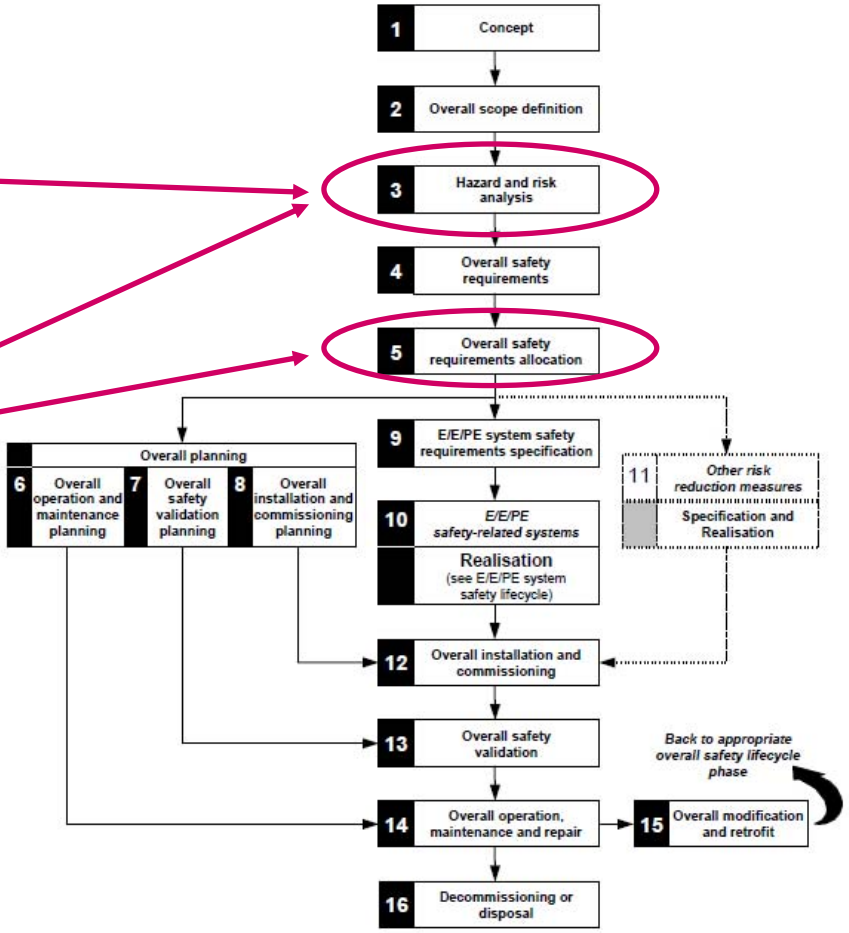
Suomen Automaatioseuran turvallisuusjaosto (ASAF) teemasarja: Toiminnallinen turvallisuus - standardisarja IEC 61508

Vaaran ja riskin arviointi & turvallisuuden eheystasojen (SIL) määritys (riskigraafi ja LOPA)

Insinöörit-ekonomit talo, Itä-Pasila, 17.10.2011

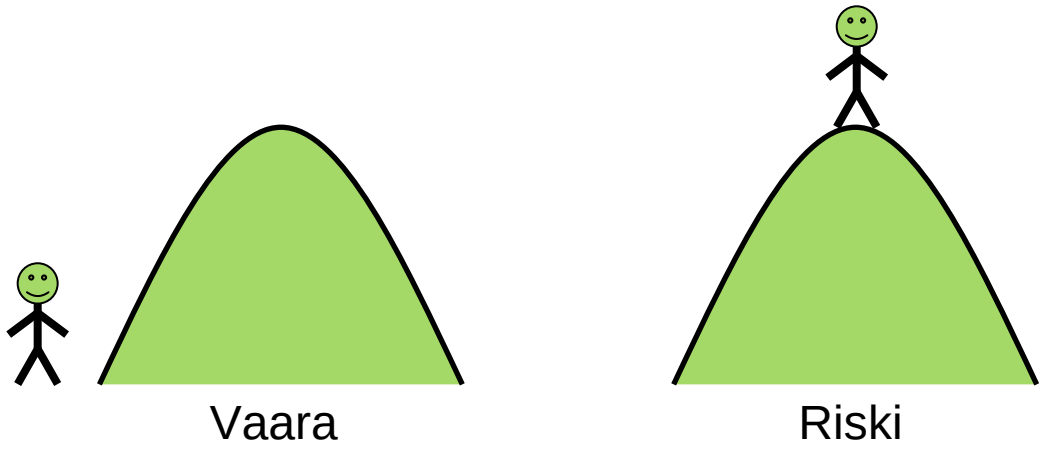
Luennon sisältö

- Osa 1: Vaarojen tunnistaminen ja riskin arviointi
- Osa 2: Layer of Protection Analysis (LOPA)
- Riskigraafi



Lähde: IEC 61508-1

Vaara ja riski – mikä on niiden ero?



