Teollisuusautomaation standardit Osio 5

Osio 1:	SESKOn Komitea SK 65: Teollisuusprosessien ohjaus
Osio 2:	Toiminnallinen turvallisuus: periaatteet
Osio 3:	Toiminnallinen turvallisuus: standardisarja IEC 61508
Osio 4:	Koneiden ohjausjärjestelmät: standardi IEC 62061
Osio 5:	**Riskin arviointi ja turvallisuuden eheyden tason SIL määrittäminen: standardit IEC 61508-5 ja IEC 62061**
Osio 6:	Koneiden ohjausjärjestelmien suunnittelutyökalu SISTEMA
Osio 7:	Hätäpysäytys: standardit ISO 13850 ja IEC 60947-5-5
Osio 8:	Turvaväylät ja niiden valinta: tekninen raportti IEC/TR 62513
Osio 9:	Logiikat: standardi IEC 61131-1 ja 61131-3
Osio 10:	Turvallisuuteen liittyvän elektroniikan asennus- ja muutostyöt

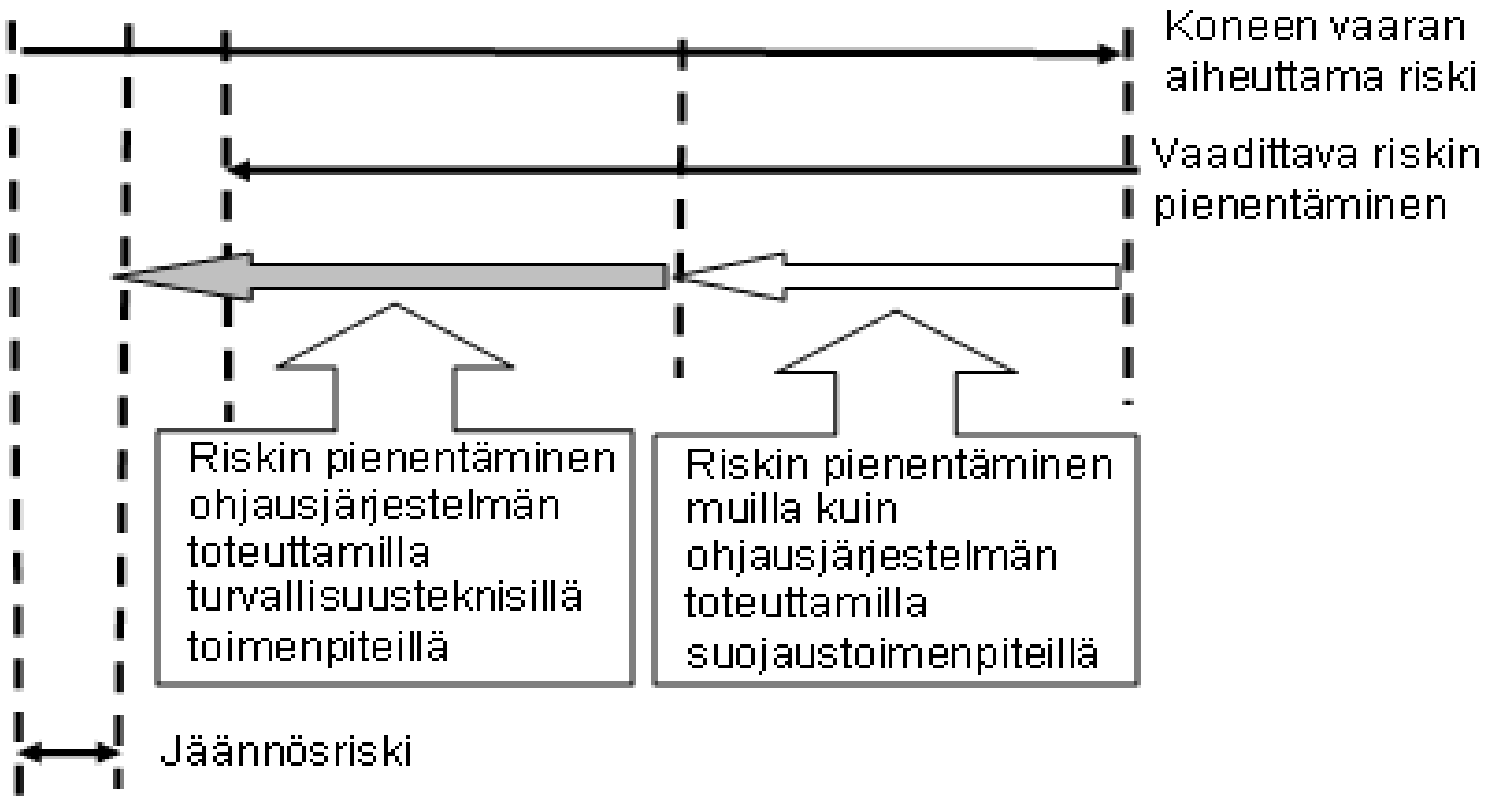
Riskin arviointi ja turvallisuuden eheyden tason SIL määrittäminen: standardi IEC 62061 ja IEC 61508-5

Matti Sundquist
Sundcon Oy

Turvallisuuteen liittyvät ohjaustoiminnot

- Ohjaustoiminnon vaarallinen vikaantuminen voi aiheuttaa riskin:
  - menetetään riskin pienentämiseksi lisätty turvatoiminto (esim. vaikutettaessa valoverhoon vaarallinen liike ei pysähdy)
  - turvallisuuteen liittyvä ohjaustoiminto vikaantuu vaarallisesti (esim. kone käynnistyy odottamatta).

