Use of LOPA in the safety lifecycle, "the BP way"

Arvid Nilsen, automasjonsingeniør.EST – BP Norge
CASIS ansvarlig BP Norge
ESRA seminar "SIL I drift"29.januar 2014

Introduksjon

- Dette er ikke et LOPA-kurs
- LOPA i «the SIS Safety Lifecycle»
- LOP – hva er det? (LOP=Layer Of Protection)
- LOPA fordeler og utfordringer
- LOPA verktøy – TRAC

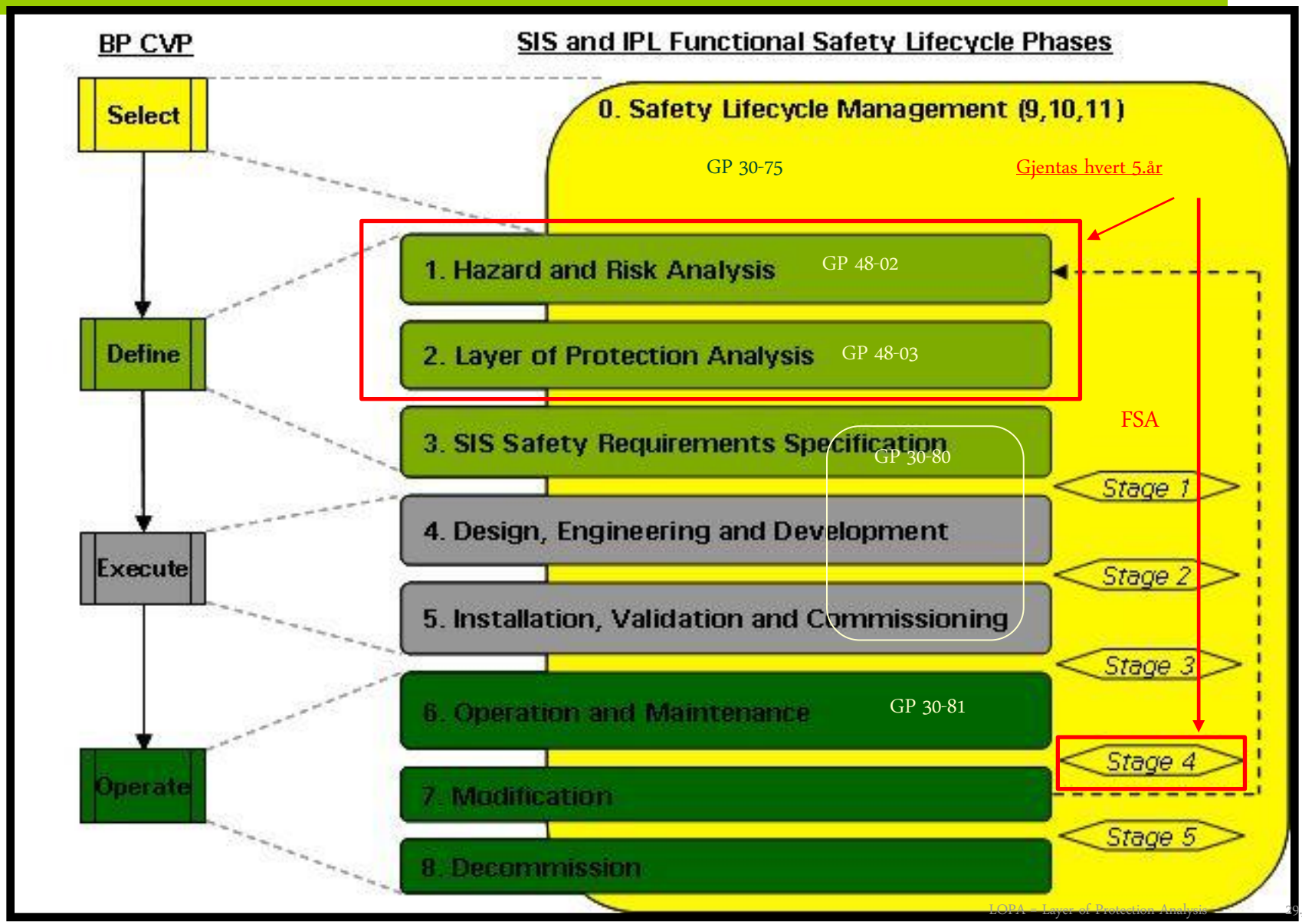
BP og "*Management of the SIS Safety Lifecycle*"