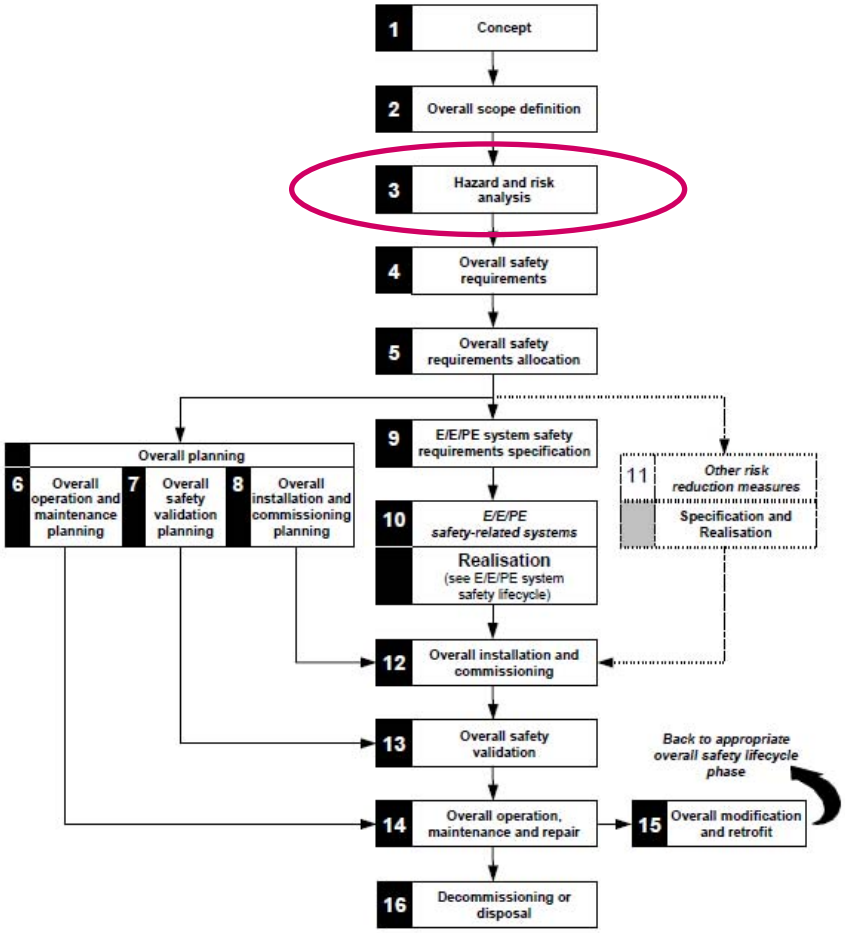
- Vaaran (eng. hazard) määritelmä
  - potential source of harm (ISO/IEC Guide 51:1990, definition 3.3)
- Riskin määritelmä
  - Riski = C x F, jossa

    C = vaarallisen tapahtuman seurauksen vakavuus ja

    F = vaarallisen tapahtuman todennäköisyys

Vaarojen tunnistaminen

- Vaarojen tunnistaminen synnyttää perustan IEC 61508 elinkaarimallin kaikille myöhemmille vaiheille.
- Jos toteutettu turva-automaatiotoiminto ei perustu mihinkään tunnistettuun vaaraan tai vaaralliseen tapahtumaan, se on hyödytön!
  - Turva-automaatiojärjestelmästä, jonka suunnitteluperusteena on jokin muu kuin tunnistetut vaarat, tulee yli- tai alimitoitettu
  - Kumpi on huonompi vaihtoehto? Miksi?



Lähde: IEC 61508-1

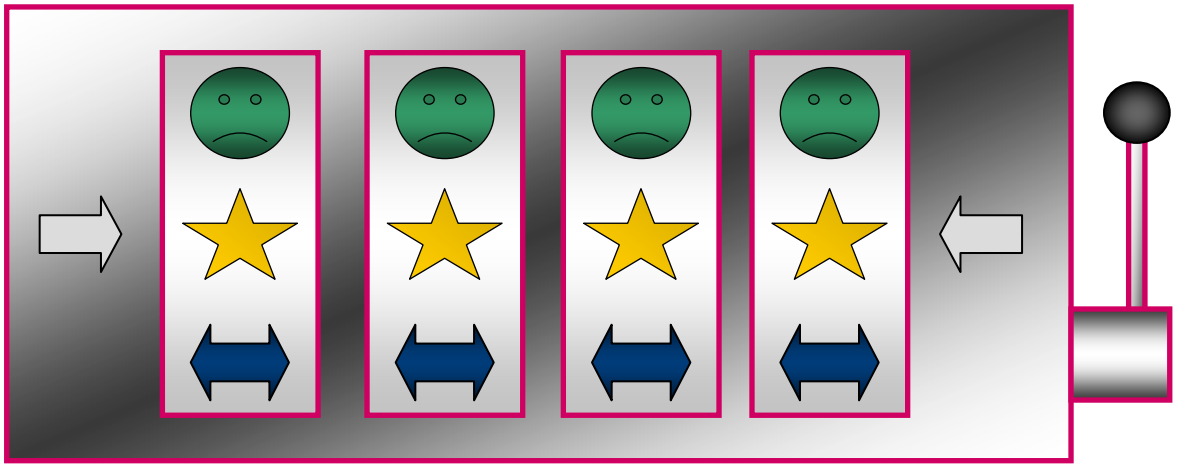
Vaarojen tunnistaminen, HAZOP

- Hazard and operability study, suom. poikkeamatarkastelu
- Kehitetty 1960-luvulla, ICI:n Mond Division (GB)
- Suosituin menetelmä prosessiteollisuuden vaarojen analysointiin
- Systemaattinen menetelmä, joka auttaa tunnistamaan ja arvioimaan kaikki tavat, joilla prosessi voi vikaantua tai joilla prosessia voidaan operoida puutteellisesti
- Voidaan tehdä suunnitteluvaiheessa tai käynnissä olevalle laitokselle
- Työryhmä: vetäjä, kirjuri, jäsenet (ryhmän optimikoko 4–8 henkilöä)

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 €. Kuinka monta kertaa uskaltaisit pelata tällaista peliä? Entä jos neljä hapannaamaa voittolinjalla merkitsisi ihmishengen menetystä?



