

# Skog 2011 SIL Safety Integrity Level





## Vad betyder SIL?

- Safety Integrity Level  
Delas upp i olika nivå från SIL 1 till SIL 4, där SIL 1 är den lägsta säkerhetsnivån och SIL 4 är den högsta
- Tillämpas i huvudsak för att fastställa att elektriska, elektroniska, elektroniska programmerbara säkerhetssystem ger en tillräcklig säkerhet

## huvudstandarden

- IEC61508 är en generell standard för elektriska, elektroniska och programmerbara komponenter och system i säkerhetsapplikationer.
- För de komponenter som är typgodkända enligt IEC 61508 anger tillverkaren den högsta SIL-nivå som komponenten kan upprätthålla och villkoren för att den ska göra det.

## Varför SIL?

- BPCS- Basic Process Control System, DCS- Distributed Control System
  - Systemet består av olika kretsar som har som uppgift att upprätthålla en variabel i processen inom ett visst intervall. Dvs det är processens styrsystem.
  - Består av sensor/sensorer, logik (PLC) och manöverdon

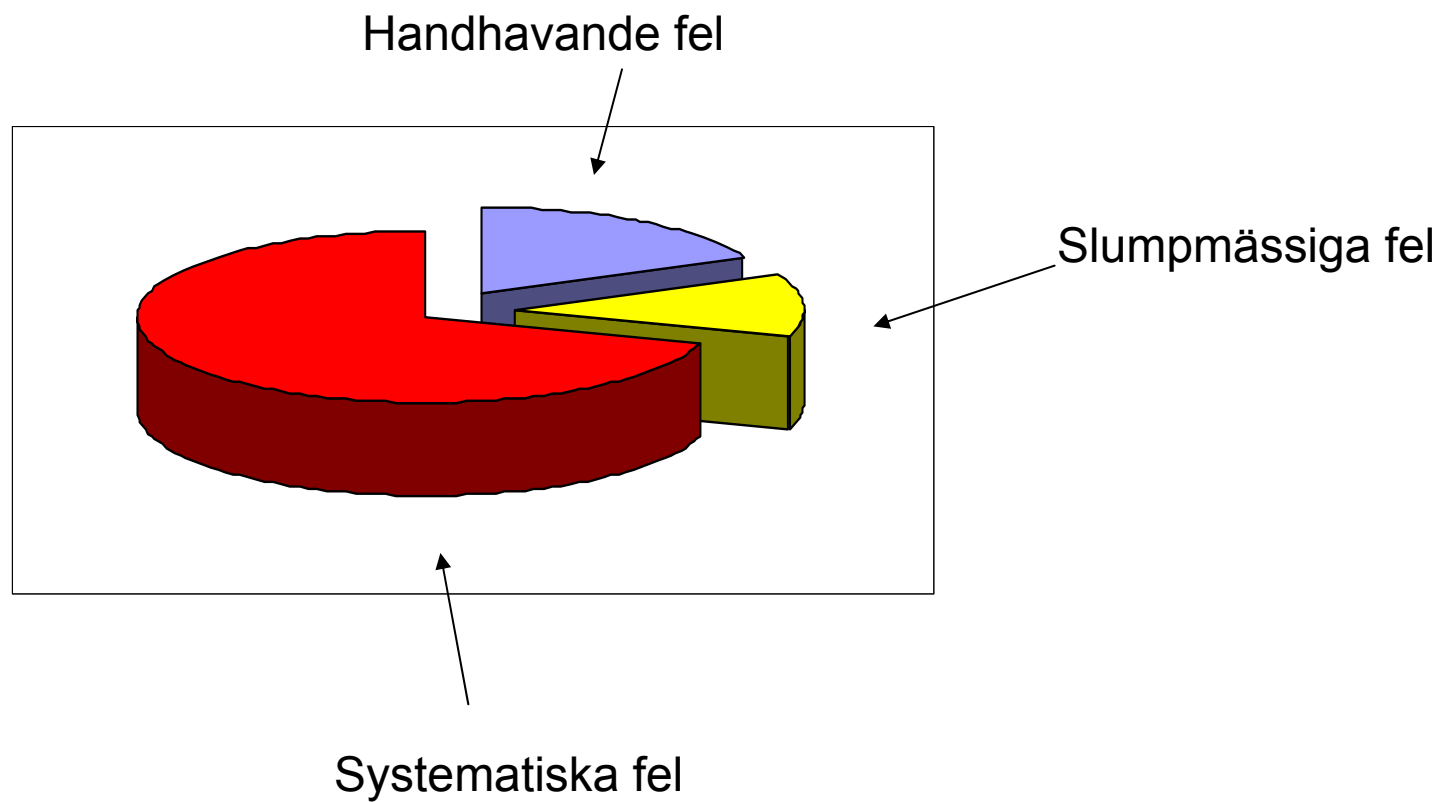
- SIS- Safety Instrumented System

SIS består SIF: Safety Instrumented Function som har en funktion att övervaka en processvariabel och ge signal när det krävs, dvs när en viss gräns har uppnåtts.