Ohjaustoiminnon osuus riskin pienentämisessä



Standardi IEC 61508-5 kuva A.1, muunneltuna

SIL-tason määrittäminen

- Ohjaustoiminnoille tarkoitettuja riskin arviointimenetelmiä on standardien liitteissä.
- Vaihtoehtoja:
  - Riskimatriisi (IEC 62061 liite A, ks. sivut 7...9)
  - Riskigraafi (SFS-EN ISO 13849-1liite A)
  - LOPA (Layer of Protection Analysis, IEC 61508-5, ks. kuvat sivuilta 12...15)
  - tai edelliset yhdessä LOPAn kanssa.

Riskimatriisi

- Riskimatriisi (Hazard Matrix) on kvalitatiivinen (luokitteluun perustuva) riskin arviointimenetelmä.
- Sen käyttöön tarvitaan insinööriasiantuntemusta.
- LOPA voi olla tässäkin apuna (ks. IEC 61511-5).

Riskin määritelmä ja riskitekijät

- Riski (R) on ei-toivotun tapahtuman seurausten (Se) ja niiden todennäköisyyden funktio.
- Seuraukset (Se) luokitellaan niiden vakavuuden mukaan.
- Seurausten todennäköisyys luokitellaan riskitekijöiden avulla:
  - vaaralle altistumisen taajuus (Fr)
  - vaarallisen tapahtuman todennäköisyys (Pr)
  - mahdollisuus välttää vaaraa (Av)

Riskimatriisi ja SIL-tasojen määrittäminen

Seuraukset	Vakavuus Se	Luokka Cl				
		3-4	5-7	8-10	11-13	14-15
Kuolema, näön tai käden menetys	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Palutumaton, sormen menetys	3			SIL 1	SIL 2	SIL 3
Palautuva, sairaanhoiti	2				SIL 1	SIL 2
Palautuva, ensiapu	1					SIL 1

Taajuus ja kesto Fr		Vaarallisen tapahtuman todennäköisyys, Pr		Vältettävyys Av.	
<= 1 tunti	5	Erittäin todennäköinen	5		
> 1 t - <=päivä	5	Todennäköinen	4		
>1 päivä - <=2 viikkoa	4	Mahdollinen	3	Mahdoton	5
>2 vko - <=1 vuosi	3	Harvoin	2	Mahdollista	3
> 1 vuosi	2	Ei huomioitava	1	Todennäköistä	1

R = f(Se,Cl) Cl = Fr + Pr + Av

Standardi IEC 62061 kuva A.3, muunneltuna

Suoritustasot PL ja turvallisuuden eheyden tasot SIL

MTTFd = keskimääräinen vaarallinen vikaantumisaika (1 vuosi on 8760 tuntia = noin 10^4 tuntia

PFH = Vaarallisen vikaantumisen keskimääräinen todennäköisyys

PL	SIL	PFH [1/tunti]	$MTTF_d$ (likimääräisesti) vuotta
a	-	$\geq 10^{-5}$ ... $< 10^{-4}$	1...10
b	1	$\geq 3 \times 10^{-6}$ ... $< 10^{-5}$	10...30
c	1	$\geq 10^{-6}$ ... $< 3 \times 10^{-6}$	30...100
d	2	$\geq 10^{-7}$ ... $< 10^{-6}$	100...1000
e	3	$\geq 10^{-8}$ ... $< 10^{-7}$	1000...10000

Standardi IEC 62061 taulukko 3, muunneltuna

Riskigraafi

- Riskigraafi on kvalitatiivinen luokitteluun perustuva riskin arviointimenetelmä.
- Standardissa IEC 61508-5 riskigraafissa on edellä esitettävien parametrien Se, Fr ja Av lisäksi turvatoiminnon vaadetaajuus (Demand Rate, W) eli kuinka usein tarvitaan turvatoimintoa (tällä on usein sama taajuus kuin alkutapahtumalla Initial Event).

LOPAn taustaa

- LOPA (Layer of Protection Analysis) perustuu toistaan riippumattomiin suojauskerroksiin, joilla pienennetään vaarallisen tapahtuman todennäköisyyttä.
- Käyttöjärjestelmään kuuluvat prosessin ohjaustoiminnot pienentävät vikaantumisen todennäköisyyttä, mutta jos ei riittävästi, tarvitaan lisäksi turva-automaatiota. Harvojen vaateiden tapauksessa turva-automaatio on usein prosessin “alasajojärjestelmä”.

