NESTEJACOBS

Layer of Protection Analysis (LOPA)

ASAF Teemasarja ”Toiminnallinen turvallisuus – uusittu standardisarja IEC 61508”

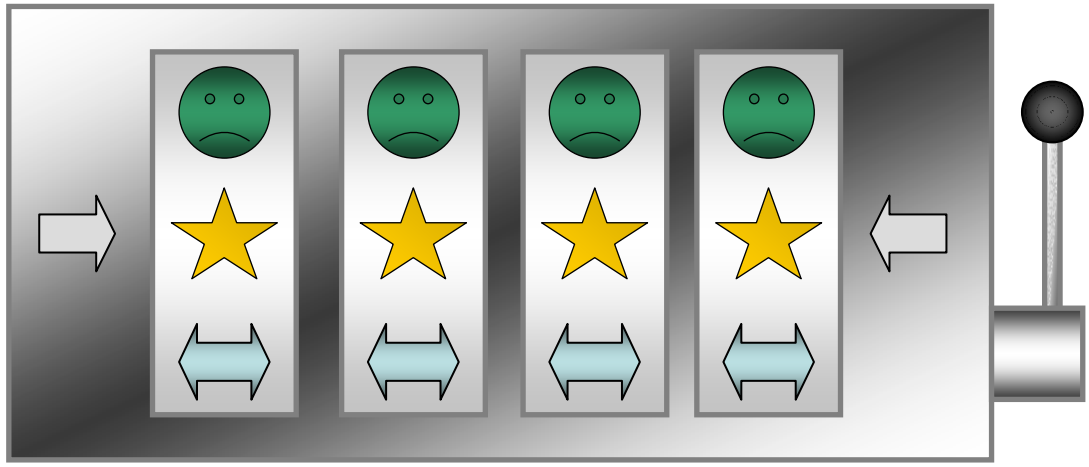
Teemapäivä 1: 11.10.2010

Alkuperäinen materiaali: Sami Matinaho
Esityksen pitäjä: Erkki Turkkila

Riskin arviointi

"Yksikätinen rosvo"

Jokaisella kehällä on 10 erilaista kuviota. Jos saat voittolinjalle neljä samaa kuviota, voitat 100 000 €. Peli on ilmainen, mutta neljä hapannaamaa voittolinjalla merkitsee, että joudut itse maksamaan 100 000 €. Kuinka monta kertaa uskaltaisit pelata tällaista peliä? Entä jos neljä hapannaamaa voittolinjalla merkitsisi ihmishengen menetystä?



Riskin arviointi

Mikä on riski?

- Riski = C x F
  - C = vaarallisen tapahtuman seurauksen vakavuus
  - F = vaarallisen tapahtuman todennäköisyys

Mikä on vaaran ja riskin ero?