SIF består av sensor, logik (PLC) och manöverdon



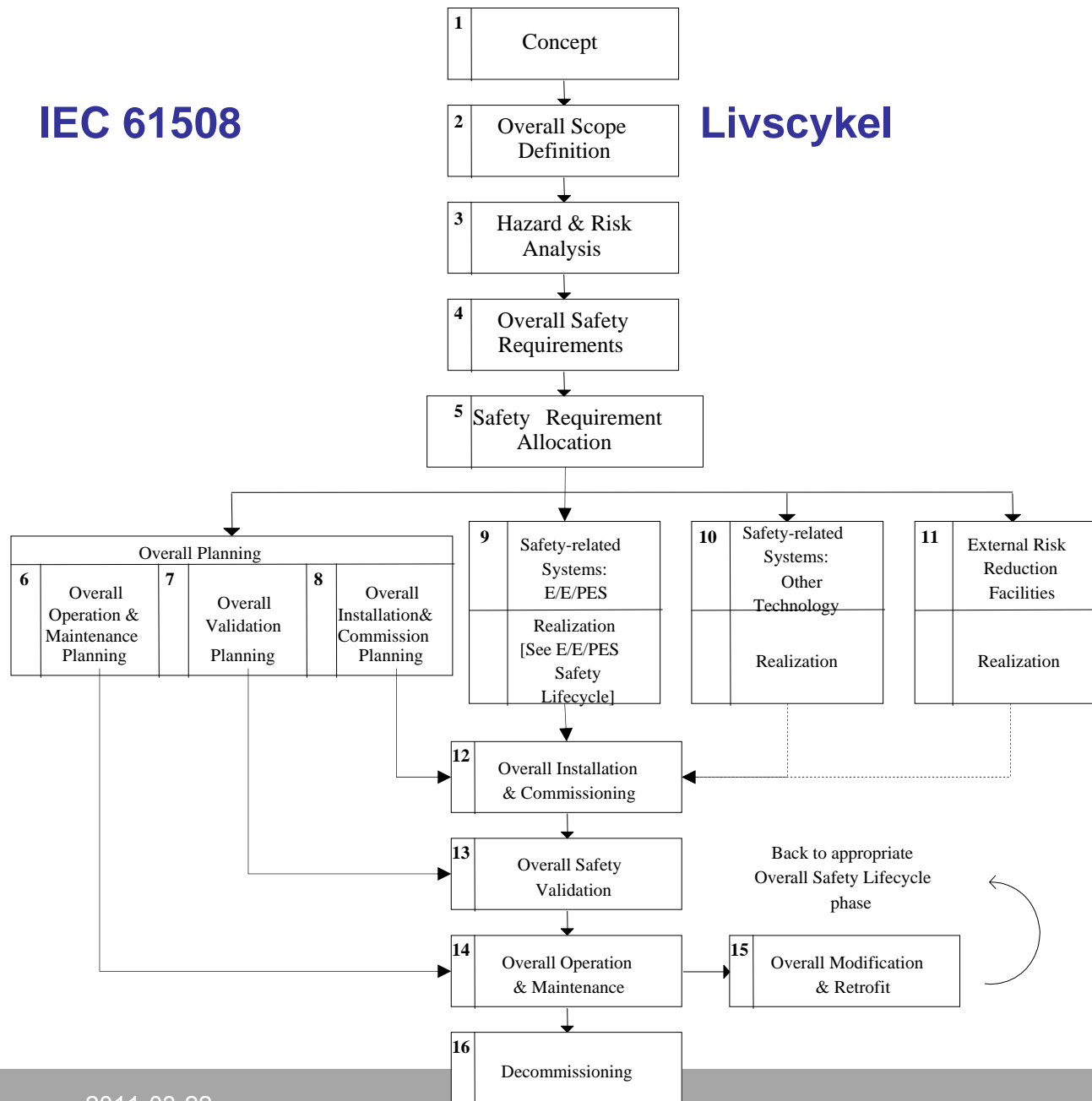
## Typer av fel i säkerhetskritiska system





## IEC 61508

## Livscykel



## Low, high demand

- Det finns två olika fall för bestämningen av SIL-nivå beroende på om funktionen anses vara low demand mode eller high demand mode.
- Low demand mode gäller generellt för processindustrin t ex tryckvakter och temperaturvakter.
- High demand mode används mest för maskiner t ex grindar och klämlister.

## IEC 61508-1

**Table 2 – Safety integrity levels: target failure measures for a safety function operating in low demand mode of operation**