- Functional Safety Management (GN 30-751 SIS SLP)
  - Organisasjon
  - Planlegging
  - Kompetanse
  - FSA (Functional Safety Assessment) og verifikasjon
  - Fare og riskovurdering (Hazop)
  - Allokering av sikkerhetsfunksjoner til beskyttelseslag(LOPA)
  - SRS (Safety Requirement Specification)
  - SIS design og Engineering (SIS=Safety Instrumented System)
  - SIS Installering og Commissioning
  - SIS Operasjon and vedlikehold
  - SIS Modifikasjon
  - SIS Decommissioning

Hvordan etterleve det som besluttes her?

LOPA = Layer of Protection Analysis

SIS Safety Lifecycle



Fra Hazop til LOPA

- LOPA utføres på definerte konsekvens nivåer fra Hazop (dvs uten safeguards)
- LOPA er ikke en metode for å identifisere farer
- LOPA skal ikke analysere eskalerende hendelser
- LOPA brukes ikke til å analysere risiko ved rømning og evakuering
- LOPA er en semi-kvantitativ metode for å definere påkrevd riskoreduksjon for et identifisert konsekvensnivå
- LOPA kan brukes opp til og med SIL2 (SIL3 vil kreve mer omfattende analyser)
- BP bruker LOPA etter nøye definerte regler og begrensninger, og funksjonene som vurderes kan best sammenlignes med SIF'er som OLF-070 kaller for «lokale sikkerhetsfunksjoner», eller prosess-sikkerhets-funksjoner

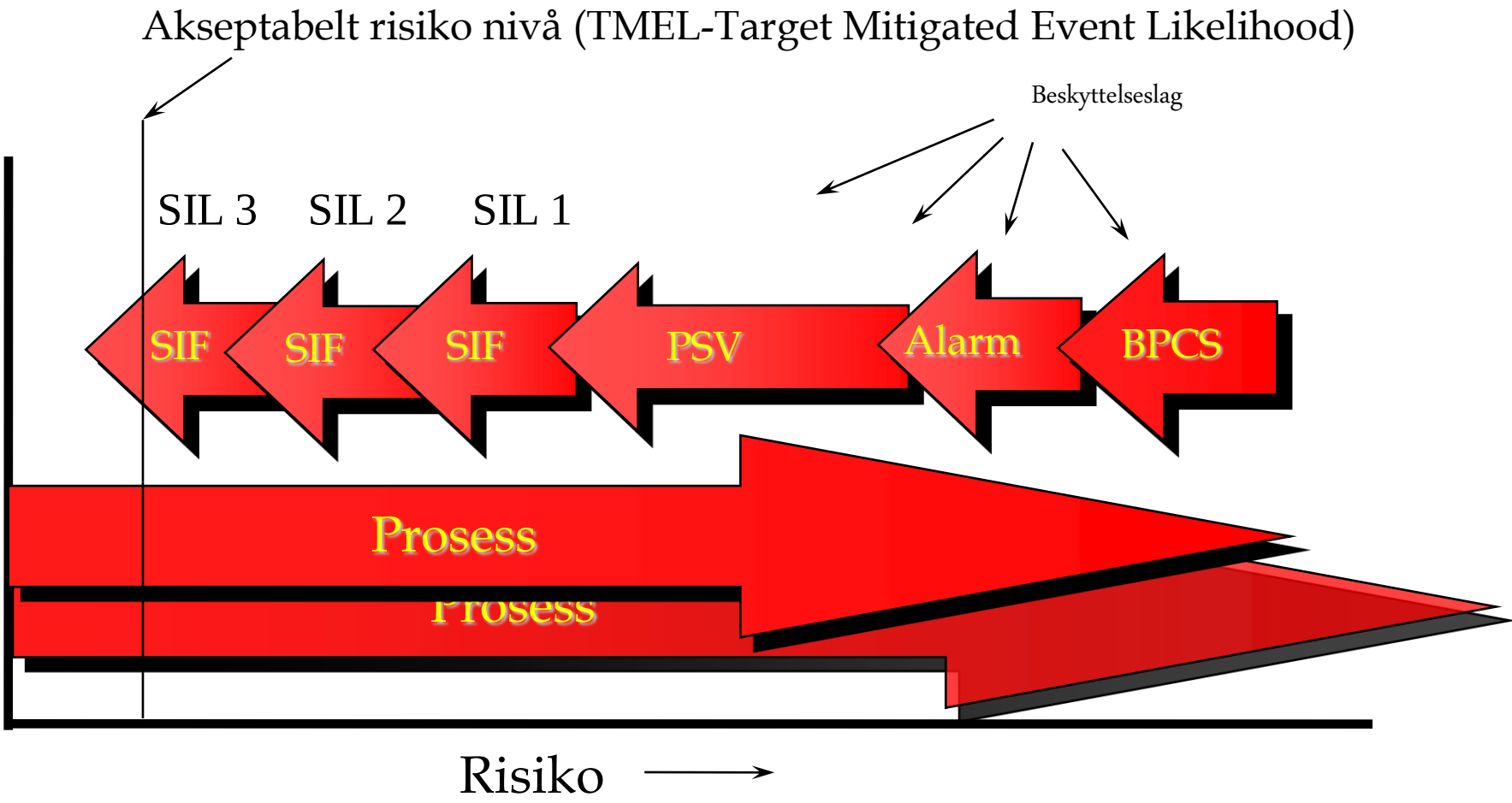
BP og akseptabel risiko - GDP 3.1-0001 Risiko Matrise

