Layers Of Protection LOPA riskienarviointimenetelmä prosessiteollisuudessa

Sami Matinaho | 07.06.2023 | Espoo

NESTE

Sisältö

IEC 61511 elinkaarimallin vaiheet

Turvatoimintojen kohdentaminen suojauskerroksille

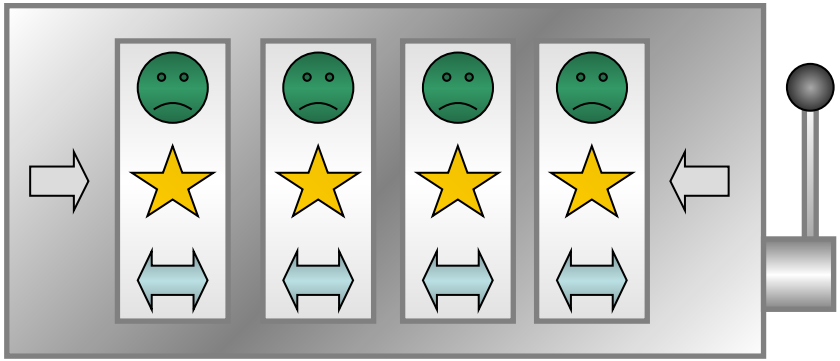
- Turva-automaatiotoimintojen SIL-määrittely

Riskin arviointi

"Yksikätinen rosvo"

Jokaisella kehällä on 10 erilaista kuviota. Jos saat voittolinjalle neljä samaa kuviota, voitat 1 000 000 €. Peli on ilmainen, mutta neljä hapannaamaa voittolinjalla merkitsee, että joudut itse maksamaan 1 000 000 €.

- Millä todennäköisyydellä joutuisit itse maksumieheksi?
- Miten monta kertaa uskaltaisit pelata peliä? Entä jos neljä hapannaamaa voittolinjalla merkitsisi ihmishengen menetystä?

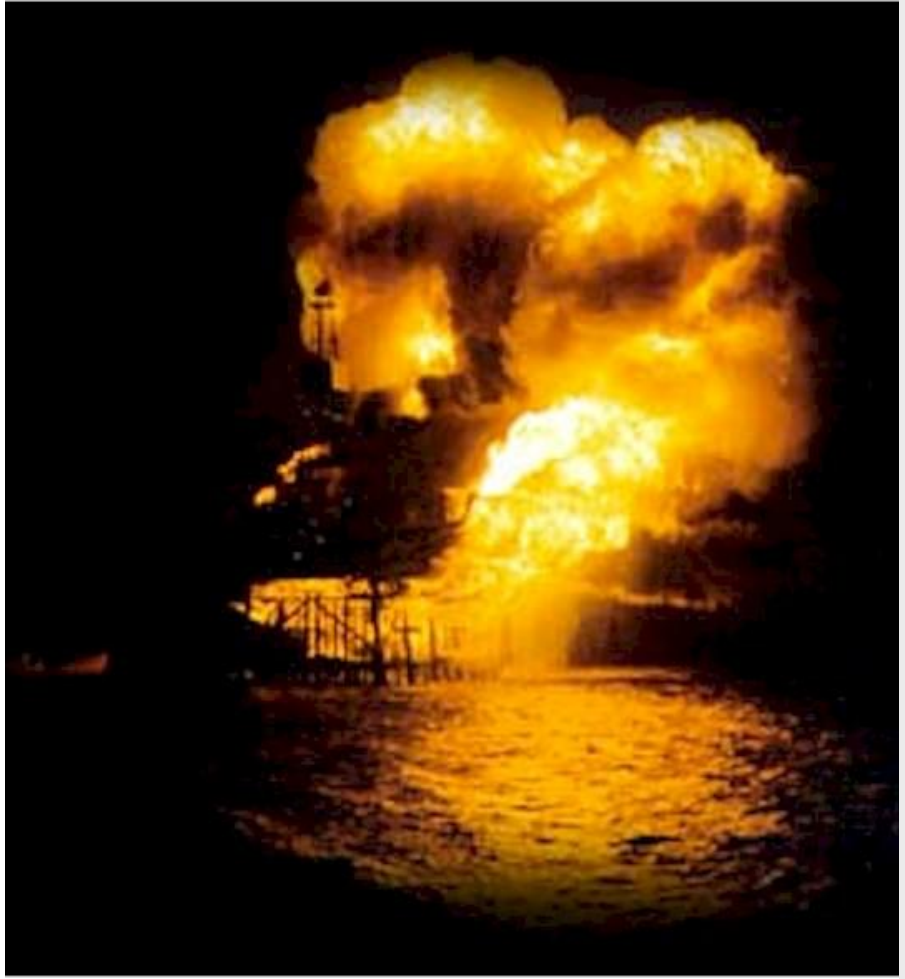


Riskin arviointi

Riskianalyysin perusta on siedettävä/hyväksyttävä riski
Miten suuri on siedettävä/hyväksyttävä riski?
Kuka sen määrittelee?