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

**Table 3 – Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation**

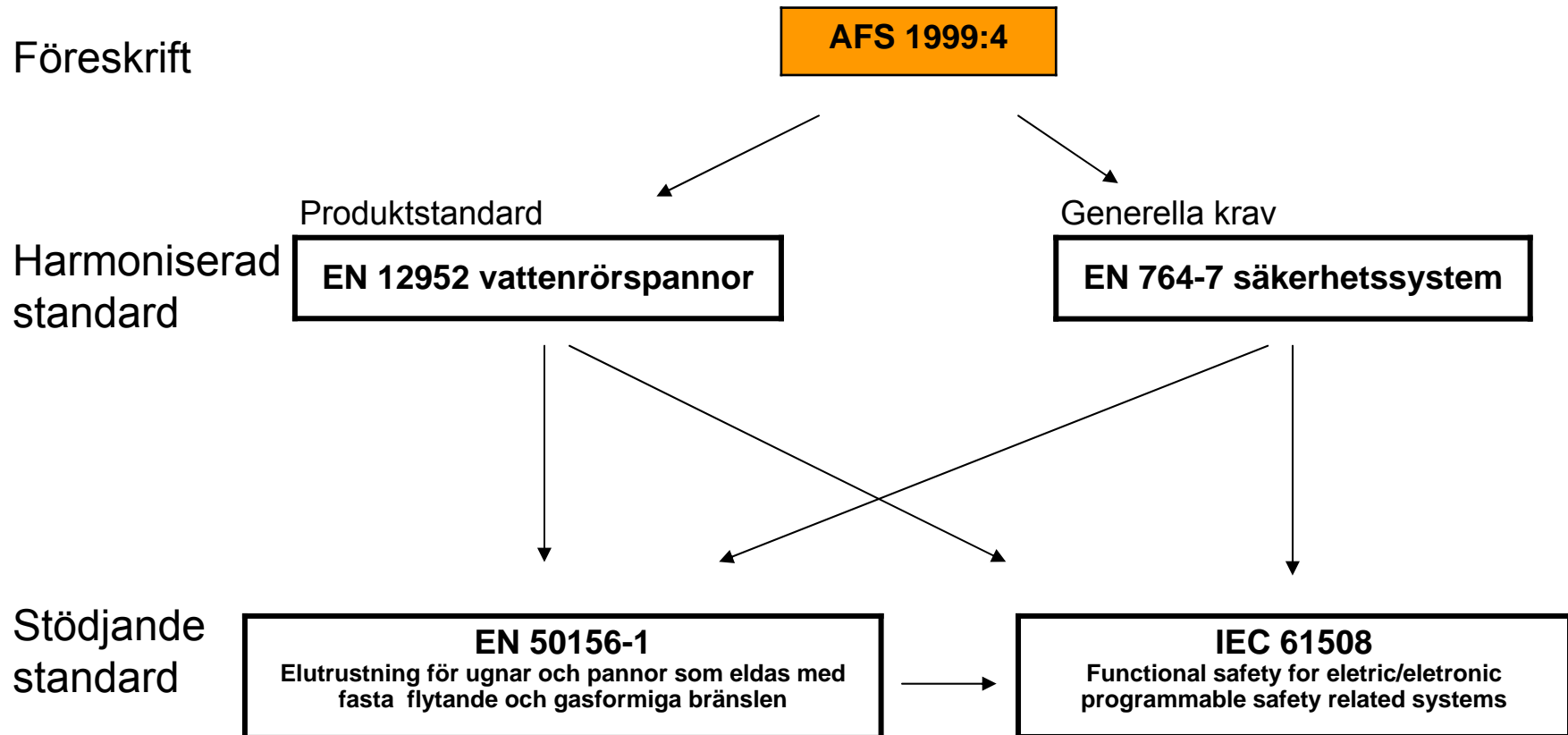
Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	



## Standarderna

- IEC 61508 huvudstandard
- IEC 61511 Processindustrin
- IEC 62061 och ISO 13849 för maskiner (ersätter 954-1,2)

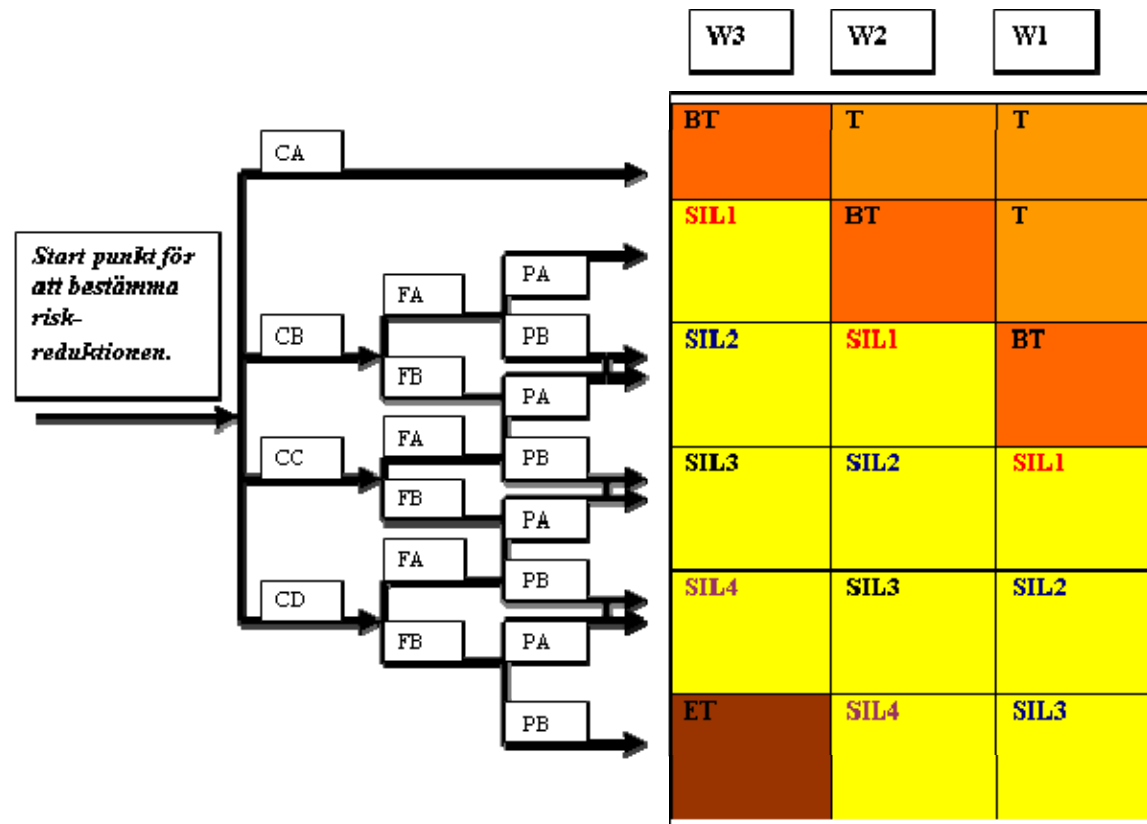
## ► Finns det koppling mellan AFS 1999:4 och SIL? Krav?