Riskin arviointi

- Riskianalyysin perusta on siedettävä riski
  - Miten suuri on siedettävä riski?
  - Kuka määrittelee siedettävän riskitason?
  - IEC 61508/61511: ALARP (as low as reasonably practicable)

Riskin arviointi, menetelmiä

- Riskimatriisi (eng. risk matrix)
- **Riskigraafi (risk graph)**
- Vikapuuanalyysi (fault tree analysis)
- Tapahtumapuuanalyysi (event tree analysis)
- Syy-seurauskaavio (cause consequence diagram)
- Asiantuntija-arvio (expert judgment)
- **LOPA (layer of protection analysis)**

- Kvalitatiiviset menetelmät
- Kvantitatiiviset menetelmät

Osa 2

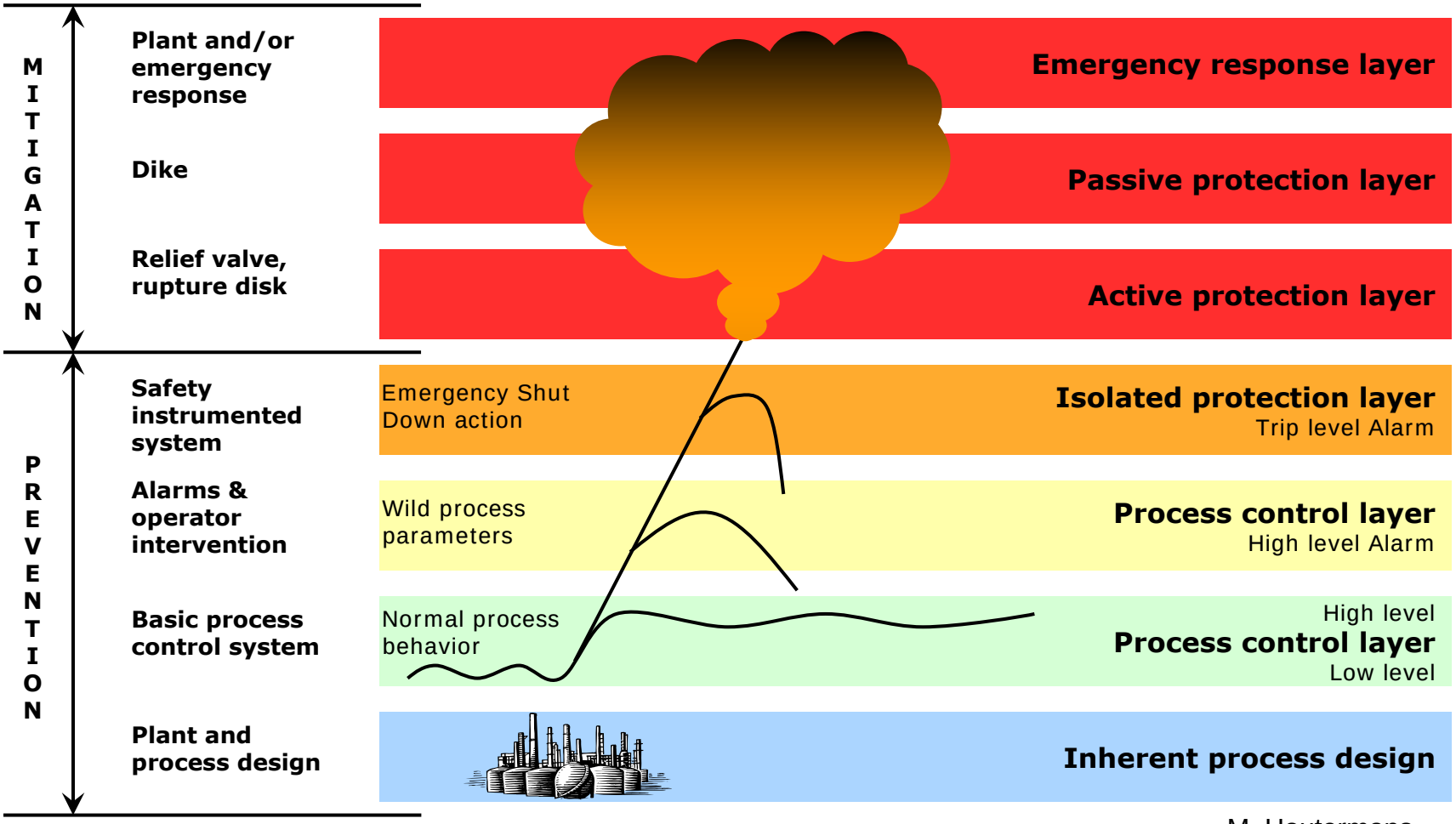
- Layer of Protection Analysis (LOPA)

LOPA, Layer of protection analysis

- Yksinkertaistettu kvantitatiivinen riskinarviointimenetelmä

- 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
- 2003, IEC 61511-3, Annex F
- **2010, IEC 61508-5, Annex F**

LOPA, Layers of protection -idea



M. Houtermans

LOPA, tavoitetaso (target frequency)

- Tavoitetaso (f_{target}) on sellainen vaarallisen tapahtuman (tai LOPA-termeillä skenaarion) esiintymistaajuus, joka täyttää viranomaisten asettamat ja/tai yrityksen omat riskikriteerit.
- Riskimatriisi on yleisimmin käytetty työkalu tämän tavoitetason määrittämiseen, ks. seuraava kalvo.

Skenaario | Kategoria | Alkutapahtuma | IPL | Saavutettu taso | **Tavoitetaso**

LOPA, riskimatriisi

Kategoria / Taajuus (/vuosi)	Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 5
10e-0...10e-1	2	2	3	4	4
10e-1...10e-2	2	2	3	3	4
10e-2...10e-3	1	2	2	3	3
10e-3...10e-4	1	1	2	2	3
10e-4...10e-5	1	1	1	2	2
10e-5...10e-6	1	1	1	1	2
10e-6...10e-7	1	1	1	1	1

- Riskiluokat
  - 4 = Toimenpiteet toteutetetaan välittömästi
  - 3 = Toimenpiteet toteutetaan kun seuraavan kerran mahdollisuus
  - 2 = Toimenpiteet voidaan haluttaessa toteuttaa
  - 1 = Ei toimenpiteitä (siedettävä riski) => tavoitetaso!
- Tavoitteena riskiluokka 1:
  - Kategorian 3 tapahtumalle f_{target} enintään 10e-4, jne...

