedenli Arıza/DC Hata Tanılama Kapsamının Belirlenmesi

CCF'ye karşı alınacak önlemler	Puan
Ayırma	15
Çeşitlilik	20
Tasarım/uygulama	20
Değerlendirme/analiz	5
Uzmanlık/eğitim	5
Çevresel	35



Bileşen

Hangi arızalar meydana gelebilir?
Arızalar tehlikeli mi?
Tehlikeli arızalar tespit edilebiliyor mu?

$$DC_1 = \frac{\sum(\text{Tespit edilen tehlikeli arıza sayısı})}{\sum(\text{Toplama tehlikeli arıza sayısı})}$$

Entire system

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dn}}}$$

SFF Güvenli Arıza Fraksiyonu

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_D + \lambda_S}$$

$DC \le SFF \le 1$

$\lambda_S = 0 \rightarrow SFF = DC$

$\lambda_D = 0 \rightarrow SFF = 1$

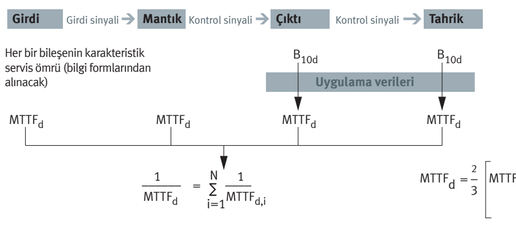
FME(D)A

Arıza tipi	Tespit edildi	Tespit edilmedi
güvenli λ_S	güvenli, tespit edildi λ_{SD}	güvenli, tespit edilmedi λ_{SU}
tehlikeli λ_D	tehlikeli, tespit edildi λ_{DD}	tehlikeli, tespit edilmedi λ_{DU}

$$SFF = \frac{\sum\lambda_{SD} + \sum\lambda_{SU} + \sum\lambda_{DD}}{\sum\lambda_{Total}} \qquad DC = \frac{\sum\lambda_{DD}}{\sum\lambda_D}$$

- **λ (arıza oranları)**
  λ_S: Güvenli arızalar için arıza oranı
  λ_D: Tehlikeli arızalar için arıza oranı
  λ_{SD}: Güvenli, tespit edilen arızalar içina arıza oranı
  λ_{SU}: Güvenli, tespit edilmeyen arızalar için arıza oranı
  λ_{DD}: Tehlikeli, tespit edilen arızalar için arıza oranı
  λ_{DU}: Tehlikeli, tespit edilmeyen arızalar için arıza oranı
- **FME(D)A (Arıza modları, etkileri ve arıza tanılama analizi)**
  Arıza tiplerinin ve arıza oranlarının nicel olarak tespit edilmesi için analiz yöntemleri
- **SFF (Güvenli Arıza Oranı)**
  Toplam arıza sayısına göre tüm güvenli ve tespit edilen arızaların oranı

4 $MTTF_d$ Arızaya Kadar Ortalama Süre'nin tanımı



$$\frac{1}{MTTF_d} = \sum_{i=1}^{N}\frac{1}{MTTF_{d,i}}$$

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

Bir kanal içerisindeki mekanik elemanın $MTTF_d$ değerini tespit etmek için kullanılan formül

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{cycle}}$$

Mekanik eleman için yıllık çalıştırma sayısının n_{op} ortalama değeri

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right]$$

İki farklı kanal için toplam $MTTF_d$ değerinin hesaplanması

Değerlendirme	$MTTF_d$
Düşük	3 yıl ≤ $MTTF_d$ < 10 yıl
Orta	10 yıl ≤ $MTTF_d$ < 30 yıl
Yüksek	30 yıl ≤ $MTTF_d$ < 100 yıl

Kaynak: DIN EN ISO 13849-1, Bölüm 4.5.2

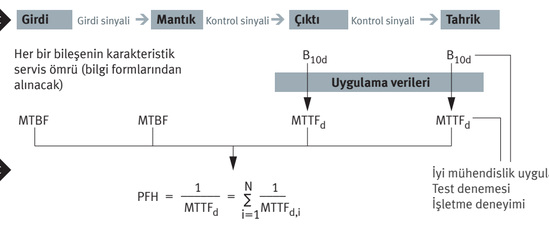
- $MTTF_d$ Arızaya Kadar Ortalama Süre)
  Tehlikeli bir arızaya kadar geçen ortalama süre
- MTTR (Arızanın Giderilmesine Kadar Ortalama Süre)
  Ortalama onarım süresi

PFH/PFD Arıza olasılığının belirlenmesi

$MTBF = MTTF + MTTR$
for $MTTF \gg MTTR$
$\rightarrow MTBF = MTTF$

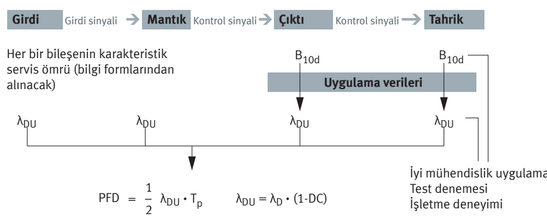
$$PFH = \frac{1}{MTTF_d}$$

Yüksek talep modu



$$PFH = \frac{1}{MTTF_d} = \sum_{i=1}^{N}\frac{1}{MTTF_{d,i}}$$

Düşük talep modu



$$PFD = \frac{1}{2}\lambda_{DU} \cdot T_p \qquad \lambda_{DU} = \lambda_D \cdot (1\text{-}DC)$$