## RISKANALYS

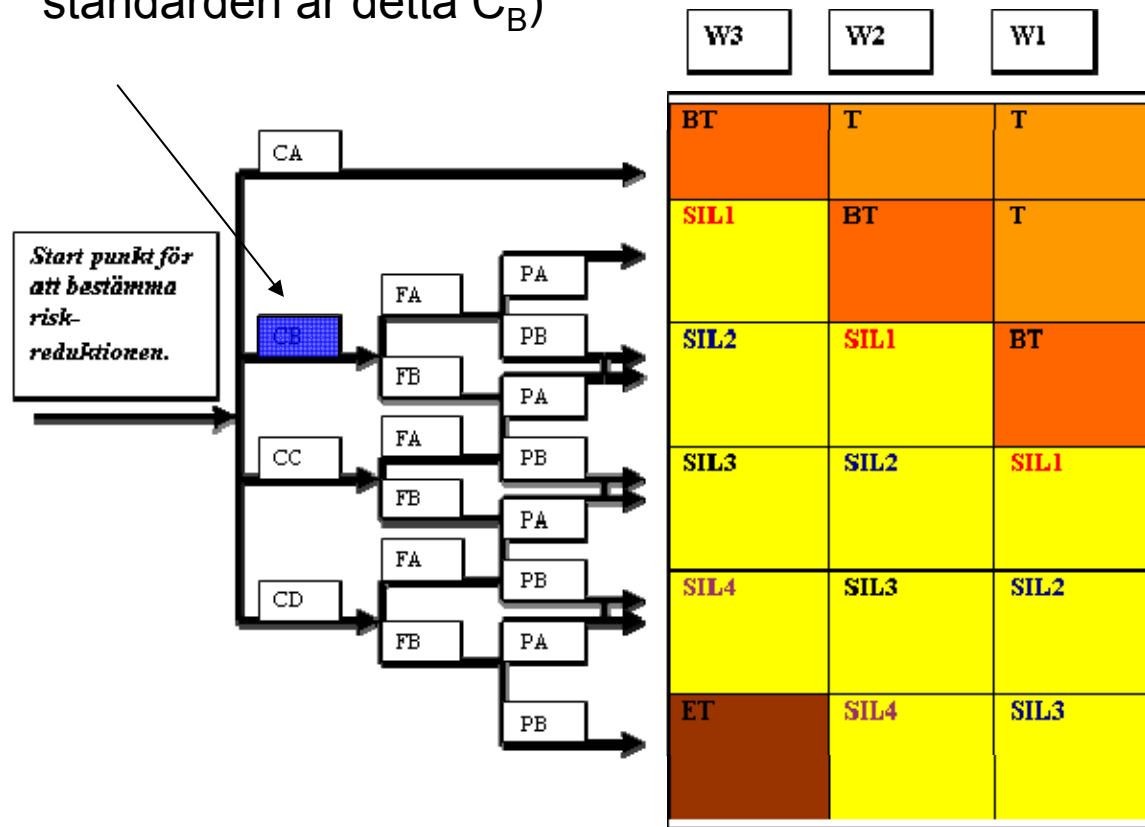
- Acceptabel risk (Myndigheter i Sverige har ej satt någon nivå)
- Bestämning av vilka kretsar som krävs (HAZOP/ harmoniserad standard)
- Bestämning av SIL-nivå
- LOPA
- Riskgrafer - kalibrering
- Resultat från riskanalysen – indata till SRS (Safety Requirement Specification)

## Riskgraf enligt IEC 61511-3



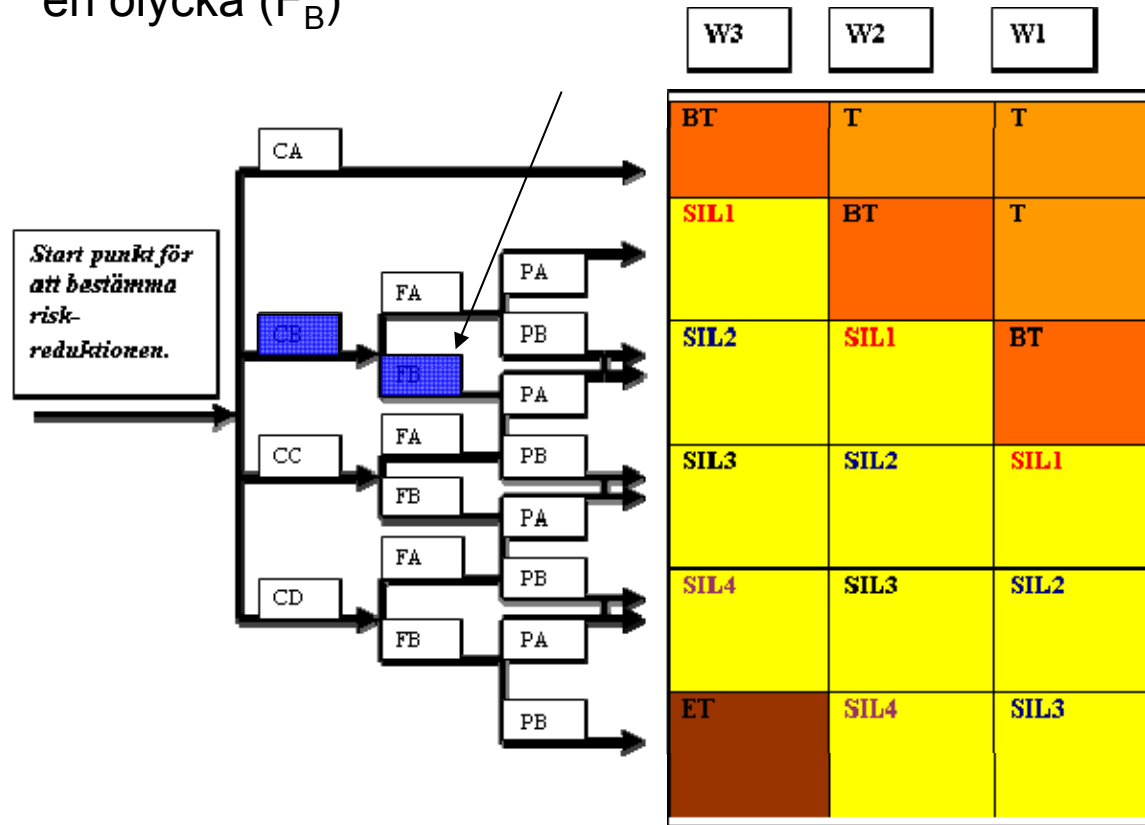
## ▶ Att läsa ut acceptabel risk ur riskgraf

