

Safety Integrity Level



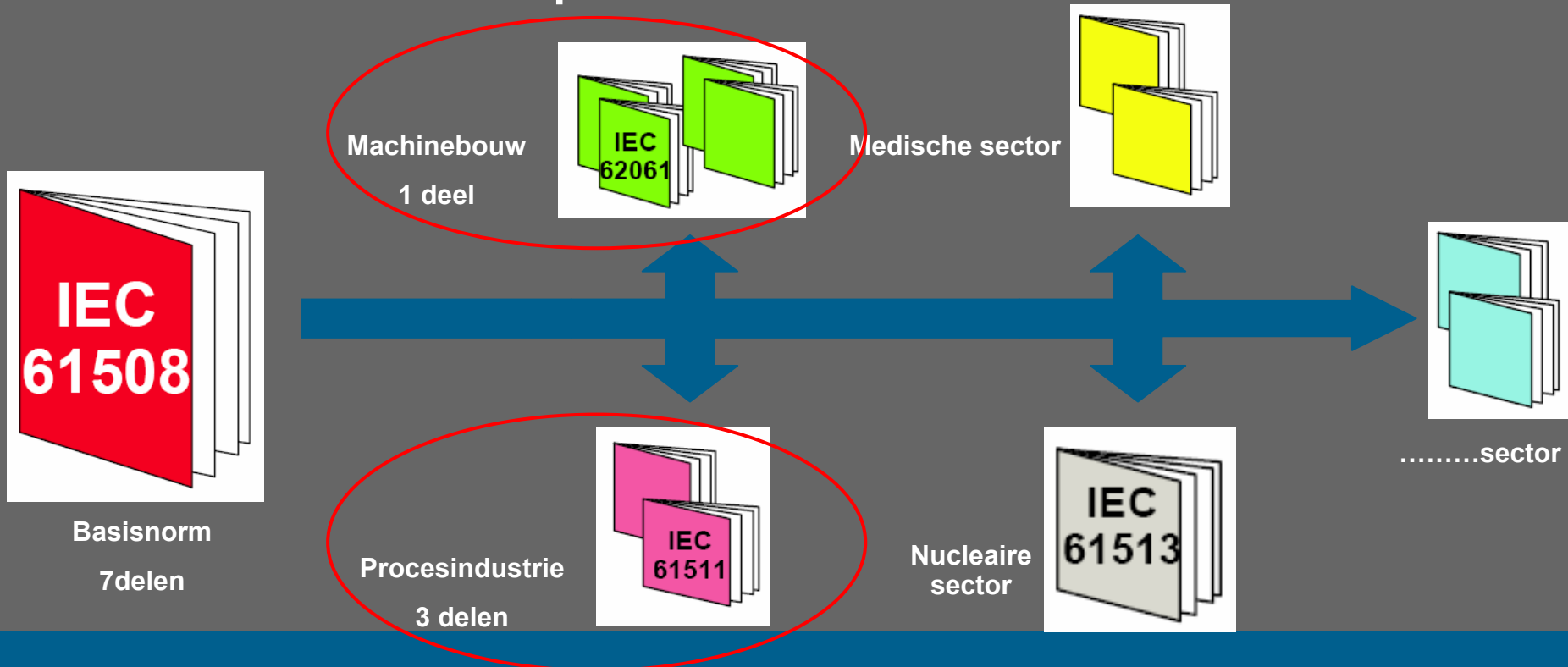
BKL Engicon

Technisch project- en adviesbureau

Basisbegrippen & Inleiding

Basisbegrippen SIL

- SIL staat voor: Safety Integrity Level
- Gebaseerd op IEC norm



Basisbegrippen SIL

- SIL is classificatie van de betrouwbaarheid van een besturingstechnisch veiligheidscircuit
- SIL wordt geclassificeerd in 4 niveau's:
 - SIL 1
 - SIL 2
 - SIL 3
 - SIL 4 (niet in de machinebouw)