LOPA, skenaario

- LOPA:n perusyksikkö on skenaario eli vaarallisen tapahtuman tapahtumaketju
  - Skenaario koostuu yhdestä syy-seurausparista
  - Skenaariot valitaan tunnistettujen vaarojen joukosta jollakin sovitulla kriteerillä
  - Yleisin LOPA-skenaario on vaarallisen aineen tai energian päästö
  - Relevantti HAZOP-skenaario ei välttämättä ole relevantti LOPA-skenaario
- Skenaario ja sen seuraukset (worst case) kuvataan mahdollisimman tarkasti
  - Suojaavia keinoja, kuten SIS ja varolaitteet, ei huomioida vielä tässä vaiheessa

LOPA, skenaario

- Relevantti LOPA-skenaario:
  - skenaario, joka voi johtaa prosessin suunnitteluarvon ylittävään poikkeamaan
  - ja joka johtaa vaarallisen aineen tai energian päästöön
  - ja jolta voidaan suojautua ehkäisevillä ja aktiivisilla keinoilla, kuten suojaustoiminnot, mekaaniset laitteet (varoventtiilit yms.), operointi, automaatiojärjestelmät
- Ei-relevantti LOPA-skenaario
  - aiheuttajana korroosio, kuluminen, suunnitteluvirhe, rakennusvirhe tms.
  - joku muu lähestymistapa suositeltavampi:
    - Lainsäädäntö, prosessin lisenssorin tai laitetoimittajan vaatimukset, standardit, konedirektiivi, suunnitteluohjeet, laatujärjestelmä

Skenaario | Kategoria | Alkutapahtuma | IPL | Saavutettu taso | **Tavoitetaso**

LOPA, kategoria

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 3	Kategoria 4	Kategoria 5	Kategoria 5	Kategoria 5	Kategoria 5
Erittäin myrkyllinen neste tai myrkyllinen kaasu	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 5	Kategoria 5	Kategoria 5
Myrkyllinen neste tai herkästi syttyvä kaasu	Kategoria 2	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 5	Kategoria 5
Herkästi syttyvä neste tai syttyvä kaasu	Kategoria 1	Kategoria 2	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 5
Syttyvä neste	Kategoria 1	Kategoria 1	Kategoria 1	Kategoria 2	Kategoria 2	Kategoria 3

Skenaarion vakavuus luokitellaan *kalibroidulla* matriisilla

	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 1	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 5

Skenaario **Kategoria** Alkutapahtuma IPL Saavutettu taso **Tavoitetaso**

LOPA, alkutapahtuma (initiating event)

- Tunnistetaan skenaarion alkutapahtuma ja määritellään alkutapahtuman esiintymistaajuus
  - Esiintymistaajuus valitaan standardiarvoista, ks. seuraava kalvo

Skenaario **Kategoria** **Alkutapahtuma** IPL Saavutettu taso **Tavoitetaso**

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

Alkutapahtuman taajuus valitaan taulukoiduista standardiarvoista

Initiating Event	Frequency Range from Literature (/year)	Frequency 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

LOPA, useampi alkutapahtuma

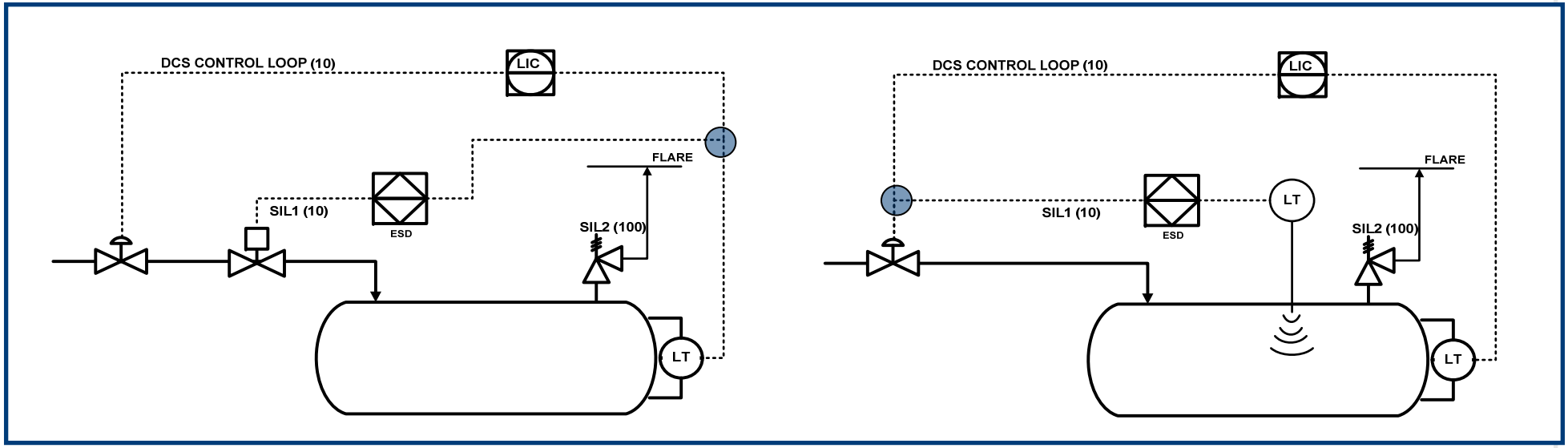
- Jos skenaarion toteutumiseen vaaditaan useampi samanaikainen alkutapahtuma, niin esiintymistaajuus saadaan taajuuksien tulona
  - esim. kahden vaadittavan alkutapahtuman tapauksessa, jossa venttiilin vikaantuminen 0,1/vuosi ja operointivirhe 0,1/vuosi => $f_{\text{inititing event}}$ = 0,1*0,1 = 0,01/vuosi
- Jos skenaarion toteutumisen mahdollistaa useampi yksittäinen alkutapahtuma, niin esiintymistaajuudeksi valitaan arvoltaan suurin taajuus
  - esim. samaan skenaarioon johtaa joko operointivirhe 0,1/vuosi tai varoventtiilin virheellinen avautuminen 0,01/vuosi => valitaan LOPA-käsittelyn pohjaksi näistä suurempi eli $f_{\text{inititing event}}$ = 0,1/vuosi