1. Välj lägsta konsekvensen som ger dödsfall (i exempelgrafen i standarden är detta  $C_B$ )



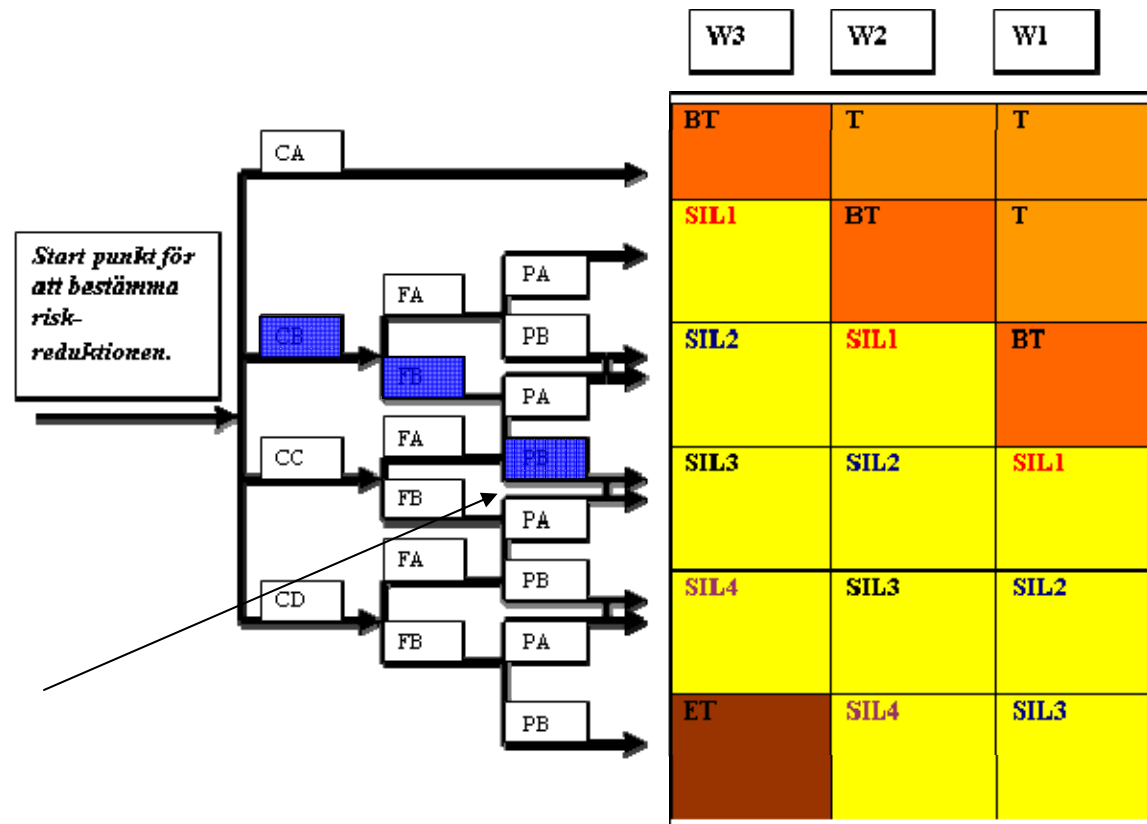
## ▶ Att läsa ut acceptabel risk ur riskgraf