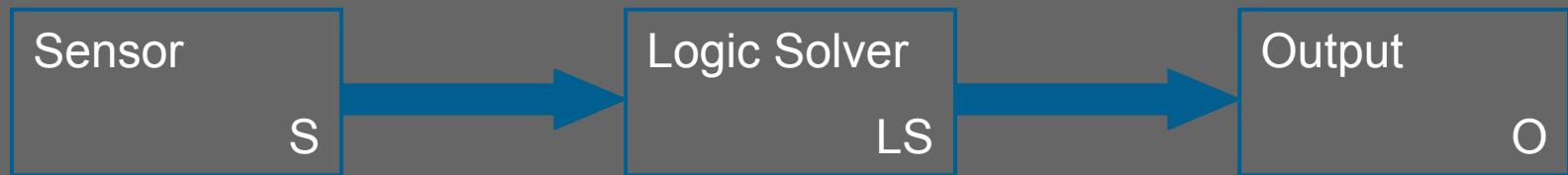
Maat voor hogere
betrouwbaarheid van
het veiligheidscircuit

Definities

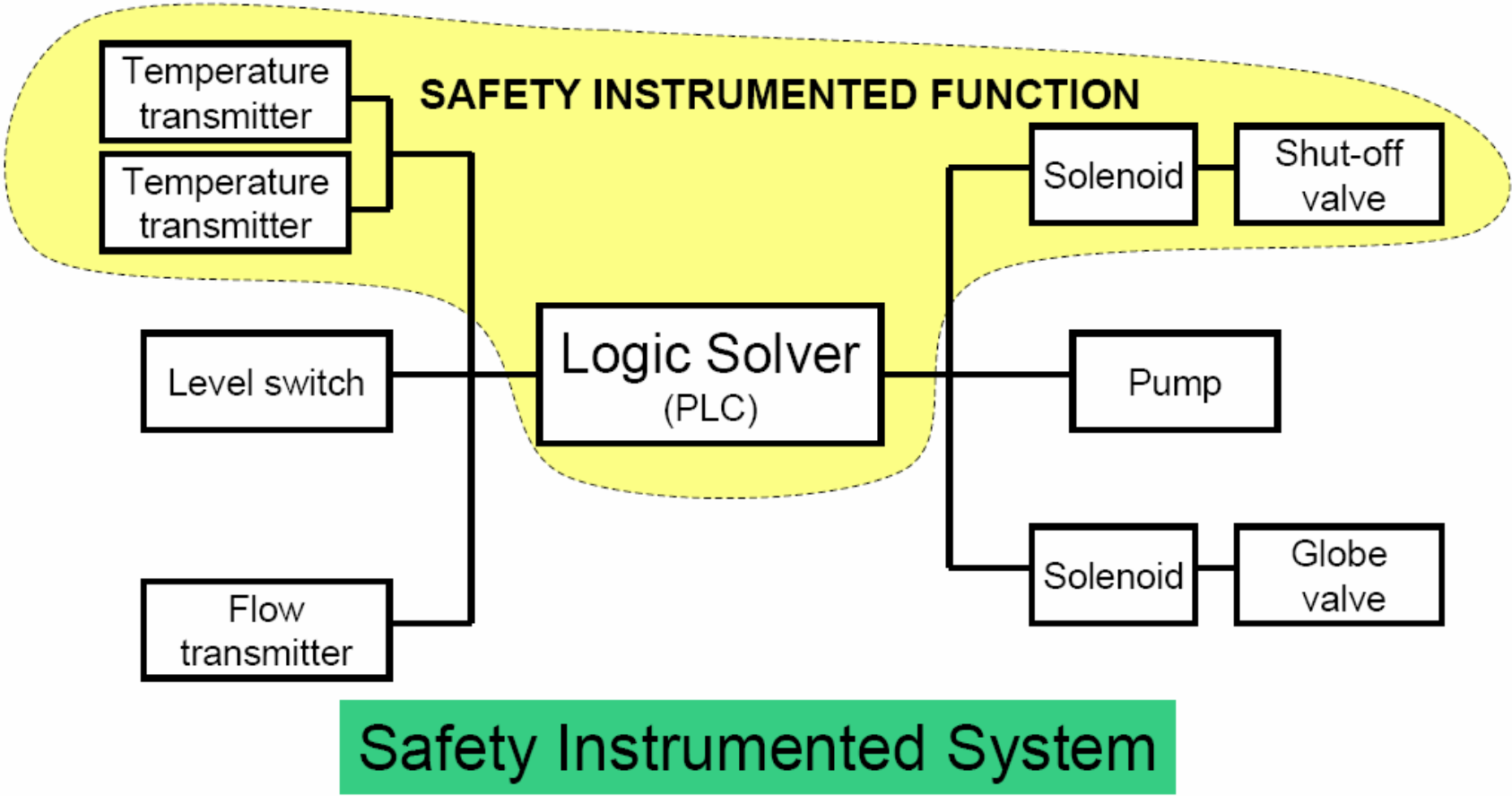
- Functionele veiligheid (Functional Safety):
 - Dat deel van de veiligheid dat afhankelijk is van het correct functioneren van de aangebrachte veiligheidsfuncties
- SIS (IEC 61511; procesindustrie):
 - Safety Instrumented System
- SRECS (IEC 62061; machinebouw):
 - Safety Related Electrical Control Systems