LOPA, suojauskerros (IPL)

- LOPA-menetelmässä keinoja vähentää riskiä kutsutaan suojauskerroksiksi (IPL, **independent** protection layer).
- Skenaarion liittyvät IPL:t tunnistetaan, kirjataan ylös ja jokaiselle kerrokselle määritellään riskinvähennyskerroin (RRF tai PFD).
- IPL:n kriteerit:
  - vähentää skenaarion riskiä vähintään kertoimella 10 (RRF > 10)
  - IPL on suunniteltu estämään tai lieventämään tiettyä vaarallista tapahtumaa
  - IPL on **riippumaton** skenaarion alkutapahtumasta ja muista samassa skenaariossa käytetyistä IPL:stä (esim. yhteisviat)
  - IPL toteuttaa luotettavasti sen toiminnon, mihin se on suunniteltu
  - IPL:n toimivuus on voitava varmentaa (dokumentointi, tarkastus, testaus, V&V...)

LOPA, suojauskerroksen riippumattomuus

- Ovatko alla olevissa esimerkeissä esitetyt IPL:t toisistaan riippumattomia?



LOPA, suojauskerroksen RRF/PFD

- Suojauskerroksen RRF (risk reduction factor, esim. 100) tai vaihtoehtoisesti PFD (probability to fail on demand, esim. $1 \cdot 10^{-2}$) valitaan standardiarvoista, ks. seuraava kalvo
  - PFD ja RRF ovat toistensa käänteislukuja, joten
    - PFD-arvo 1/100 vastaa RRF-arvoa 100 jne.

IPL Type	Description	PFD from Literature and Industry	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, saavutettu taso (final frequency)

- Saavutettu riskitaso (final frequency) lasketaan alkutapahtuman taajuuden ja suojauskerrosten PFD-arvojen tulona

$$f_{final} = f_{initiating\ event} \times PFD_{IPL\ 1} \times PFD_{IPL\ 2} \times \ldots$$

- Esim. $f_{final} = 0{,}1*0{,}1*0{,}01 = 1*10^{-4}$

Skenaario | **Kategoria** | **Alkutapahtuma** | **IPL** | **Saavutettu taso** | **Tavoitetaso**

LOPA, final frequency vs. target frequency

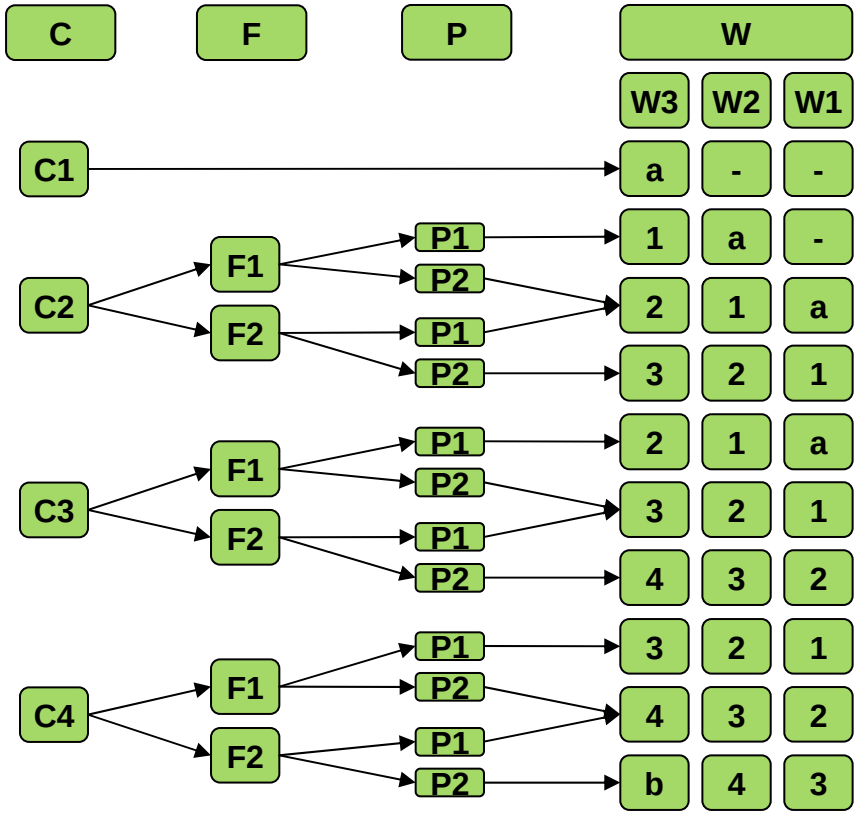
- Skenaarion riskille saavutettua tasoa verrataan aiemmin mainittuun tavoitetasoon, joka perustuu yrityksen omiin ja viranomaisten asettamiin riskikriteereihin.