2. Förutsätt att det inte finns någon möjlighet att undkomma vid en olycka ( $F_B$ )



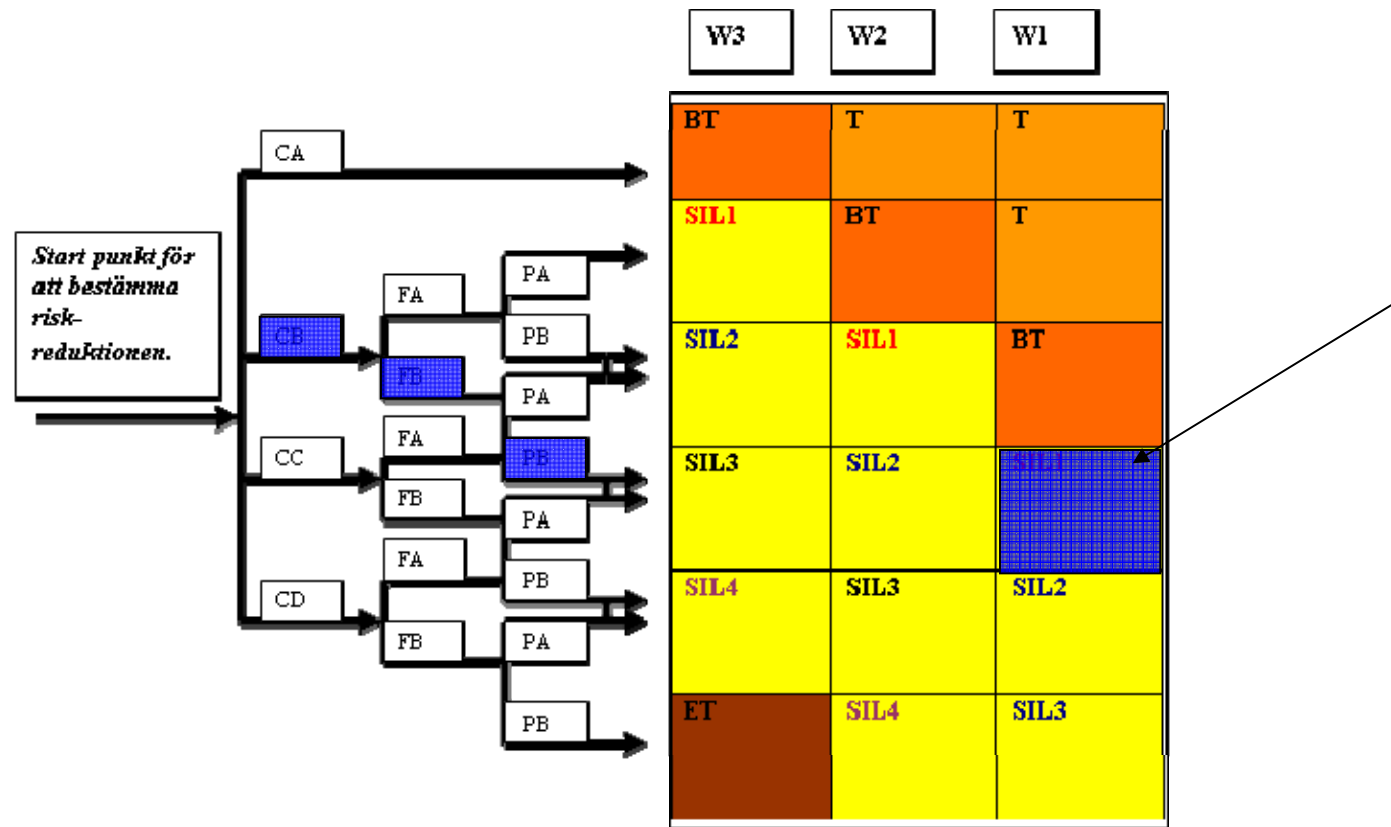
## ▶ Att läsa ut acceptabel risk ur riskgraf

3. Förutsätt att det alltid finns personer närvarande ( $P_B$ )



## ▶ Att läsa ut acceptabel risk ur riskgraf

4. Välj valfri olycksfrekvens där det krävs SIL och läs ut SIL-nivå





## ▶ Att läsa ut acceptabel risk ur riskgraf

5. Beräkna högsta sannolikhet för dödsfall enligt de valda parametrarna.

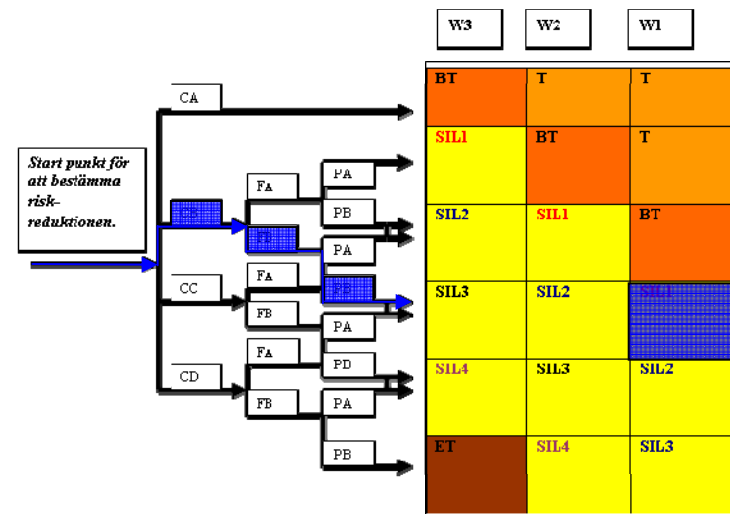
### *Exempel enligt exempelgraf i standard*

Enstaka dödsfall motsvaras av  $C_B$

Ingen reduktion av sannolikheten med avseende på personnärvaro eller möjlighet att omkomma ( $F_B$ ,  $P_B$ )

$W_1$  motsvaras av en gång på 10-100 år (1 gång på 10 år högsta värdet)

SIL 1 reducerar risken 10-100 gånger (10 gånger ger högsta sannolikheten för olycka)



**Resultat:** I exempelgrafen från standarden så är den acceptabla risken 1 dödsfall på 100 år. (1 dödsfall på 10 år reduceras 10 gånger med en SIL 1 SIF till att 1 gång på 100 år)

## Acceptabel risk

- Hur mycket risk (dödsfall/år eller dylikt) kan en anläggning acceptera?
- Alla företag måste ta ett eget beslut om acceptabel risknivå.
- Används riskgrafer/riskmatriser från IEC 61508 / 61511 så måste de omkalibreras.
- Vad är acceptabelt? Inga dödsfall / 1 dödsfall per år / 1 dödsfall per 10 år / 1 dödsfall per 100 år / 1 dödsfall på 1000 år / 1 dödsfall på 10 000 år
- Väldigt viktigt att den acceptabla risknivån bestäms!