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

LOPA, Layer Of Protection Analysis

Yksinkertaistettu kvantitatiivinen riskinarviointimenetelmä

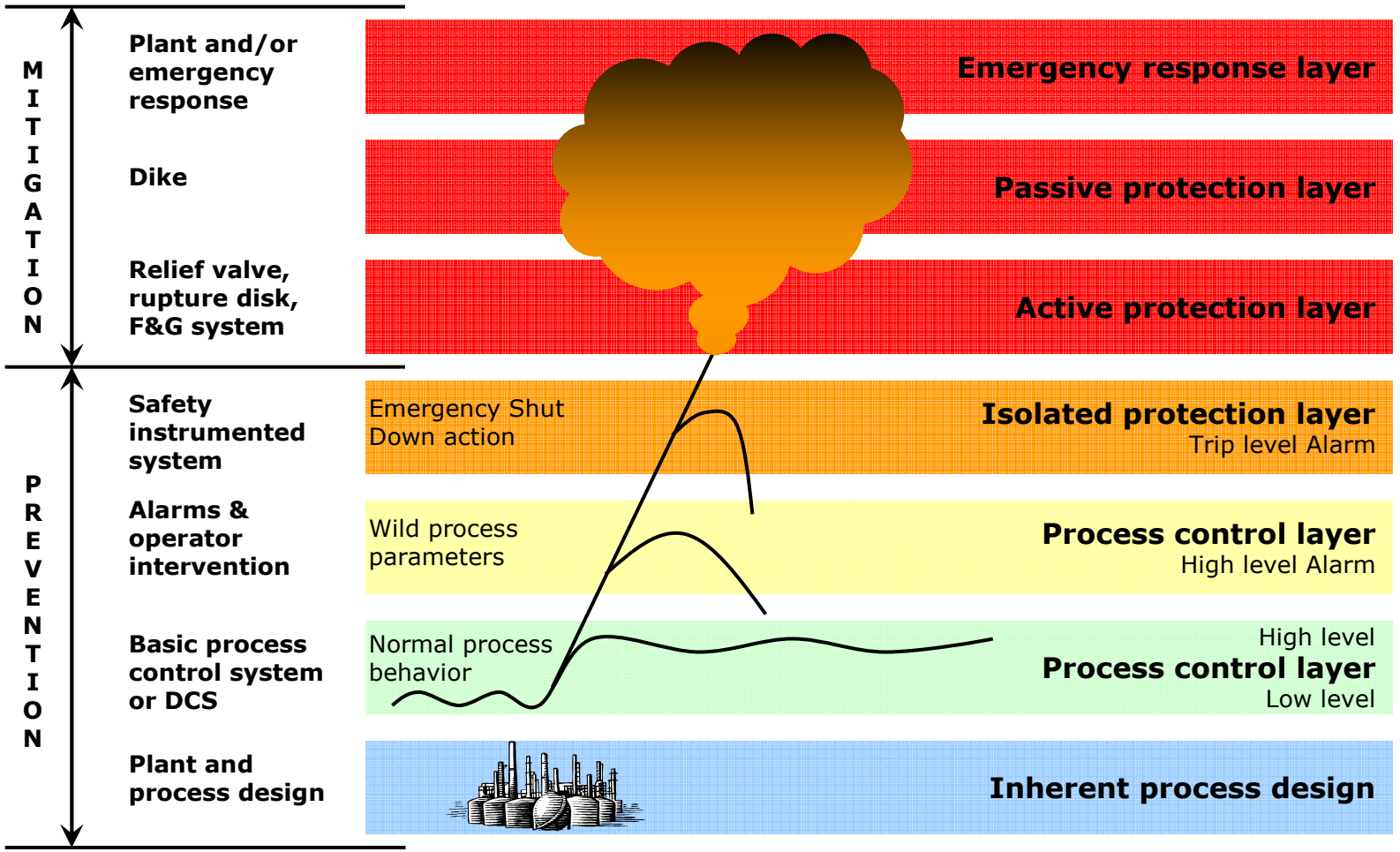
1993, CCPS: Guidelines for Safe Automation of Chemical Processes, "risk-based SIS integrity