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

- Saavutetaanko tavoitetaso?
  - **Kyllä**: kyseinen LOPA-skenaario on käsitelty ja voidaan siirtyä analyysissä eteenpäin
  - **Ei**: harkitaan mahdollisia uusia suojauskerroksia (IPL) riskin vähentämiseksi
    - Turva-automaatiotoiminnoilla (SIF) on keskeinen rooli riskinvähennysvajeen täyttäjänä

Osa 3

- Riskigraafi



Riskigraafi

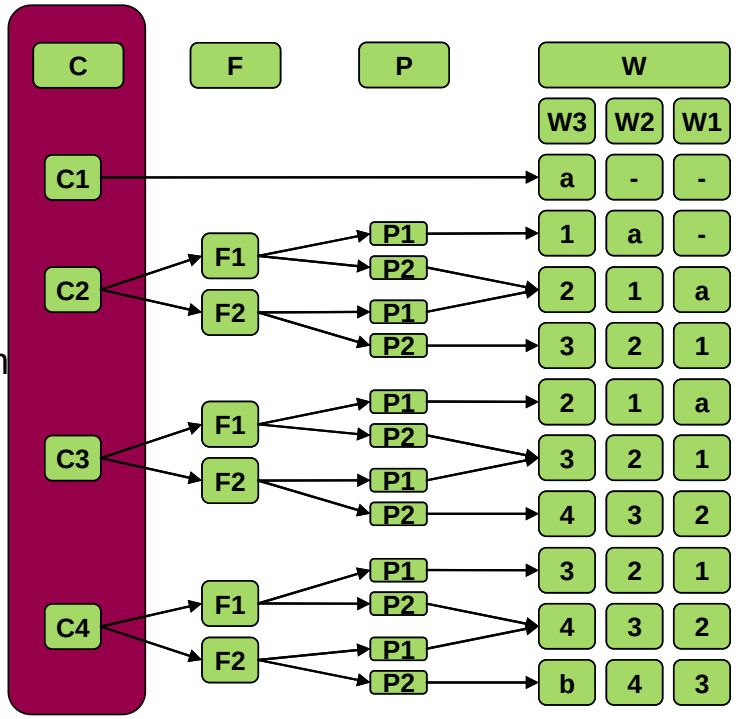
- Standardoitu menetelmä turvatoimintojen turvallisuuden eheystasojen määrittämiseen
- Menetelmänä tapahtumapuun ja riskimatriisin yhdistelmä

- **IEC 61508** Functional safety of electrical/electronic/programmable electronic safety-related systems, **Part 5**: Examples of methods for the determination of safety integrity levels, **Annex D**
- IEC 61511 Functional safety: Safety Instrumented Systems for the process industry sector – Part 3: Guidance for the determination of safety integrity levels, Annex D

C, Seurausmuuttuja

- Vaarasta seurauksena oleva tapahtumien lukumäärä ja vakavuus

C1	<0.01	Lievä vamma
C2	0.01 – 0.1	Vakava pysyvä vamma yhdelle tai useam henkilölle, yksi kuolemantapaus
C3	>0.1 – 1.0	Monta kuolemantapausta
C4	>1.0 - 10	Erittäin monta kuolemantapausta



- C voidaan laskea myös haavoittuvuustekijän V avulla:

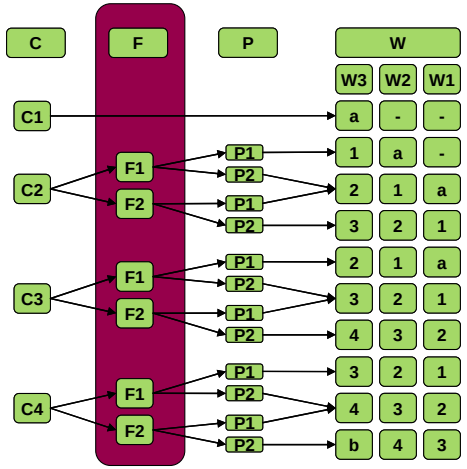
  C = V * henkilömäärä

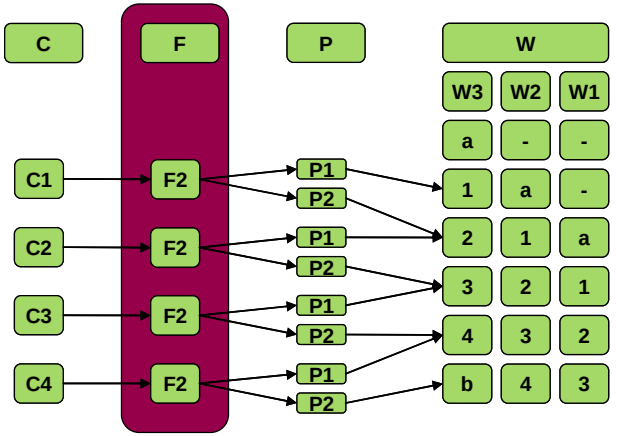
F, Oleskelumuuttuja

- Todennäköisyys että vaaralle alttiilla alueella on ihmisiä
  => osuus ajasta joka alueella oleskellaan
- Poikkeustilanteissa (käynnistys, pysäytys, häiriö…) miehitys on usein suurempi kuin normaalisti

F1 Harvinainen oleskelu, <10% työvuoron pituudesta alueella
F2 Toistuva tai jatkuva oleskelu, ≥10% työvuoron pituudesta

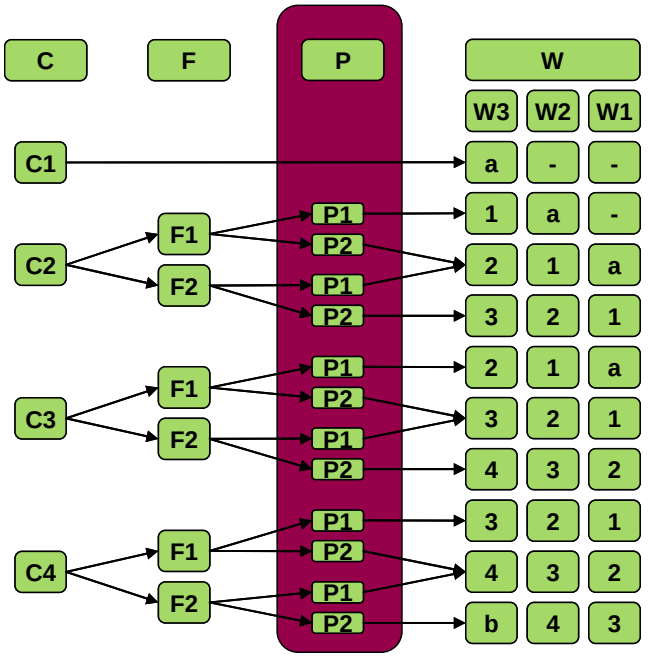
- Ympäristö- ja taloudelliselle riskille valitaan aina F2, koska riskitekijä on jatkuvasti läsnä