	Likelihood of Risk Event							
	1	2	3	4	5	6	7	8
Severity Level	A similar event has not yet occurred in our industry and would only be a remote possibility	A similar event has not yet occurred in our industry	Similar event has occurred somewhere in our industry	Similar event has occurred somewhere within the BP Group	Similar event has occurred, or is likely to occur, within the lifetime of 10 similar facilities	Likely to occur once or twice in the facili lifetime	Event likely to	Common
A	8	9	10	11	12	13		
B	7	8	9	10	11	12		
C	6				10	11	12	13
D	5	6	7	8	9	10	11	12
E	4	5	6	7	8	9	10	11
F	3	4	5	6	7	8	9	10
G	2	3	4	5	6	7	8	9
H	1	2	3	4	5	6	7	8

Scenarier som går til LOPA

Det finnes noen scenarier som kan inkludere C til LOPA for visse hendelser dersom visse forhold eller forutsetninger er oppfylt (husk at BP definerer SIL, EIL og CIL)

Reduksjon av risiko ved å legge på beskyttelseslag - prinsippskisse



- Iboende prosess risiko er ikke den samme for alle prosesser eller systemer
  - Eks.drikkevann vs. hydrokarbonsystem

Hva er et beskyttelseslag - LOP?

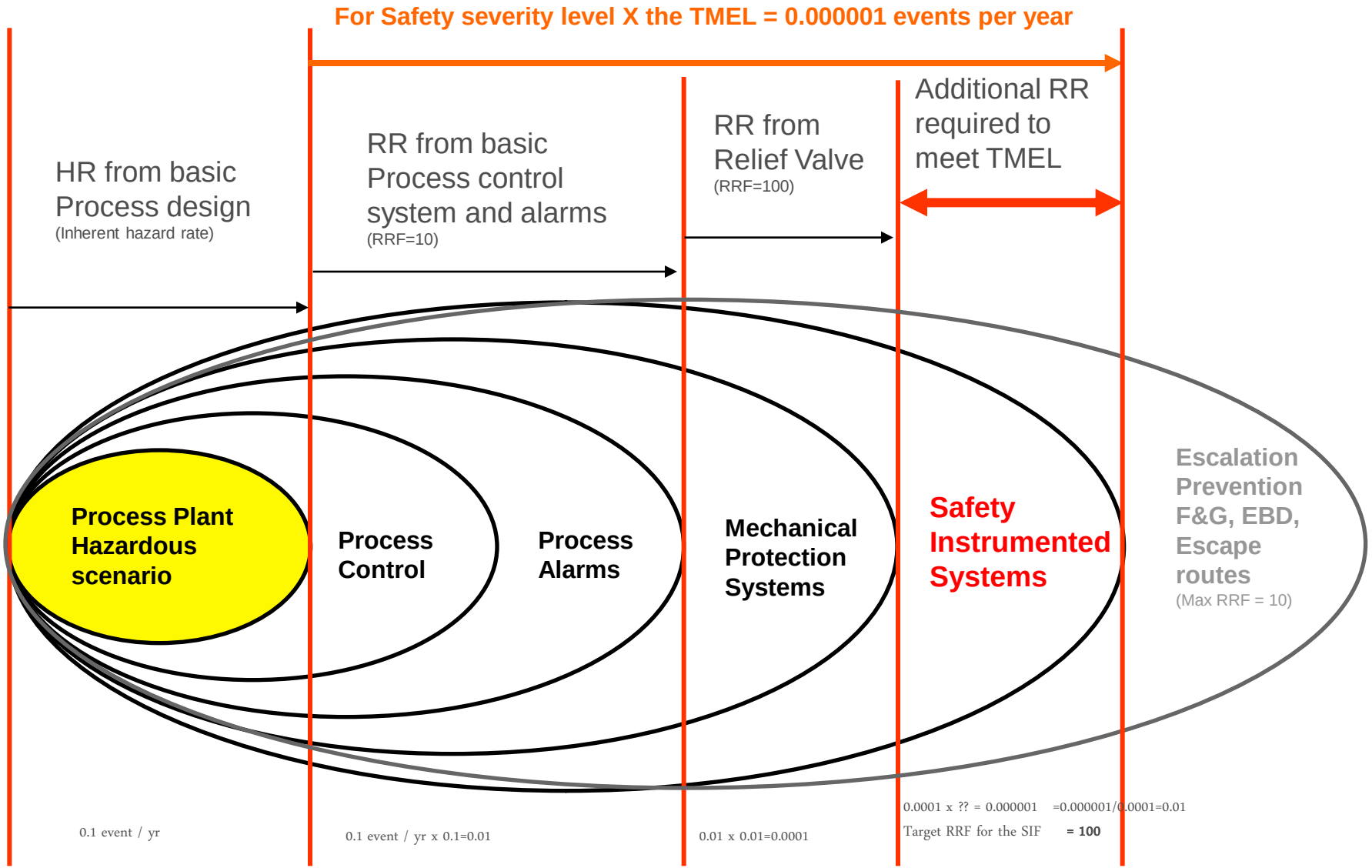
Et beskyttelseslag skal;

- Definert selvstendighet
- Definert pålitelighet
- Redusere risiko
- Behandles som et sikkerhetssystem/funksjon