- Health & Safety Executive, UK, 10^{-4}
- VROM, Alankomaat, 10^{-5}

ALARP-periaate
(As Low As Reasonably Practicable)



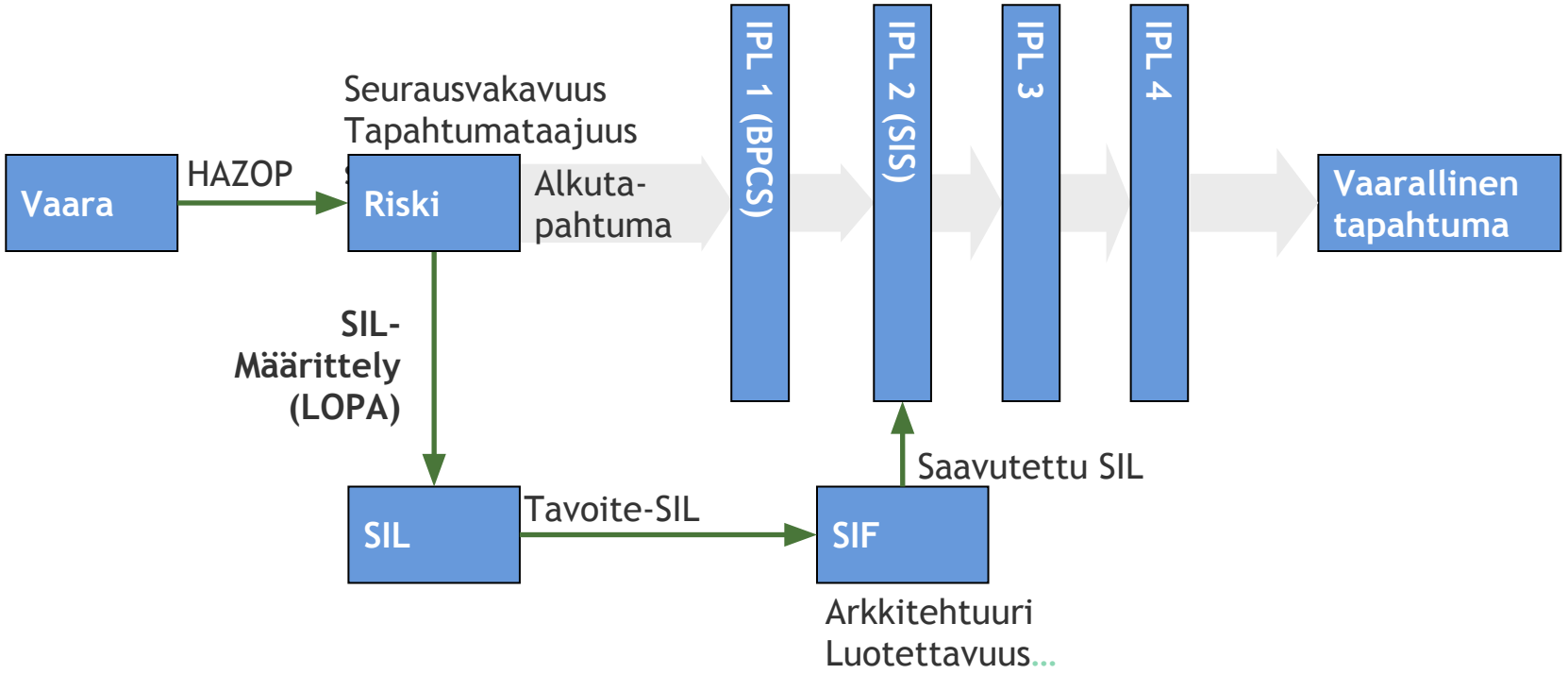
Riskin arviointi, menetelmiä

- Asiantuntija-arvio (expert judgment)
- Riskimatriisi (risk matrix)
- Syy-seurauskaavio (cause consequence diagram)