level method", tämän jälkeen menetelmää on kehitetty eri yrityksissä

2001, CCPS: Layer of Protection Analysis — Simplified Process Risk Assesment

2010, EN 61508-5, Annex F

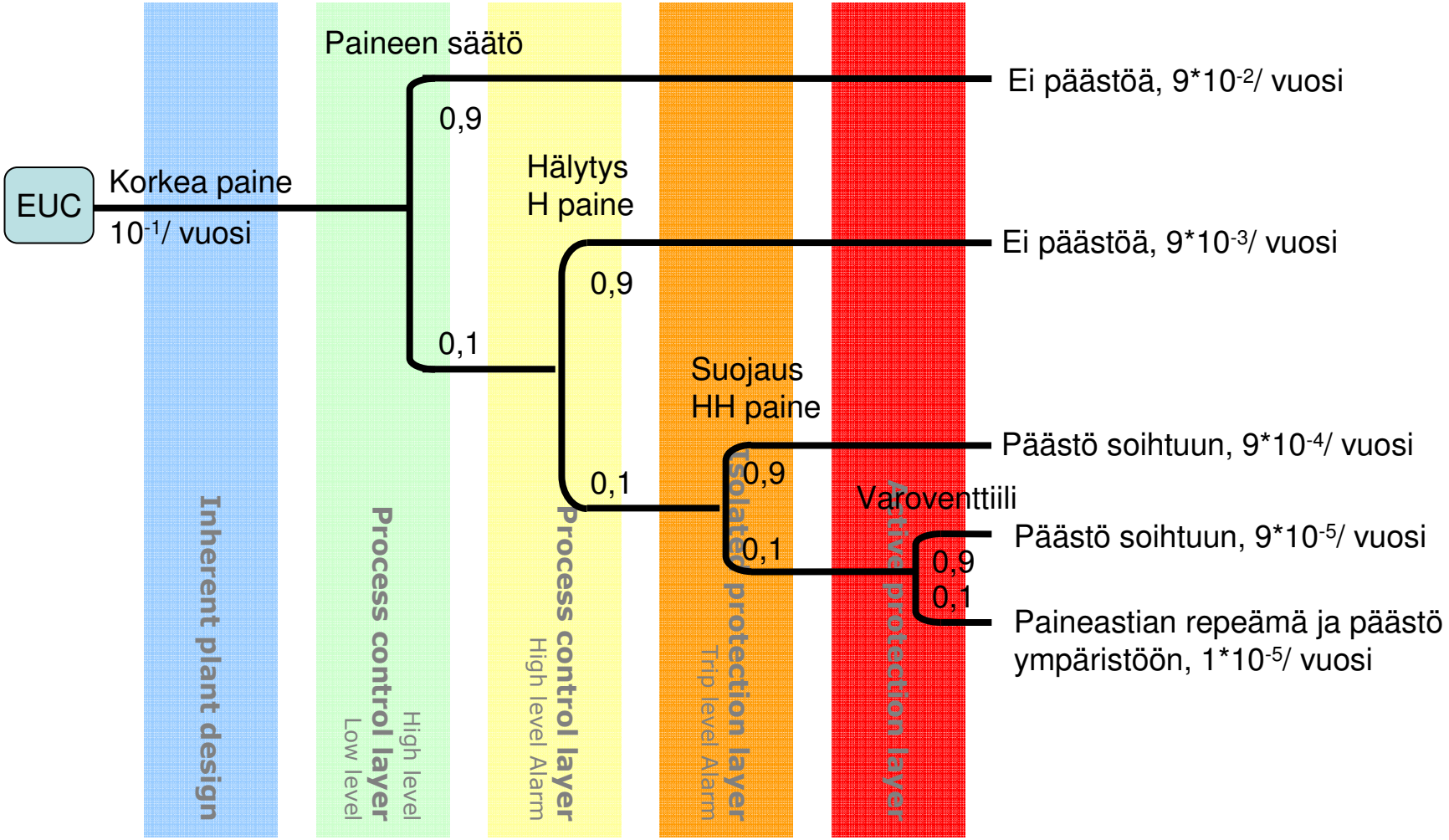
LOPA vaatii käyttäjäkohtaisen käyttöönottoprosessin ja kalibroinnin!