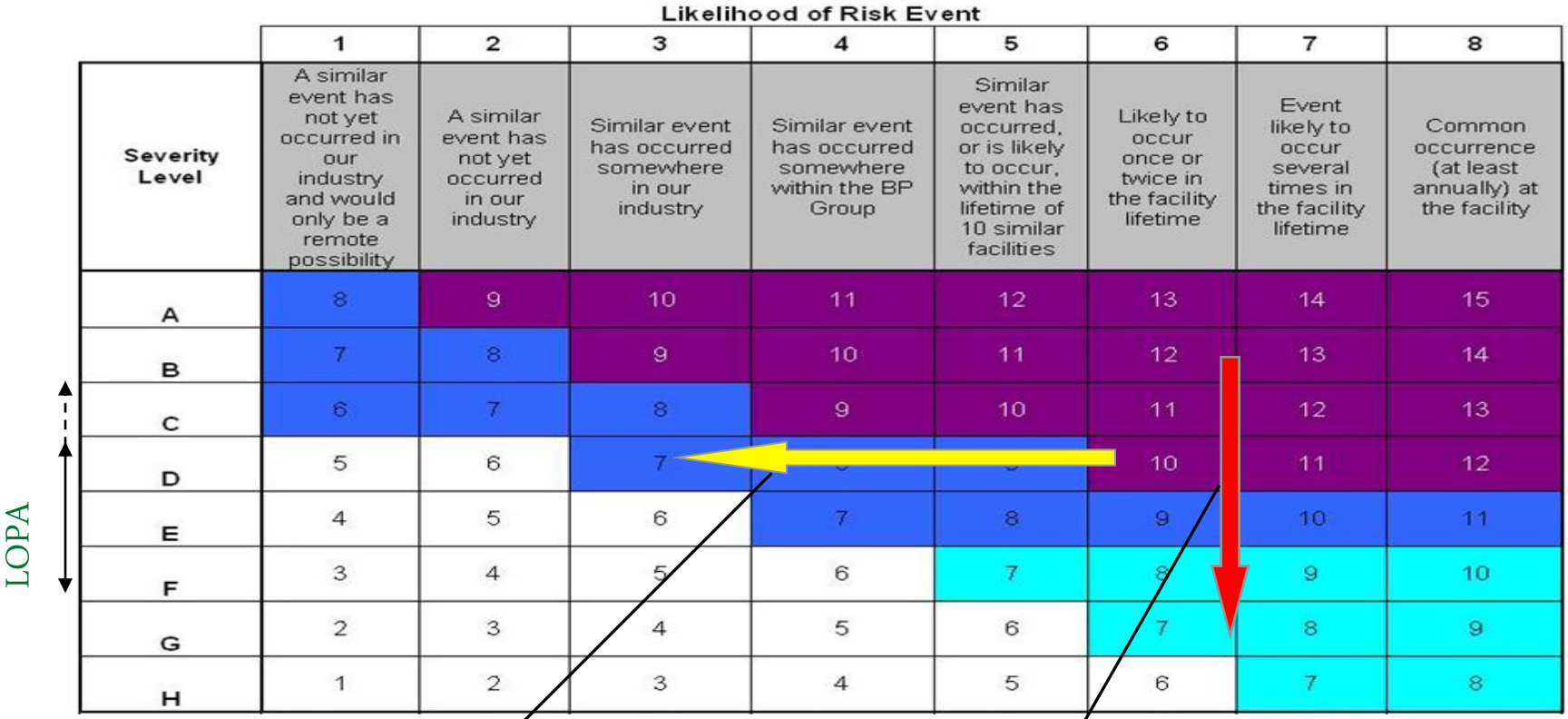
Typiske LOP:

- Alarm
- Kontrollsløyfe/funksjon
- Sikkerhetsventil
- (Tennsannsynlighet)
- (Occupancy)

Vist på en annen måte – risikoreduksjon I praksis, eksempel



BP og akseptabel risiko - GDP 3.1-0001 Risiko Matrise



Protection – Redusere frekvens v.hj.a LOPA

Mitigation – begrense konsekvens

Fra GP 48-03 - LOPA

- Definert minimum LOPA team
- Kompetanse for LOPA personell
- Hvilke beskyttelseslag er lovlige
- Regler om uavhengighet mellom beskyttelseslag
- Regler om maks tillatt risikoreduksjon for ulike typer beskyttelseslag
- Responstid
- Operasjonell prosedyrebruk
- Feilrater/menneskelig feil
- Tennsannsynlighet
- Beregning av eksponering/occupancy/time at risk
- Feilrater utstyr (GN 30-802, Equipment Failure Rate Data)
- Krav til skjerming av beskyttelseslag slik at de ikke kan endres uten endringskontroll ihht MoC-prosedyrer

LOPA team

- LOPA fasilitator
  - Kompetansevurdert og forhåndsgodkjent
  - Fasilitator holder kurs for arbeidsgruppen
- Andre deltagere, typisk
  - Sekretær
  - Sikkerhetsingeniør
  - Prosessingeniør
  - Produksjonsrepresentant
  - Instrumentingeniør/tekniker
  - Andre disipliner som elektro og mekanisk etter behov