- **Riskigraafi (risk graph)**
- **LOPA (layer of protection analysis)**

- Tapahtumapuuanalyysi (event tree analysis)
- Vikapuuanalyysi (fault tree analysis)

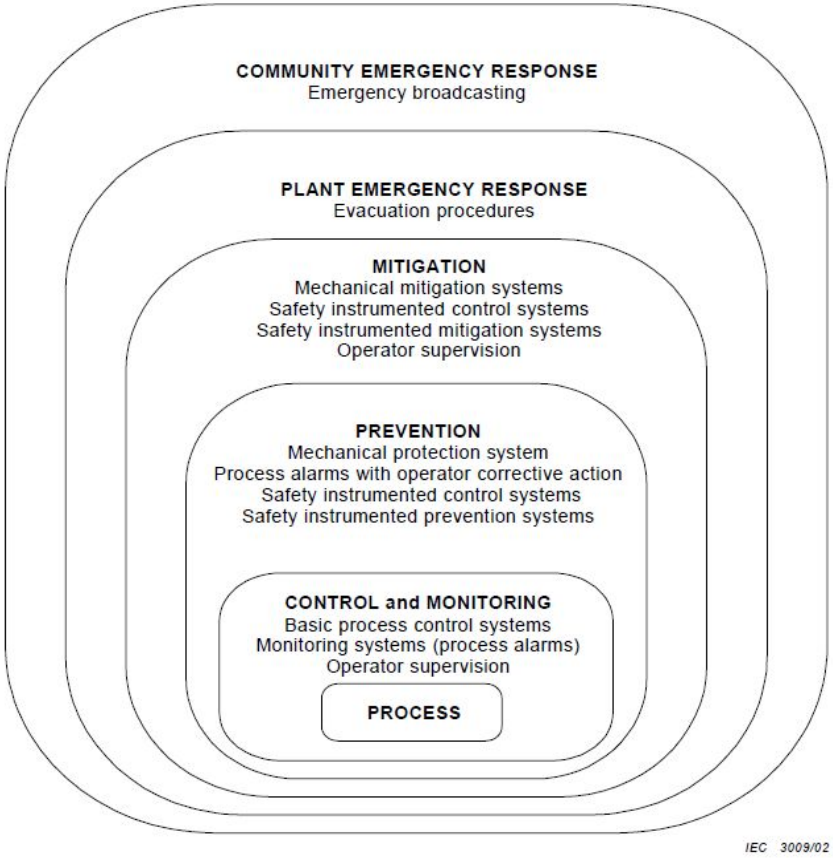
HAZOP/SIL-rajapinta



LOPA, Layer of protection analysis

- Yksinkertaistettu kvantitatiivinen riskinarviointimenetelmä
- ”Semi-kvantitatiivinen” menetelmä
- 1993, CCPS: Guidelines for Safe Automation of Chemical Processes, "risk-based SIS integrity level method", tämän jälkeen menetelmää on kehitetty eri yrityksissä
- 2001, CCPS: Layer of Protection Analysis — Simplified Process Risk Assesment
- IEC 61511-3, Annex F
- IEC 61508-5, Annex F

- Käytössä Nesteellä vuodesta 2017



LOPA, skenaario

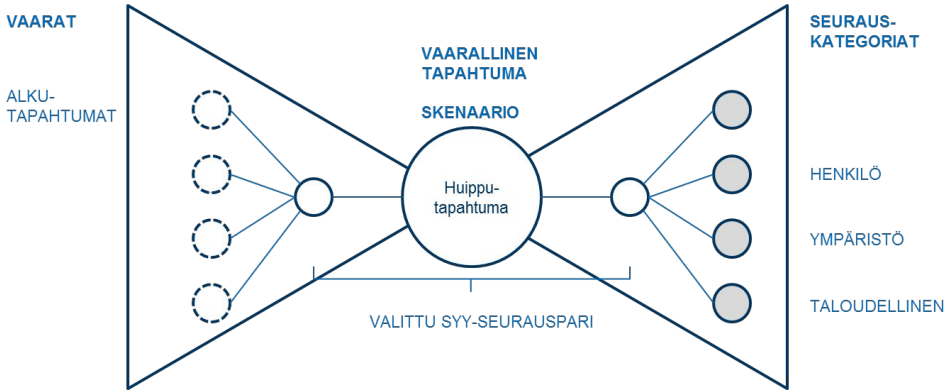
LOPA:n perusyksikkö on skenaario eli vaarallisen tapahtuman tapahtumaketju