P, Vaaran välttämisen todennäköisyys

- P kuvaa mahdollisuutta (todennäköisyyttä) välttää vaarallinen tapahtuma siinä tilanteessa, että suojaustoiminto epäonnistuu .
- P1 valitaan, jos kaikki kolme seuraavaa ehtoa toteutuvat:
  - suojauksen toimimattomuus voidaan havaita, ja
  - on aikaa ja keinot ohjata prosessi manuaalisesti turvalliseen tilaan, ja
  - on poistumistie ja turvalliseen poistumiseen on aikaa
- Muussa tapauksessa valitaan P2

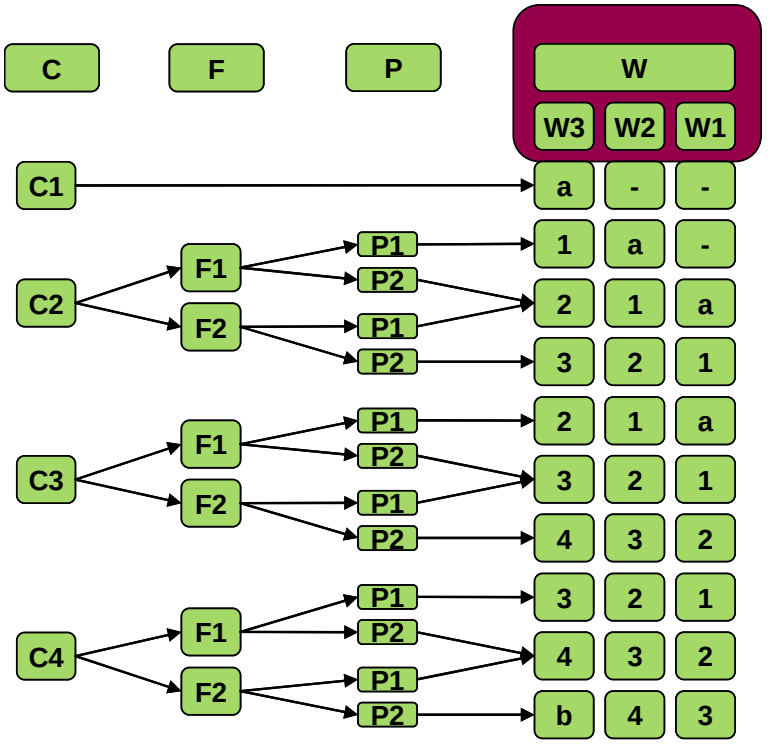


W, Vaarallisen tilanteen esiintymistiheys

- W kuvaa vaaran syntymistodennäköisyyttä, kun automaation avulla tehtävää suojaustoimintoa ei huomioida
- Huomioidaan kaikki vaaraan johtavat vikaantumiset

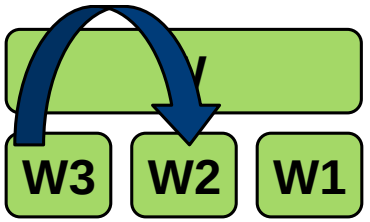
W1: < 0,1 D /vuosi
W2: 0,1 D – D /vuosi
W3: D – 10 D /vuosi

Eli jos **D** = 0,1:
W1: < 1/100 vuosi
W2: 1/100 – 1/10 vuosi
W3: 1/10 – 1 /vuosi



W, Vaarallisen tilanteen esiintymistiheyden lieventäminen

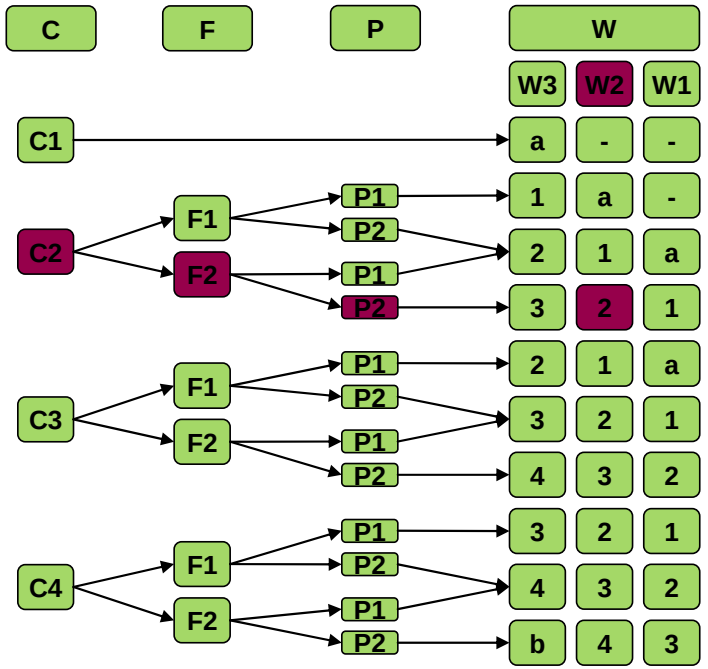
- Tapahtuman todennäköisyyttä voidaan alentaa pienentämällä siihen johtavan tapahtumaketjun alkamistodennäköisyyttä automaation avulla
  - Säätöventtiilin ohjauksen ja asennon välinen eromittaus ja -hälytys
  - Kahden rinnakkaisen mittauksen välinen eromittaus ja -hälytys
- Tapahtuman todennäköisyyttä voidaan alentaa vaaditun suojaustoiminnon tapahduttua myös muiden riskinvähennyskeinojen avulla
  - Varoventtiilit,, murtolevyt ja räjähdysluukut
  - Takaiskuventtiilit
  - Kaasunhaistajat ja palonilmaisimet
  - Pilottipolttimet, liekinvalvojat