Definities

- SIS en SRECS worden opgedeeld in een blokschema dat er in het algemeen als volgt uitziet:



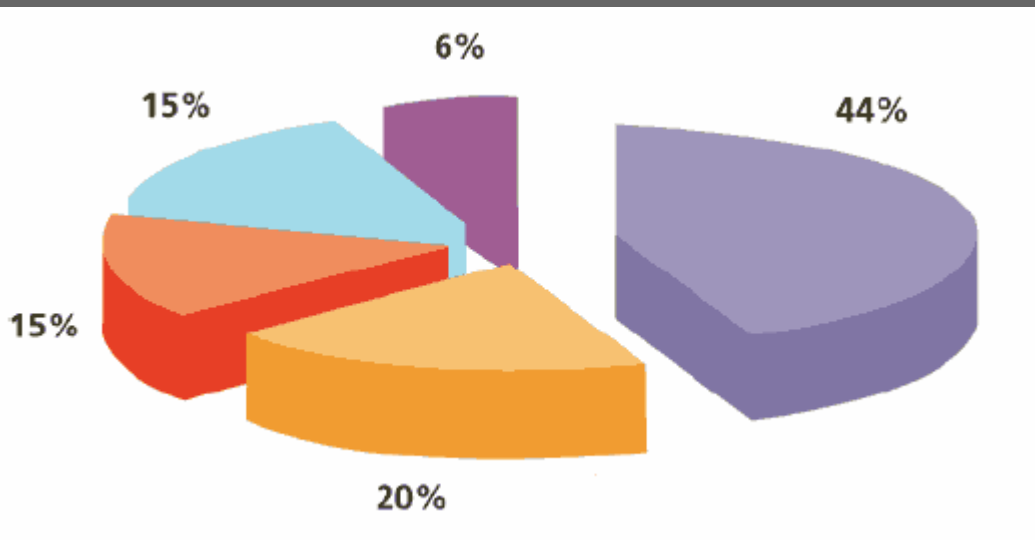
Definitives



Functionele veiligheid

- Waarom een norm die het falen van veiligheidsfuncties beschrijft:

Onderzoek “Out of control” door de Engelse arbeidsinspectie:



44%: Gebrek aan specificaties

20%: Wijzigingen na commisioning

15%: Ontwerp en toepassing

15%: Bedrijf en onderhoud

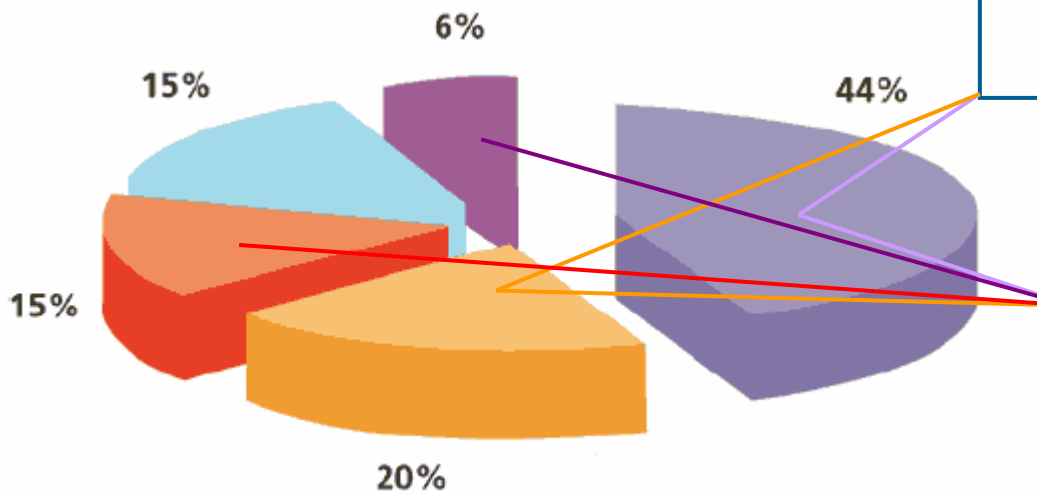
6%: Tijdens installatie en ingebruikname