- Skenaario koostuu yhdestä syy/seuraus-parista
- Prosessiteollisuudessa yleisin LOPA-skenaario on vaarallisen aineen tai energian päästö

Skenaario ja sen seuraukset kuvataan mahdollisimman tarkasti

- Täydennetään HAZOP:ista saatua kuvausta
- Pyritään kuvaamaan vakavin tapaus
- Suojaavia keinoja kuten turva-automaatio ja varolaitteet ei vielä huomioida

  => ne huomioidaan myöhemmin suojauskerroksina eli IPL:inä



“Bow-tie”

LOPA, seurauksen vakavuuden arviointi

Tässä esityksessä esitellään kaksi eri tapaa seurauksen vakavuuden arviointiin:

1. **Päästön suuruus ja tyyppi**
2. Loukkaantumisten/ kuolemantapausten määrä

LOPA, seurauksen vakavuuden arviointi
Tapa 1: Päästön suuruus ja tyyppi

Päästön tyyppi	Päästön suuruus					
	1 - 10 kg	10 - 100 kg	100 - 1000 kg	1000 - 10 000 kg	10 000 - 100 000 kg	100 000+ kg
Erittäin myrkyllinen kaasu	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 4	Kategoria 4	Kategoria 4
Erittäin myrkyllinen neste tai myrkyllinen kaasu	Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 4	Kategoria 4
Myrkyllinen neste tai herkästi syttyvä kaasu	Kategoria 1	Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 4
Herkästi syttyvä neste tai syttyvä kaasu	Kategoria 0	Kategoria 1	Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4
Syttyvä neste	Kategoria 0	Kategoria 0	Kategoria 0	Kategoria 1	Kategoria 1	Kategoria 2

	Vahingosta aiheutuvat kustannukset				
	0 - 10 000 €	10 000 - 100 000 €	100 000 - 1 000 000 €	1 000 000 - 10 000 000 €	10 000 000+ €
Korjauskustannukset ja menetetty tuotanto	Kategoria 0	Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4

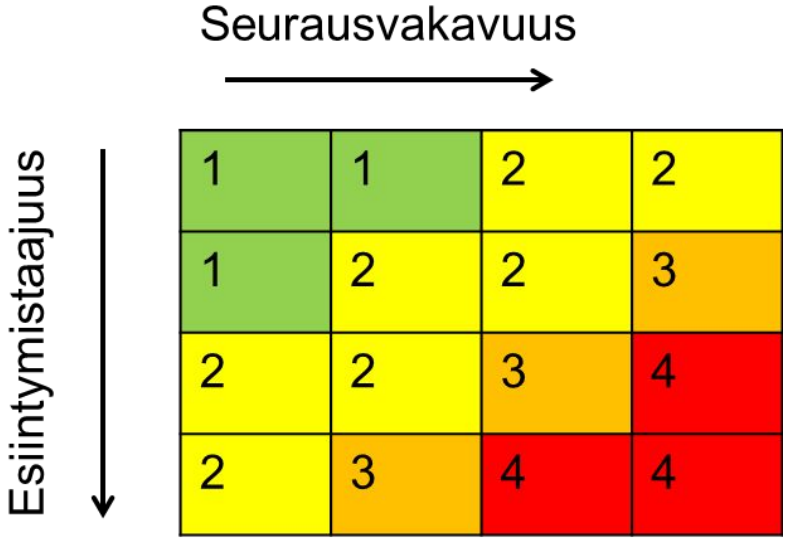
LOPA, seurauksen vakavuuden arviointi
Tapa 2: Loukkaantumisten/kuolemantapausten määrä

Kategoria	Henkilö	Ympäristö	Taloudellinen
1	Lievä loukkaantuminen; ei menetettyä työaikaa	Kirjattava tapahtuma, mutta ei viranomaisilmoitusta tai ympäristöluvan rikkomista	Kustannukset alle 100 000 €
2	Yksi ei-vakava loukkaantuminen; mahdollisesti menetettyä työaikaa	Tapahtuma, joka johtaa viranomaisilmoitukseen tai ympäristöluvan rikkomiseen.	Kustannukset 100 000 – 1 000 000 €
3	Yksi tai useampi vakava loukkaantuminen	Merkittävä päästö, jolla vakavia seurauksia alueen ulkopuolella.	Kustannukset 1 000 000 – 10 000 000 €
4	Yksi kuolemantapaus tai pysyvästi vammautunut	Sama kuin ed. ja välittömiä tai pitkäaikaisia terveysvaikutuksia.	Kustannukset yli 10 000 000 e