LOPA, Layers of protection -idea



NESTEJACOBS

LOPA, idea tapahtumapuun muodossa



NESTEJACOBS

LOPA, tavoitetaso (tolerable frequency)

Tavoitetaso ($f_{tolerable}$) 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.

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

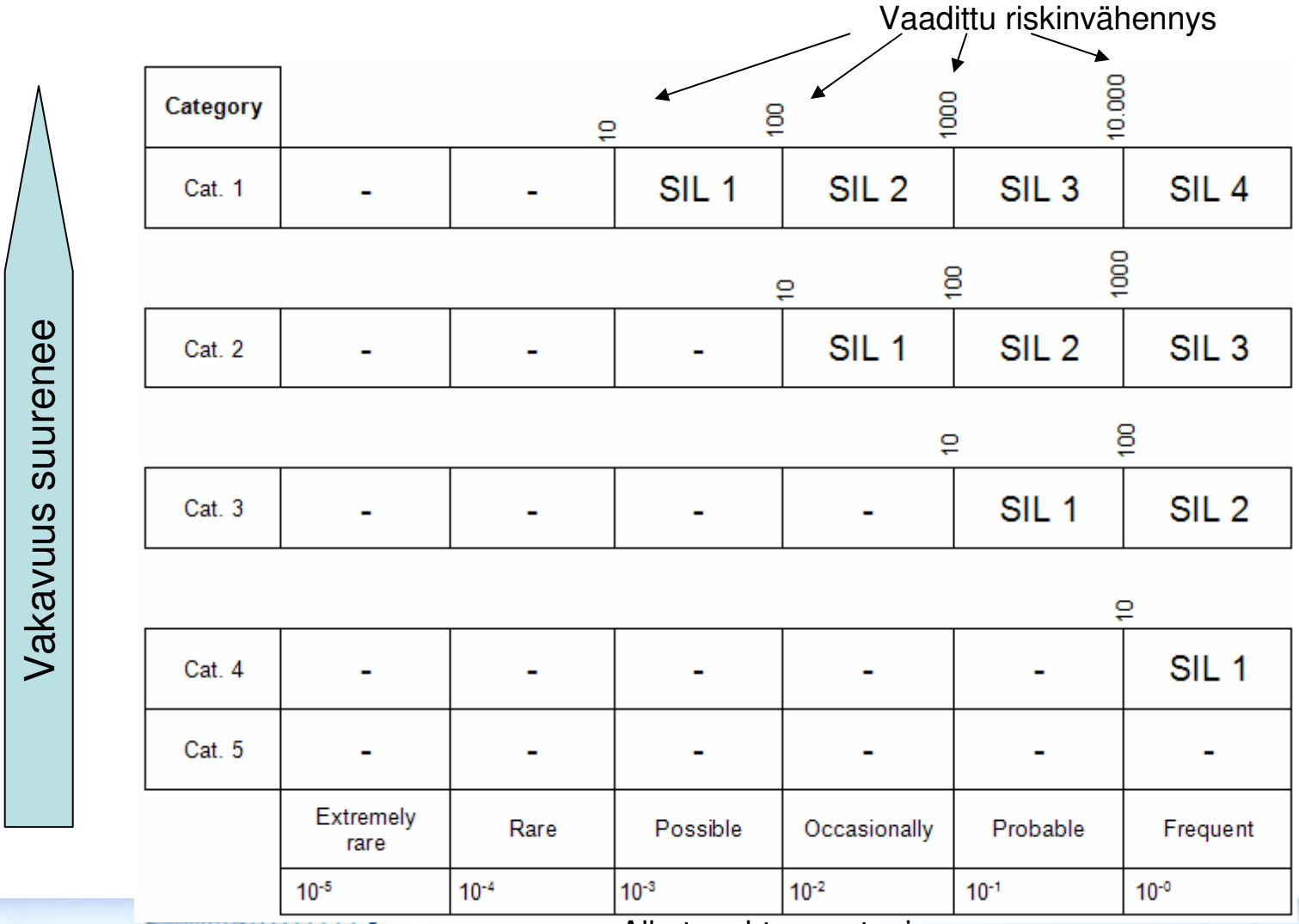
Riskiluokat

- 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-riskimatriisi, case "Yritys"



NESTEJACOBS

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 poikkemaan
- 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

- aihettajana korroosio, kuluminen, suunnitteluvirhe, rakennusvirhe tms.
- joku muu lähestymistapa suositeltavampi:
  - Lainsäädäntö, prosessin lisensorin tai laitetoimittajan vaatimukset, standardit,, konedirektiivi

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 => $f_{inititing\ event}$ = 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 $f_{inititing\ event}$ = 0,1/vuosi

LOPA, enabling event

Jos skenaario on mahdollinen vain tietyissä olosuhteissa, esim. talvella, panosprosessin tietyssä vaiheessa, jäähdytyksen ollessa käytössä jne, niin tämä voidaan huomioida enabling eventin avulla, joka on todennäköisyys (eikä taajuus kuten alkutapahtuma) ja siten aina arvoltaan välillä 0...1

- Esim. Skenaarion alkutapahtumana on jäähdytysveden katko $f_{inititing\ event}$ = 0,1, mutta prosessissa tarvitaan jäähdytysvettä vain kesä-elokuussa, jolloin enabling event = 3/12 = 0,25 ja korjattu $f_{inititing\ event}$ = 0,25*0,1= 0,025. Enabling eventin avulla $f_{inititing\ event}$ pienenee 1/4-osaan, jolloin skenaarion tavoitetaso on neljä kertaa alkuperäistä lähempänä, minkä ansiosta saatetaan välttyä jonkin riskinvähennyskeinon, esim. uuden suojaustoiminnon lisäämiseltä.

LOPA, suojauskerros (IPL)

LOPA-menetelmässä keinoja vähentää riskiä kutsutaan suojauskerroksiksi (IPL, **independent** protection layer).