Functionele veiligheid

64% van de ongevallen door een gebrek aan duidelijkheid:

Over de veiligheidsfunctie die het systeem moest uitvoeren

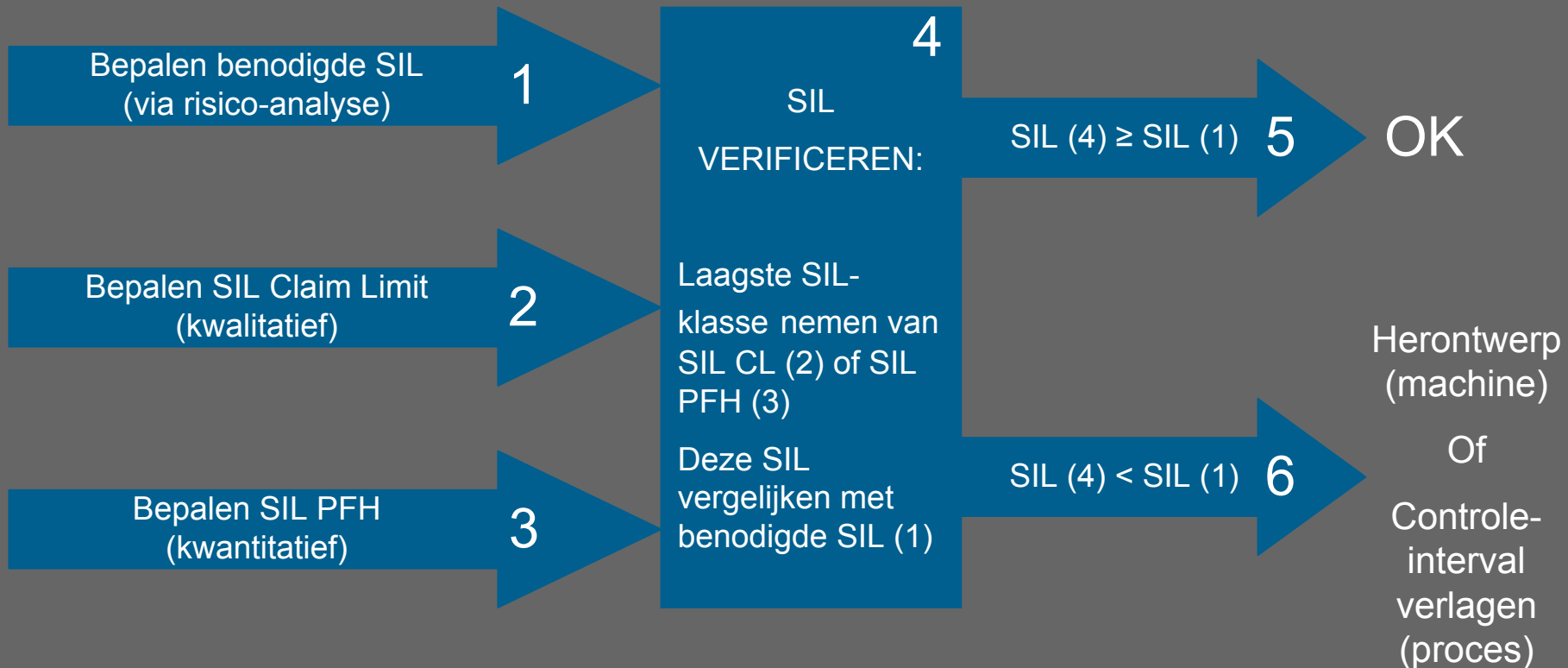
Over de mate waarin dit systeem dit moest doen