LOPA, tavoitetaso (target frequency)

Tavoitetaso (f_{target}) on se skenaarion esiintymistaajuus, jolla riski on siedettävällä/hyväksyttävällä tasolla

Riskimatriisi on yleisimmin käytetty työkalu tavoitetason määrittämiseen



LOPA, riskimatriisi

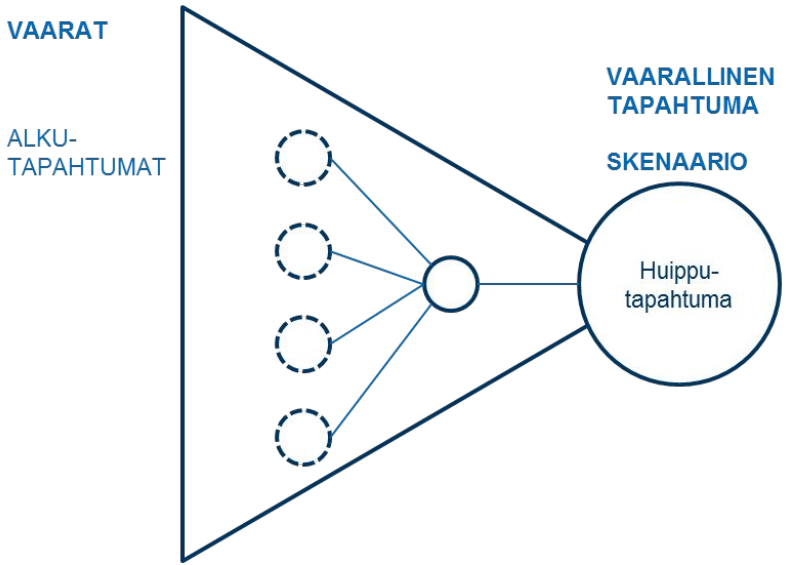
Vakavuus Todennäköisyys/vuosi (Tapahtumataajuus)	Kategoria 0 Erittäin lievä	Kategoria 1 Lievä	Kategoria 2 Vakava	Kategoria 3 Erittäin vakava	Kategoria 4 Katastrofaalinen
100 % (tapahtuu vuosittain, 1/1 a)					
10 % (tapahtuu 1/10 a)					
1 % (tapahtuu 1/100 a)					
0,1 % (… 1/1000 a)					
0,01 % (… 1/10000 a)					

	Erittäin matala riski	Toimenpiteet ovat tehottomia, riski on hyväksyttävä
	Matala riski	Toimenpiteitä ei tarvita, riski on siedettävä
	Kohonnut riski	Toimenpiteet voidaan haluttaessa toteuttaa
	Korkea riski	Toimenpiteet toteutettava kun seuraavan kerran mahdollisuus
	Erittäin korkea riski	toimenpiteet toteutetaan välittömästi
	Kriittinen riski	Toiminta lopetettava välittömästi

LOPA, alkutapahtuma (initiating event)

Tarkastellaan skenaarion mahdolliset alkutapahtumat ja määritellään alkutapahtuman esiintymistaajuus

- Esiintymistaajuus valitaan etukäteen määritetyistä taulukkoarvoista (ks. seuraava kalvo)