NB – Viktig:
Sluttbrukere involveres i risikovurderingene

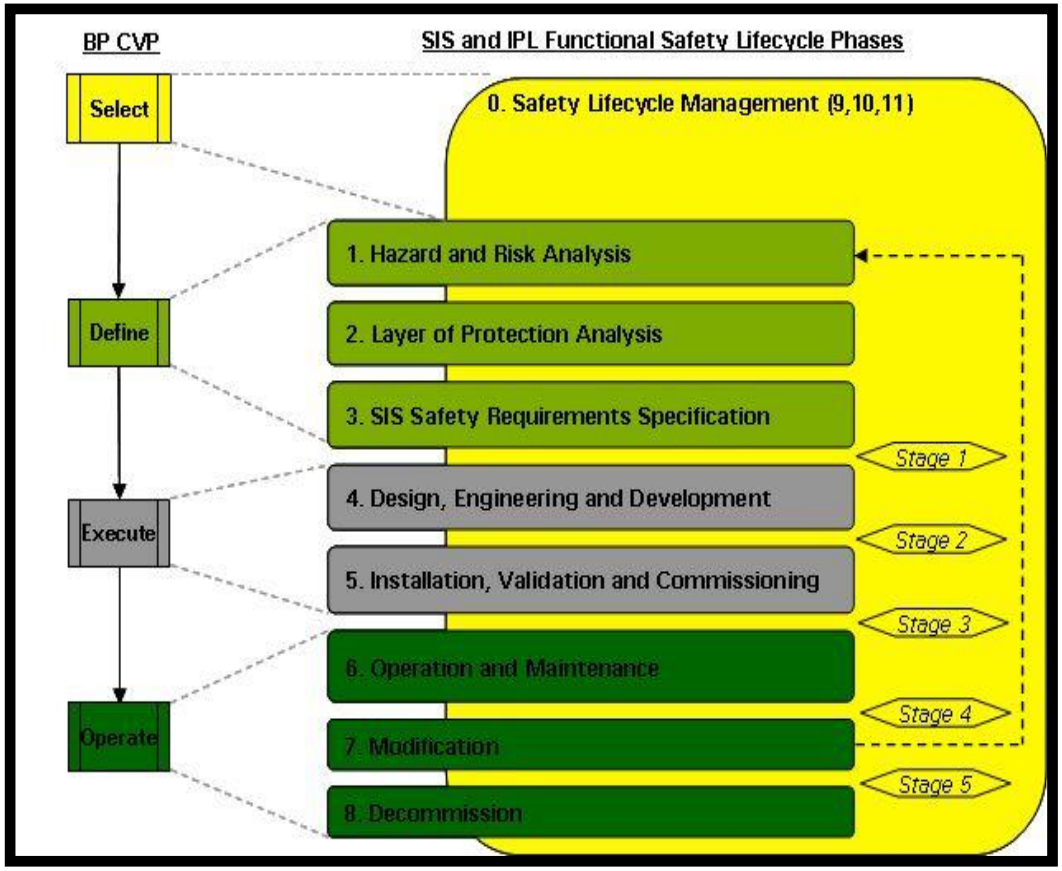
Fordeler med LOPA

- Bedre risikoforståelse
- Egnet for «screening»
- T.o.m. SIL2
- Riktig IL nivå definert for funksjonen sett i forhold til omkringliggende beskyttelsesfunksjoner – hvordan henger dette sammen? Ikke alltid at et strengt SIF-krav er løsningen
- PFD-verdi, ikke IL-nivå
- Håndterer multiple «causes»/årsaker
- Stimulerer tenkning mot «Inherent Safe Design»
- Dokumenterer vurderinger og forutsetninger, som i senere tid kan verifiseres og etterprøves
- LOPA verktøy er dynamisk, kan enkelt justeres
- Gir bilde av forventet demandrate
- Involverer sluttbrukere i risiko-vurderingen, verdifull informasjon kan tas med i operasjonelle prosedyrer
- Hjelper til å se sammenhenger mellom risikonivå og utkobling-/overbroings-tid
- Underlag for utarbeidelse av kompenserende tiltak ved overbroing (BP:SORA=Safety Override Risk Assessment)
- Ikke nødvendigvis mer tidskrevende

Utfordringer – bruk av LOPA (og generelt)

- Risikoreduksjon fra non-safety beskyttelseslag medfører at utstyret må behandles som et sikkerhetssystem (for eksempel SRA og BPCS)
- Krever tilgang til detaljert informasjon og avhengig av et «fast» design
- Avhengig av erfarent og dedikert personell
- Kredittagning for kontrollsløyfe krever at den skal stå i auto
- Visualisering av instrumenterte beskyttelseslag på HMI
- Verifikasjon av LOPA forutsetninger (stemmer LOPA tallene med virkeligheten?)
- Innsamling av feilrater krever ryddige testrutiner og godt definerte feilmodus
- Demandrate-målinger
- Holde LOPA dokumentasjon oppdatert gjennom drift og modifikasjon
- Opplæring og vedlikeholde kompetansen