- **PFH (Saatlik Arıza Olasılığı)**
  PFH (Saatlik Arıza Olasılığı)
- **MTBF (İki Arıza Arası Ortalama Süre)**
  İki ardışık arıza arasında geçen ortalama süre
- **PFD (Talep Anında Arıza Olasılığı)**
  Düşük bir gereksinim oranında herhangi bir güvenlik işlevinin talep anında çalıştırılamama olasılığı
- **T_p (Deneme test aralığı)**
  İşlevin normal olarak tamamen incelenmesi

5 Tüm sistem – Hedef: $PL > PL_r$

Bir kontrol sisteminin güvenlikle ilgili parçalarına ait örnek yerleşim düzeni

Girdi	Mantık	Çıktı		Tahrik
		Bileşen 1	Bileşen 2	
$B10_d$		$B10_d$	$B10_d$	
		$MTTF_d$	$MTTF_d$	
$MTTF_d$		Her bir kanal başına $MTTF_d$		
Cat		Cat		
DC		DC		
CCF		CCF		
PL	PL	PL		

İmalatçı tarafından belirlenir — Sistem işletmecisi tarafından belirlenecek

En düşük PL PL_{low}	En düşük PL sayısı N_{low}	Tüm sistem PL
a	>3	izin yok
	≤3	a
b	>2	a
	≤2	b
c	>3	b
	≤3	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Hedef: $SIL > SIL_r$

Tek bir güvenlik döngüsü içerisindeki bir güvenlik işlevine ait alt sistemler arasındaki PFD/PFH dağılımı

Sensör ≤ 35%		Mantık ≤ 15%		Aktüatör ≤ 50%	
PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}

$SIL_{required}$ (SIL_r)

PFD_{total}/PFH_{total}

İmalatçı tarafından belirlenir — Sistem işletmecisi tarafından belirlenecek

6 Değerlendirme – Hedef: $PL > PL_r$

$MTTF_d$ tanımı= Arızaya Kadar Ortalama Süre (tehlikeli)

PL tanımı = Performans Seviyesi

	DC < 60% yok	DC < 60% yok	60% ≤ DC < 90% düşük	90% ≤ DC < 99% orta	60% ≤ DC < 90% düşük	90% ≤ DC < 99% orta	99% ≤ DC yüksek
a							
b							
c							
d							
e							
	Kat B	Kat 1	Kat 2		Kat 3		Kat 4
	CCF ilgili değil		CCF > 65 %				

Değerlendirme	$MTTF_d$
Düşük	3 yıl ≤ $MTTF_d$ < 10 yıl
Orta	10 yıl ≤ $MTTF_d$ < 30 yıl
Yüksek	30 yıl ≤ $MTTF_d$ < 100 yıl

→ **PL > PL_r**

Hedef: $SIL > SIL_r$

SIL-Seviyesi	Yüksek Talep Modu	Güvenlik sisteminin maks. kabul edilebilir	Cihaz tipi A – Güvenli Arıza Fraksiyonu (SFF) <60%	60...90%	90...99%	>99%	Cihaz tipi B – Güvenli Arıza Fraksiyonu (SFF) <60%	60...90%	90...99%	>99%	Düşük Talep Modu	
	a	$10^{-5} \le PFH < 10^{-4}$	Her 10.000 saatte bir arıza riski									
1	b	$3 \cdot 10^{-6} \le PFH < 10^{-5}$	Her 1250 günde bir arıza riski	HFT 0				HFT 1	HFT 0			
	c	$10^{-6} \le PFH < 3 \cdot 10^{-6}$	Her 115,74 yılda bir arıza riski								$10^{-2} \le PFD < 10^{-1}$	Her 10 yılda bir
2	d	$10^{-7} \le PFH < 10^{-6}$	Her 115,74 yılda bir arıza riski	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0	$10^{-3} \le PFD < 10^{-2}$	Her 100 yılda bir
3	e	$10^{-8} \le PFH < 10^{-7}$	Her 1157,41 yılda bir arıza riski	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \le PFD < 10^{-3}$	Her 1000 yılda bir
4		$10^{-9} \le PFH < 10^{-8}$	Her 11.574,1 yılda bir arıza riski		HFT 2	HFT 1 HFT 2	HFT 1 HFT 2			HFT 2	HFT 1 HFT 2	$10^{-5} \le PFD < 10^{-4}$	Her 10.000 yılda bir

[her saatte]

- **A tipi cihaz**
  Tüm bileşenlerine ait arıza davranışının ve arıza karakteristiklerinin yeterince belirlendiği cihaz
- **B tipi cihaz**
  En az bir bileşenine ait arıza davranışının ve arıza esnasındaki davranışının yeterince belirlenmemiş olduğu cihaz

→ **SIL > SIL_r**

54707 tr 2010/12