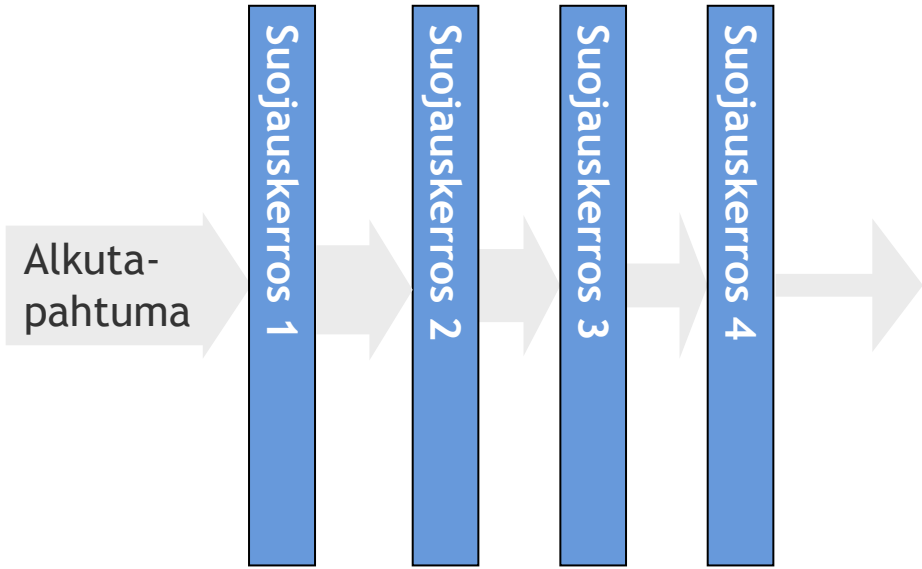


LOPA, alkutapahtuman taajuus, $f_{initiating\ event}$

Initiating Event	Frequency Range from Literature (/year)	Example Value Chosen for LOPA (/year)
Pressure vessel rupture	10^{-5} to 10^{-7}	$1 \cdot 10^{-6}$
Piping Leak (10% section) - 100 m	10^{-3} to 10^{-4}	$1 \cdot 10^{-3}$
Gasket/Packing Blowout	10^{-2} to 10^{-6}	$1 \cdot 10^{-2}$
External Impact (by backhoe, vehicle, etc.)	10^{-2} to 10^{-4}	$1 \cdot 10^{-2}$
Safety Valve Opens Spuriously	10^{-2} to 10^{-4}	$1 \cdot 10^{-2}$
Cooling Water Failure	1 to 10^{-2}	$1 \cdot 10^{-1}$
Pump Seal Failure	10^{-1} to 10^{-2}	$1 \cdot 10^{-1}$
BPCS Instrument Loop Failure	1 to 10^{-2}	$1 \cdot 10^{-1}$
Operator Failure (to execute a complete, routine procedure; well-trained operator, unstressed, not fatigued)	10^{-1} to 10^{-3} /Opportunity	$1 \cdot 10^{-2}$ /Opportunity
Pump failure (motor or mechanical failure)		$1 \cdot 10^{-1}$
Wrong manipulation of random valve (opened or closed)		$1 \cdot 10^{-1}$

LOPA, suojauskerros (IPL)

1. **Riippumattomuus**
   - skenaarion alkutapahtumasta ja muista suojauskerroksista
2. **Tehokkuus**
   - Vähentää skenaarion riskiä vähintään kertoimella 10 (RRF > 10)
   - ”Big enough, strong enough, fast enough”
3. **Jäljitettävyys**



LOPA, suojauskerros (IPL)

Passiiviset IPL:t

- Pato, viemäröinti, hönkäputki, palonkestävät rakenteet, suojaseinä, ”inherently safe” suunnittelu, liekinestin

Aktiiviset IPL:t

- Automaatio: käyttöautomaatiojärjestelmä (BPCS), turva-automaatiojärjestelmä (SIS)
- Varolaitteet: varoventtiili, murtolevy

Operaattoritoiminto IPL:nä

- Edellytyksenä riittävä reagointiaika (Esim. Nesteellä 30 min)

Näitä ei yleensä pidetä IPL:inä:

- Koulutus, ohjeet, normaali testaus, kunnossapito, viestintä, merkinnät, palontorjunta

LOPA, IPL:ien hierarkia

1. Mekaaniset IPL:t
2. Turva-automaatiotoiminnot (SIF)
3. Passiiviset IPL:t, esim. pato
4. BPCS:ssä toteutetut turva-automaatiotoiminnot ja operaattoritoiminnot