## SRS

- Funktionskrav (tätningar, material m.m), integritets krav (SILnivå), SFF krav, tillgänglighetskrav, testintervallskrav m.m

## Design av säkerhetssystemet

- Skall minst nå den erforderliga integritetsnivån och RRF (riskreduceringsfaktor)
- Påverkas av
  - förutbestämd livslängd
  - utformning av säkerhetssystem arkitektur, komponentval m.m
- - testintervall

## Krav på testintervall

- Utdrag ur AFS:1999:4 Bilaga1 – Grundläggande säkerhetskrav
- 2.11.1 Säkerhetsutrustning skall uppfylla följande krav.
- a) *Den skall vara konstruerad och tillverkad så, att den är tillförlitlig och anpassad för sin avsedda användning och så, att behovet av underhåll och provning har beaktats*
- Utdrag ur AFS:2005:3 - Krav vid besiktning
- Återkommande besiktning
- Driftprov.
- 14§ *Vid återkommande besiktning genom driftprov skall systemkontroll och funktionskontroll av säkerhetsutrustning utföras.*
- 16§ *Vid funktionskontroll av säkerhetsutrustning skall*
- *kontrolleras att utrustningen som behövs med hänsyn till säkerheten finns och fungerar tillfredsställande, och*
- *en invändig undersökning göras av säkerhetsutrustning vars funktion bedöms ha kunnat påverkas negativt av de fluider som utrustningen kommit i kontakt med.*

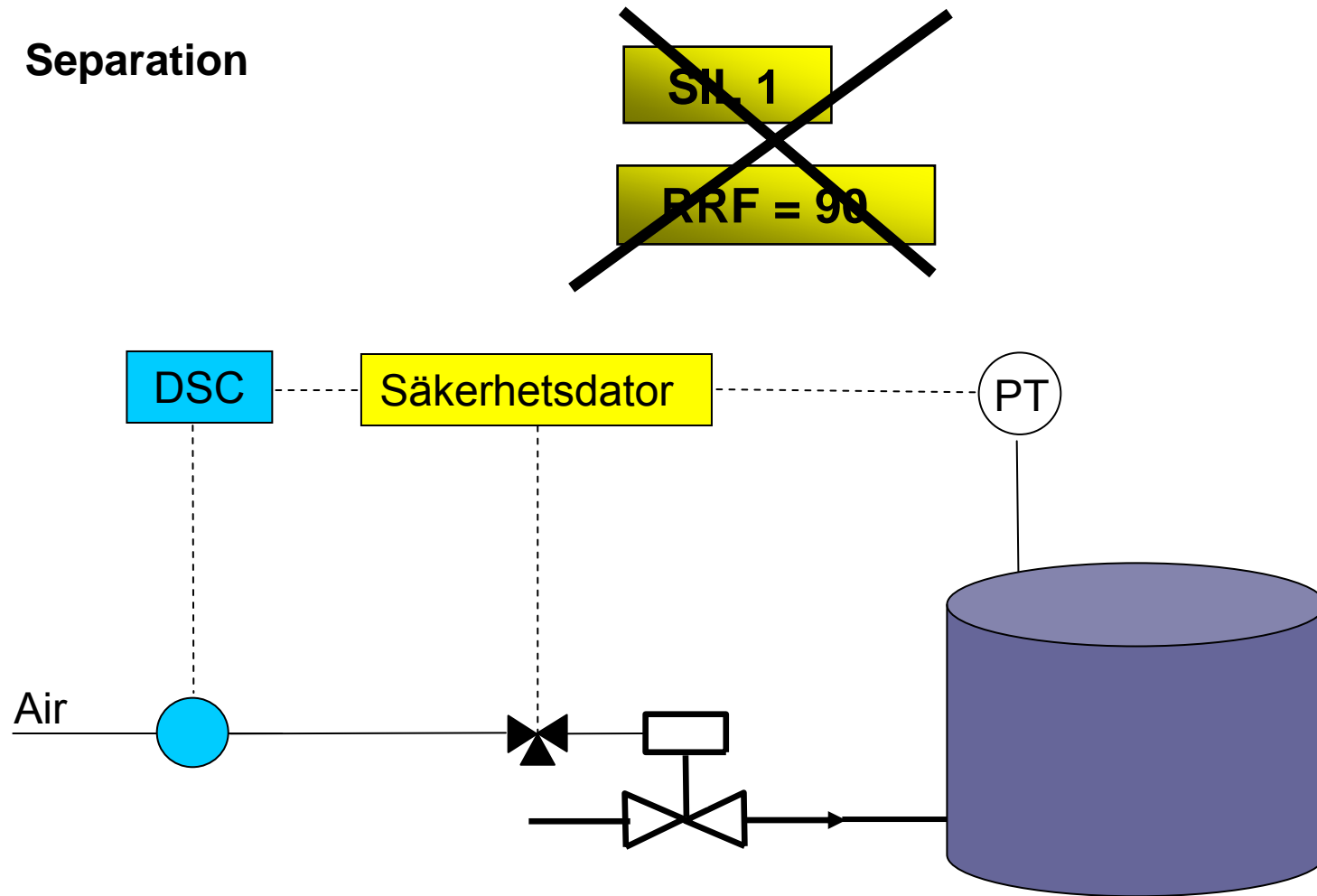
## Krav på testintervall

- När det rör sig om det grundläggande kravet avseende maximalt testintervall enligt IEC61508/61511 fås den från definitionen av "low demand mode". Enligt standarden så innebär detta man för att få tillgodoräkna sig testningens inverkan inte får ha ett förväntat anrop på säkerhetsfunktionen oftare än en gång om året eller oftare än minst den dubbla tiden mellan två tester.