LOPAn menettelytapa

- Ei-toivotun tapahtuman määrittäminen
- Siedettävän riskin määrittäminen
- Laukaisevat tekijät (Initial Events) ja niiden yhteinen taajuus
- Riskiä pienentävät toimenpiteet (riippumattomat LOPA-suojauskerrokset)
- Tuloksena on ei-toivotun tapahtuman taajuus, jota verrataan siedettävään riskiin.

LOPAn menettelytapa

- Vaarallisen tapahtuman toteutumisen todennäköisyys saadaan kertomalla alkutapahtuman taajuus LOPA-suojauskerrosten toiminnan onnistumisen todennäköisyyksillä (ks. sivu 15).
- Jos saatu riski on suurempi kuin siedettävä riski, alkutapahtuman taajuutta on pienennettävä tai lisättävä suojauskerroksia.
- Tavallisesti lisätään turva-automaatio (sivulla 15 punaisella merkitty suojauskerros).

Esimerkki LOPA-analyysistä

Tulipalon todennäköisyys = 0,5 / vuottax0,01x0,07x0,03 = 0,00021 / vuotta

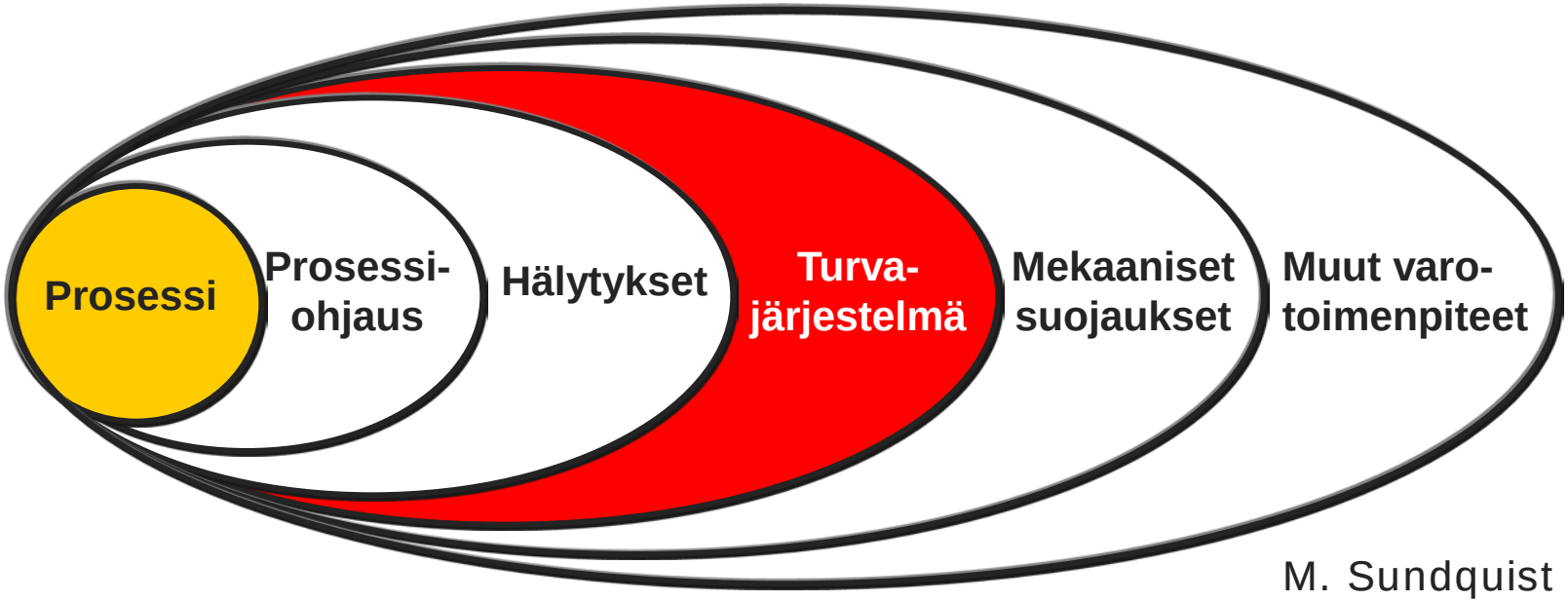
Jäähdytys-veden menetys	Prosessi-suunnittelu	Operaattorin toiminta	Varo-venttiili	Ei sytytystä	Tulipalo
				0,3	$2,1x10^{-5}$
			0,07		
		0,2			
	0,01				
0,5 / vuosi					

Lähjde: W. Goble/Exida

Ei tapahtumaa

Prosessisuojauksen ”sipulimalli”

Prosessin vaaran etenemisen riskiä pienennetään toisistaan riippumattomilla suojauskerroksilla (Layer of Protection Analysis, LOPA)



M. Sundquist