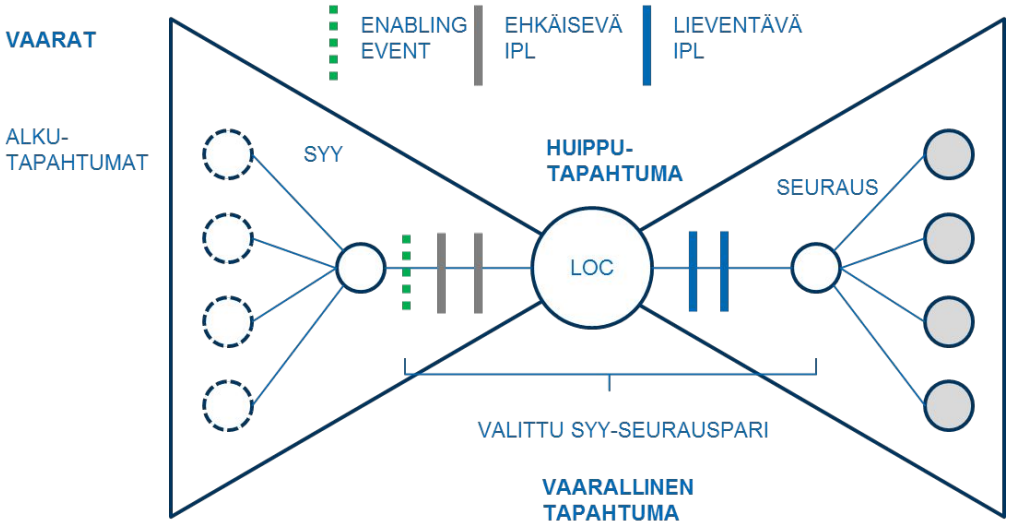
LOPA, IPL:n riskinvähennys

Suojauskerroksen (IPL) riskinvähennyskykyä kuvaa:

- **PFD** (Probability to Fail on Demand) tai
- **RRF** (Risk Reduction Factor)

PFD ja RRF ovat toistensa käänteislukuja

Arvot valitaan etukäteen määritetyistä taulukkoarvoista (ks. seuraava kalvo)

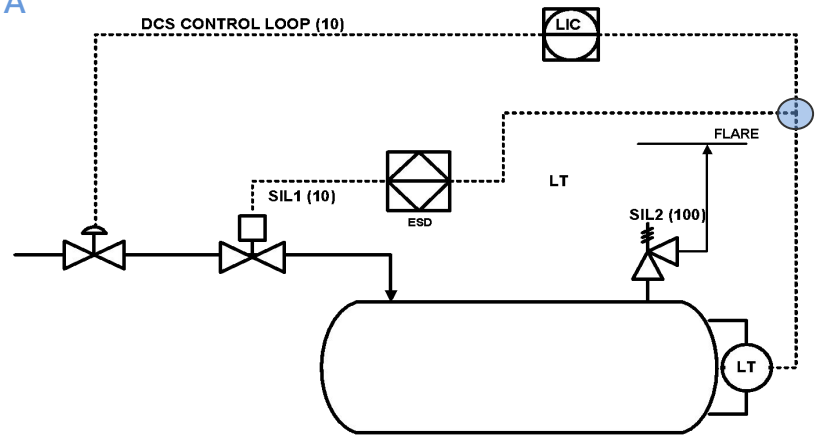


IPL Type	Description	PFD from Literature and Industry	Example PFD Chosen for LOPA	RRF
BPCS (DCS)	Basic process control system; automatic control loop independent of the initiating event	10^{-1} to 10^{-2}	$1 \cdot 10^{-1}$	10
Human response (10 min available)	Human response with 10 minutes available for response; notification must be independent of initiating event and other IPLs, and operator training must include required response	1 to 10^{-1}	1	1
Human response (40 min available)	Human response with 40 minutes available for response; notification must be independent of initiating event and other IPLs, and operator training must include required response	10^{-1} to 10^{-2}	$1 \cdot 10^{-1}$	10
Passive	Passive device (e.g., a dike with good control over drains) that is not required to take an action in order for it to achieve its function in reducing risk	10^{-1} to 10^{-3}	$1 \cdot 10^{-2}$	100
Relief device	Relief valve or rupture disk (effectiveness is sensitive to service and experience)	10^{-1} to 10^{-5}	$1 \cdot 10^{-2}$	100
SIL 3 SIF	**SIL 3 interlock independent of other interlocks**	**10^{-3} to 10^{-4}**	**$1 \cdot 10^{-3}$**	**1000**
SIL 2 SIF	**SIL 2 interlock independent of other interlocks**	**10^{-2} to 10^{-3}**	**$1 \cdot 10^{-2}$**	**100**
SIL 1 SIF	**SIL 1 interlock independent of other interlocks**	**10^{-1} to 10^{-2}**	**$1 \cdot 10^{-1}$**	**10**