Riskigraafin kalibrointi

- Mikä on siedettävä riski tällä kalibroinnilla?
  - W2, vaarallisen tapahtuman esiintymistiheys harvemmin kuin 1/10 vuotta
  - C2, seurauksena kuolemantapaus tai vakavia vammaantumisia
  - Ei lievennystä vaaran välttämistodennäkyisyydelle eikä oleskelulle (P2, F2)

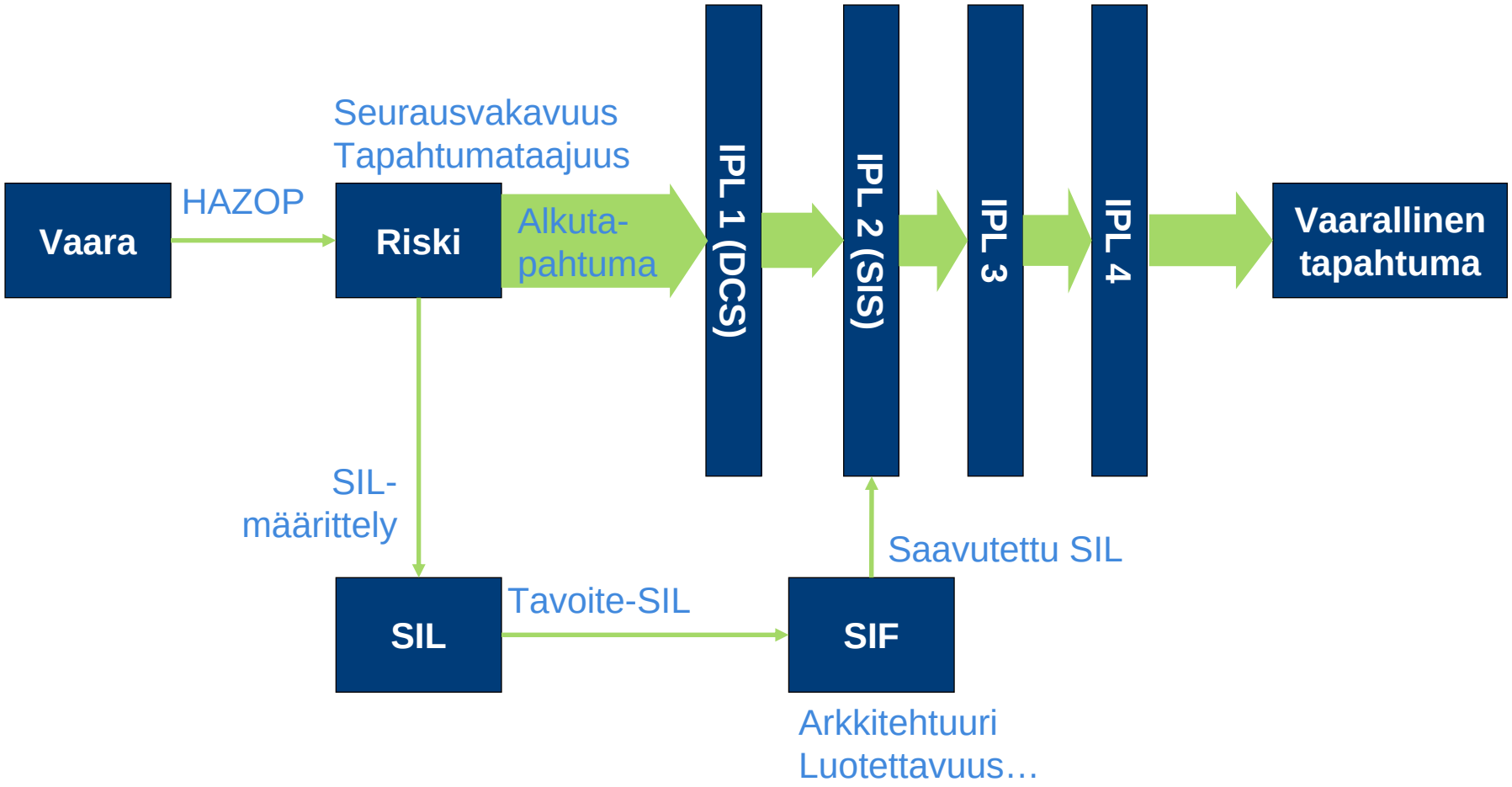
=> SIL3 = 1/1000 turvatoiminto epäonnistuu



Onnistunut SIL-määrittely riskigraafilla

- Vaarallisen tapahtuman tapahtumaketjun kattava kuvaus
- Muiden riskinvähennyskeinojen kuvaus
- W- ja P-muuttujien erottaminen ja oikeanlainen käyttö
- Hyvin tehty kalibrointi
- Riskigraafissä on useita ”vapausasteita” ja se tarvitsee jatkuvaa ohjausta
  - Analyysikohteen riittävä tuntemus
  - Menetelmän antamat tulokset voivat vaihdella työryhmästä toiseen
  - Menetelmästä huolimatta yksittäisillä työryhmän jäsenillä saattaa olla voimakkaita mielipiteitä, jotka heijastuvat analyysin lopputulokseen

Yhteenveto - miten tämän luennon asiat liittyvät toisiinsa?



Sami Matinaho
Fortum, Power Division
POB 100, 00048 FORTUM, Finland

Keilaniementie 1, Espoo
Mobile +358 (0)40 198 2756
sami.matinaho@fortum.com