## Separation DCS- SIS

- SILklassade kretsar ska vara separerade från styrsystemet och ingå i en säkerhets-PLC.

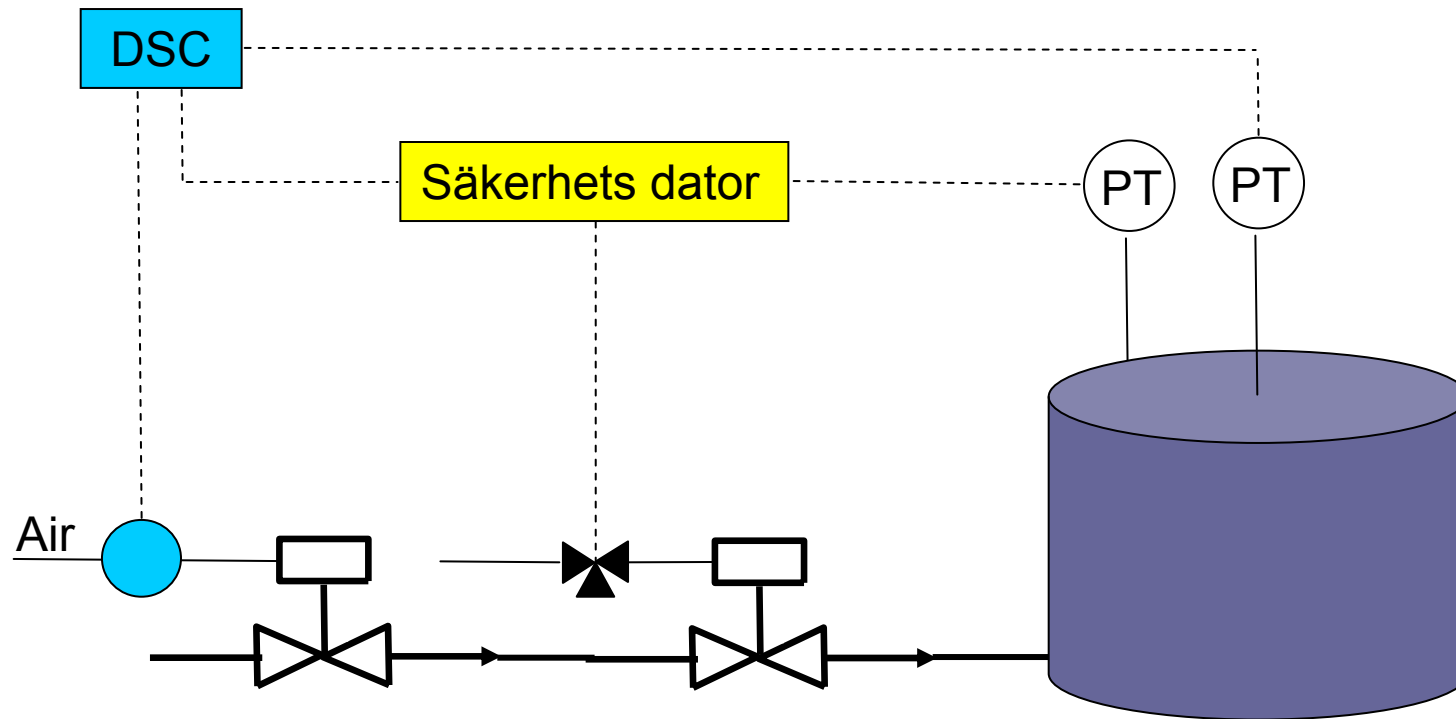
## ▶ Separation



Barriären och säkerhetssystemet delar signal, och säkerhetssystemet tillför i princip **ingen riskreduktion!!!**



## Separation



Rätt utförande med en barriär och ett säkerhetssystem

## Verifiering

- När man har PFDavg värden på alla komponenter i en krets summeras de ihop. Den jämförs sedan med det värde som krävs för kretsen. T ex:
- Sensor                      PFDavg  $5,78 \times 10^{-4}$
- Logik                        PFDavg  $1,05 \times 10^{-3}$
- Manöverdon              PFD avg  $5,26 \times 10^{-3}$
- Summa PFDavg  $6,89 \times 10^{-3}$ . RRF (Risk Reduction Factor) är då  $1 / 6,89 \times 10^{-3} = 145$
- Kretsen har uppnått SIL 2.

## SIL-rapport

- Sammanfattning för varje SIL-krets:
- SILkrav
- Komponentval
- Arkitektur
- Testintervall

SRS+verifieringsrapport+ annan relevant information

## Validering

- FAT frivillig
- SAT 3e part närvarande för besiktningspliktiga objekt
- Checka av mot SRS, SIL-rapport (verifieringens krav och val av komponenter, arkitektur, testintervall)



## Sammanfattning av IEC 61508 / 61511

### Processen

- Riskanalys, bestämmer var det krävs säkerhetsutrustning
- Bestämning av **processens SIL-nivå** utan säkerhetsutrustning
- LOPA kan reducera erforderlig SIL-nivå

### Säkerhetssystemet

- Konstruera ett säkerhetssystem för uppgiften
- Beräkna **säkerhetssystemets SIL-nivå (verifiering)**
  - Omfattar hela säkerhetssystemet från givare till aktiveringsfunktion
  - Beräkna erforderligt testintervall för vidbehålla SIL-nivån PLUS vad finns det för lagkrav på testintervall på objektet?

### Nu kan säkerhetssystemet byggas

## Kurs, SIL-klassning

- Inspectas kurskatalog 2011, planerat datum 9 juni i Gbg

▶ TRUST & QUALITY [www.inspecta.com](http://www.inspecta.com)