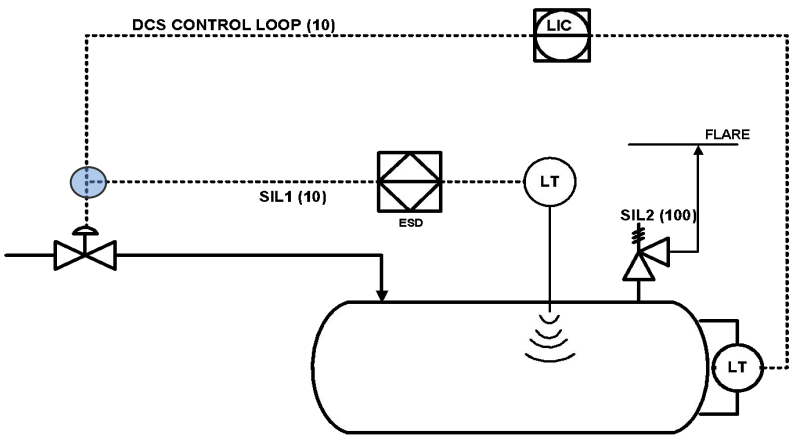
LOPA, suojauskerroksen riippumattomuus

Ovatko alla olevissa kuvissa esitetyt IPL:t toisistaan riippumattomia?

A



B



LOPA, saavutettu taso (final frequency)

Saavutettu riskitaso (final frequency) lasketaan skenaarion alkutapahtuman taajuuden, enabling eventin ja IPL:ien PFD-arvojen tulona

$$f_{final} = f_{i\_event} \times PFD_{IPL\ 1} \times PFD_{IPL\ 2} \times \ldots$$

Seuraavilla arvoilla:
f_{i_event} = 1/10 vuotta = 0,1
$PFD_{IPL\ 1}$ = 0,1 (varoventtiili)
$PFD_{IPL\ 2}$ = 0,1 (SIL 1 SIF)

$f_{final} = 0{,}1*0{,}1*0{,}1 = 1*10^{-3}$ (= 1/1000 vuotta)

LOPA, final frequency vs. target frequency

Skenaarion saavutettua riskitasoa verrataan skenaarion tavoitetasoon

$$f_{final} \leq f_{target}$$

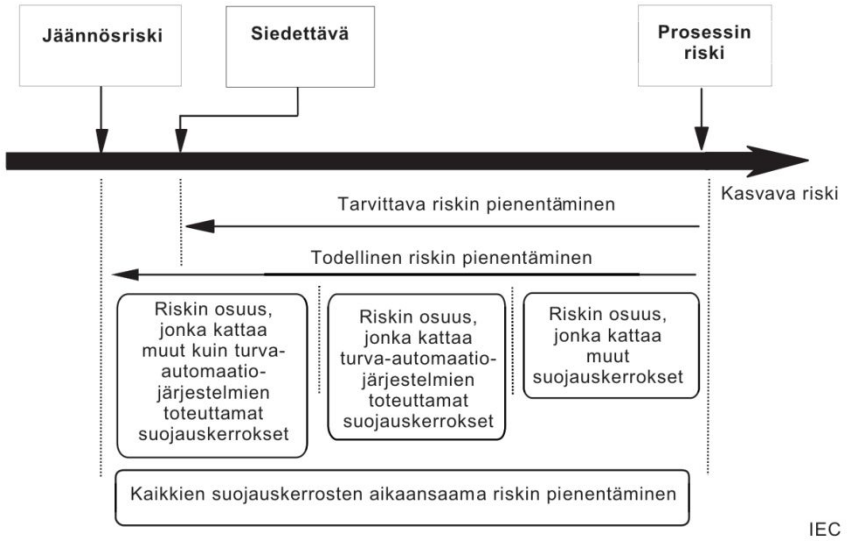
Saavutetaanko tavoitetaso?

Kyllä

- kyseinen LOPA-skenaario on käsitelty ja voidaan siirtyä seuraavaan skenaarioon

Ei

- Harkitaan uusia IPL:iä tai parannetaan jo olemassa olevia
- Jos jäännösriski jää kohonneeksi => suoritetaan ALARP-demonstraatio (Nesteen käytäntö)



LOPA:n toteutus Nesteellä

- Neste käyttää PHA Pro -ohjelmistoa HAZOP:in ja LOPA:n tekemiseen
- HAZOP-skenaario siirtyy automaattisesti LOPA-käsittelyyn mm. seuraavissa tapauksissa
  - SIL-vaateellinen turvatoiminto
  - operaattoritoiminto IPL:nä
  - seurausvakavuus Category 4
  - kohonnut jäännösriski
- SIF:n lopullinen SIL-vaade määritetään SRS-dokumentissa (Safety Requirements Specification)


NESTE
Change runs on renewables