Aktiviteter etter LOPA



Etablere eller revidere

- SRS (Safety Requirements Specification)
- IPL register (Independent Protective Layer Register)
- Testprosedyrer
- HMI
- SORA's (Safety Override Risk Assessment's, inkludert definisjon av max tillatt overbroingstid)
- Applikasjoner
- For prosjekter og modifikasjoner: Sørge for at commissioning tester de riktige tingene
- Competency is key

LOPA - noen anbefalinger

- Forankres i en SIS safety lifecycle plan
- LOPA regler definert på forhånd
- LOPA bør utføres tidlig nok i prosjektet slik at endring av design er mulig
- I prosjekt bør noen ganger LOPA gjennomføres 2 ganger
- Søke å ha færrest mulig beskyttelseslag?
- Bruk et godt LOPA verktøy (kombinert hazop og LOPA verktøy er fordelaktig)
- Samme personell i hazop og LOPA)

LOPA verktøy - TRAC

Input Test Interval	2wk	1m	2m	3m	4m	6m	1y	18m	2y	3y	4y
4y	~~.1347~~	~~.1362~~	~~.1390~~	~~.1418~~	~~.1445~~	~~.1501~~	~~.1668~~	~~.1834~~	~~.2001~~	~~.2334~~	~~.2668~~
3y	~~.1014~~	~~.1029~~	~~.1057~~	~~.1084~~	~~.1112~~	~~.1168~~	~~.1334~~	~~.1501~~	~~.1668~~	~~.2001~~	~~.2334~~
2y	.0680	.0695	.0723	.0751	.0779	.0834	.1001	.1168	.1334	.1668	~~.2001~~
18m	.0514	.0529	.0557	.0584	.0612	.0668	.0834	.1001	.1168	.1501	~~.1834~~
1y	.0347	.0362	.0390	.0418	.0445	.0501	.0668	.0834	.1001	.1334	~~.1668~~
6m	.0180	.0195	.0223	.0251	.0279	.0334	.0501	.0668	.0834	.1168	~~.1501~~
4m	.0125	.0140	.0168	.0195	.0223	.0279	.0445	.0612	.0779	.1112	~~.1445~~
3m	.0097	.0112	.0140	.0168	.0195	.0251	.0418	.0584	.0751	.1084	~~.1418~~
2m	.0069	.0084	.0112	.0140	.0168	.0223	.0390	.0557	.0723	.1057	~~.1390~~
1m	.0042	.0057	.0084	.0112	.0140	.0195	.0362	.0529	.0695	.1029	~~.1362~~
2wk	.0027	.0042	.0069	.0097	.0125	.0180	.0347	.0514	.0680	.1014	~~.1347~~

OLF-070, kap 7.7 og demand rate (fra «deviations from minimum SIL requirements»

- a high demand rate[1] on a particular safety function is foreseen or experienced. Identification of a high demand rate may be done in the design phase, e.g. during HAZOP, but would normally result from operational experience (in which case it according to ISO terms, will actually represent a non-conformity, ref. section 4.2). A very high demand rate on a safety function would often represent an operational problem with respect to production availability and as such initiate alternative solutions and/or re-design.
- a high *accumulated* demand rate is foreseen for a particular safety function, e.g. due to a very large number of risers, in which case a higher SIL requirement for the function "isolation of riser" could result.

• a special consideration related to the *consequences* of the associated hazard, e.g. due to concept specific

[1] No specific demand rates form the basis for the minimum SIL requirements in Table 7.1. However, in Appendix A some "typical" demand rates for an "average" operation are given and can be used as a basis unless more project s
5
t

A.2.2 Demand rates

It should be noted that this revision of the document does not include average demand rates. This has been deleted due to several reasons:

- The demand rates are highly installation specific and it is therefore difficult to give generic values;
- Since this document gives standard SIL requirements, the demand rates are not applied when determining the SIL requirements (see chapter 7 in main document);

In order to enable follow-up during operation, it will however, be required to estimate the demand rates as part of the SRS work.

Spørsmål?