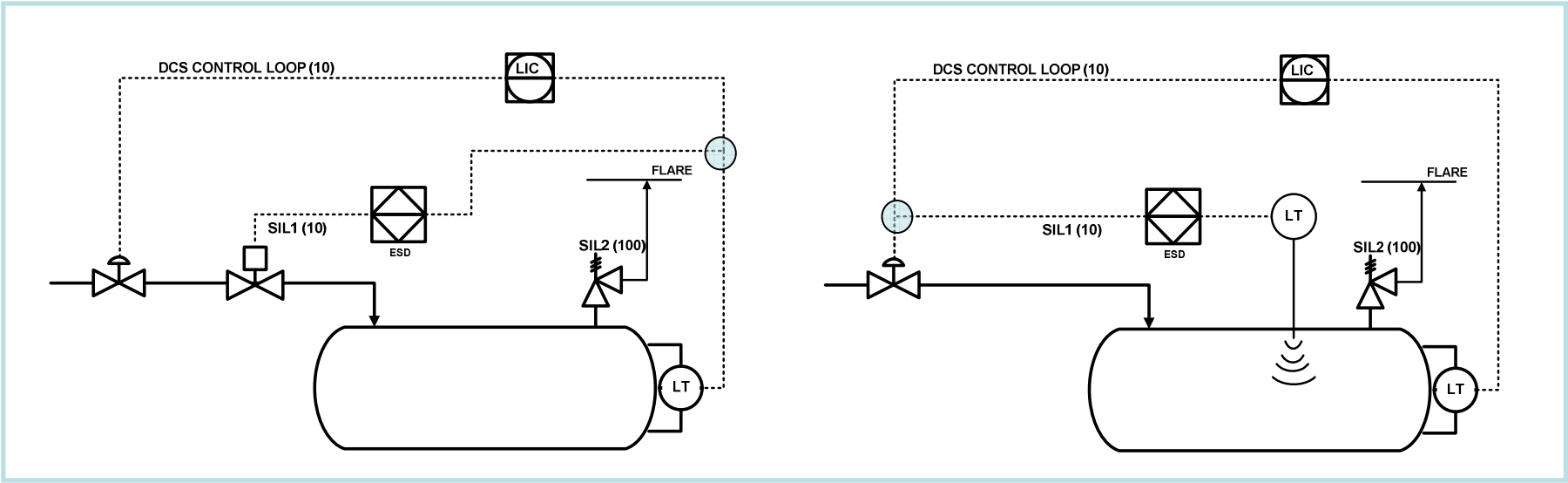
Skenaarion liittyvät IPL:t tunnistetaan, kirjataan ylös ja jokaiselle kerrokselle määritellään riskinvähennyskerroin (RRF tai PFD).

- IPL:n kriteerit:
  - vähentää skenaarion riskiä vähintään kertoimella 10 (RRF > 10)
  - spesifisyys: IPL on suunniteltu estämään tai lieventämään tiettyä vaarallista tapahtumaa
  - **riippumattomuus**: riippumaton skenaarion alkutapahtumasta ja muista samassa skenaariossa käytetyistä IPL:stä (esim. yhteisviat)
  - luotettavuus: IPL tekee sen, mitä sen on tarkoituskin tehdä
  - jäljitettävyys: IPL:n toimivuus pitää voida varmentaa (dokumentointi, tarkastus, testaus...)

Skenaario	Kategoria	Alkutapahtuma	IPL	Saavutettu taso	Tavoitetaso

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 of failure 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.

Skenaario	Kategoria	Alkutapahtuma	IPL	Saavutettu taso	Tavoitetaso

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 mahdollisen enabling event -muuttujan) ja suojauskerrosten PFD-arvojen tulona

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

Esim. $f_{final} = 0{,}1*0{,}25*0{,}1*0{,}01 = 2{,}5*10^{-5}$

Skenaario	Kategoria	Alkutapahtuma	IPL	Saavutettu taso	Tavoitetaso

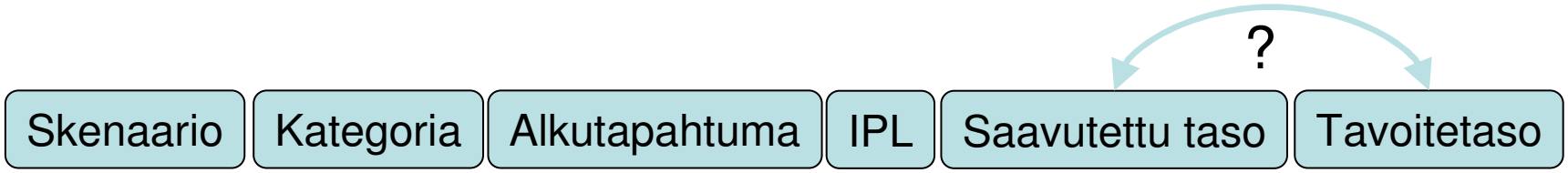
LOPA, final frequency vs. target frequency

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

$$f_{final} \leq f_{tolerable}$$

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



Lisätietoja tämän luennon aiheista

HAZOP

- CCPS: Guidelines for Hazard Evaluation Procedures, with Worked Examples, 2nd Edition, 1992
- VTT: riskianalyysit.vtt.fi

LOPA

- CCPS: Layer of Protection Analysis — Simplified Process Risk Assesment, 2001
- IEC 61511-3, Annex F (informative), Layer of Protection Analysis (LOPA)

Excellency in engineering

NESTEJACOBS

Kysymykset ja kommentit:

Sami Matinaho
Functional Safety Engineer
Neste Jacobs Oy
PL 146, 02101 Espoo
Mobile: +358 (0)50 458 9766
e-mail: sami.matinaho@nestejacobs.com