85% = engineeringgerelateerd

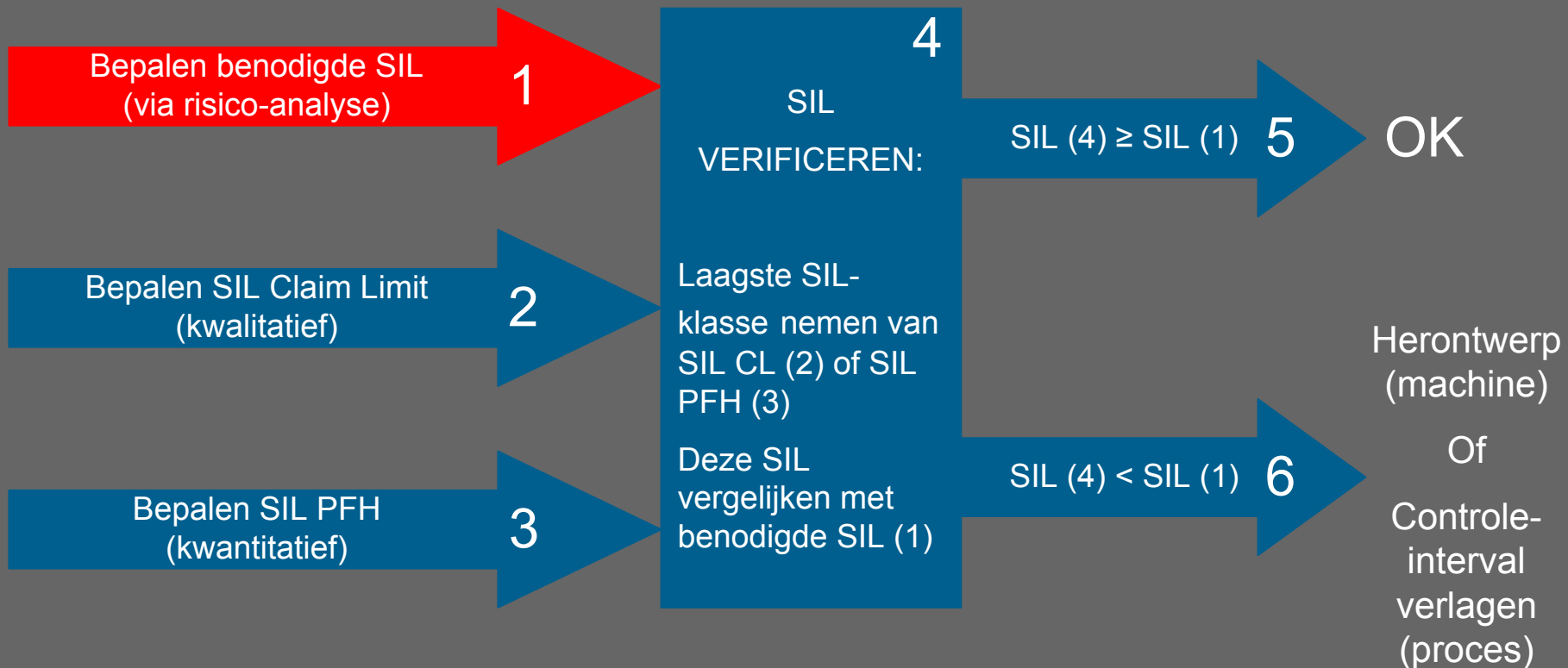
Bepalen van SIL

- Hoe wordt SIL bepaald?:



1. Bepalen benodigde SIL

- Hoe wordt SIL bepaald?:

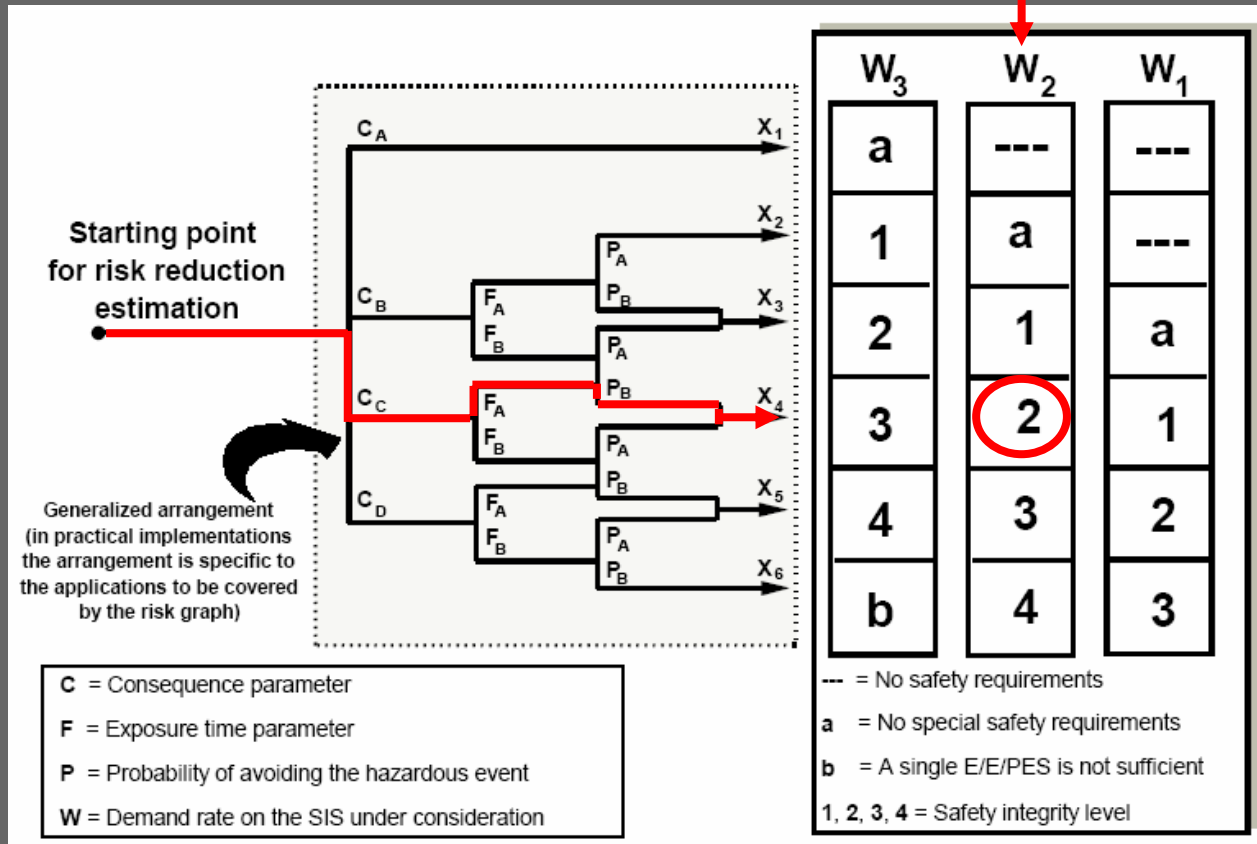


1. Bepalen benodigde SIL

- Methode van risicobepaling:
 - Procestechniek: Risico-analyse bv.: HAZOP-studie, ALARP-principe, enz...
 - Machinebouw: Risicobeoordeling bv.: Methode van Fine & Kinney, Risicograaf, ...

1. Bepalen van benodigde SIL

- Procesindustrie:



1. Bepalen van benodigde SIL

- Machinebouw:

Consequences	Severity (SE)
Irreversible: death, loosing an eye or arm	4
Irreversible: broken limb(s), loosing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Frequency of exposure	> 10 min.
≤ 1 hour	5
> 1 hour to ≤ 1 day	5
> 1 day to ≤ 2 weeks	4
> 2 weeks to ≤ 1 year	3
> 1 year	2

Probability of occurrence	Probability (Pr)
Very High	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Impossible	5
Rarely	3
Probable	1

1. Bepalen van benodigde SIL

- Machinebouw:

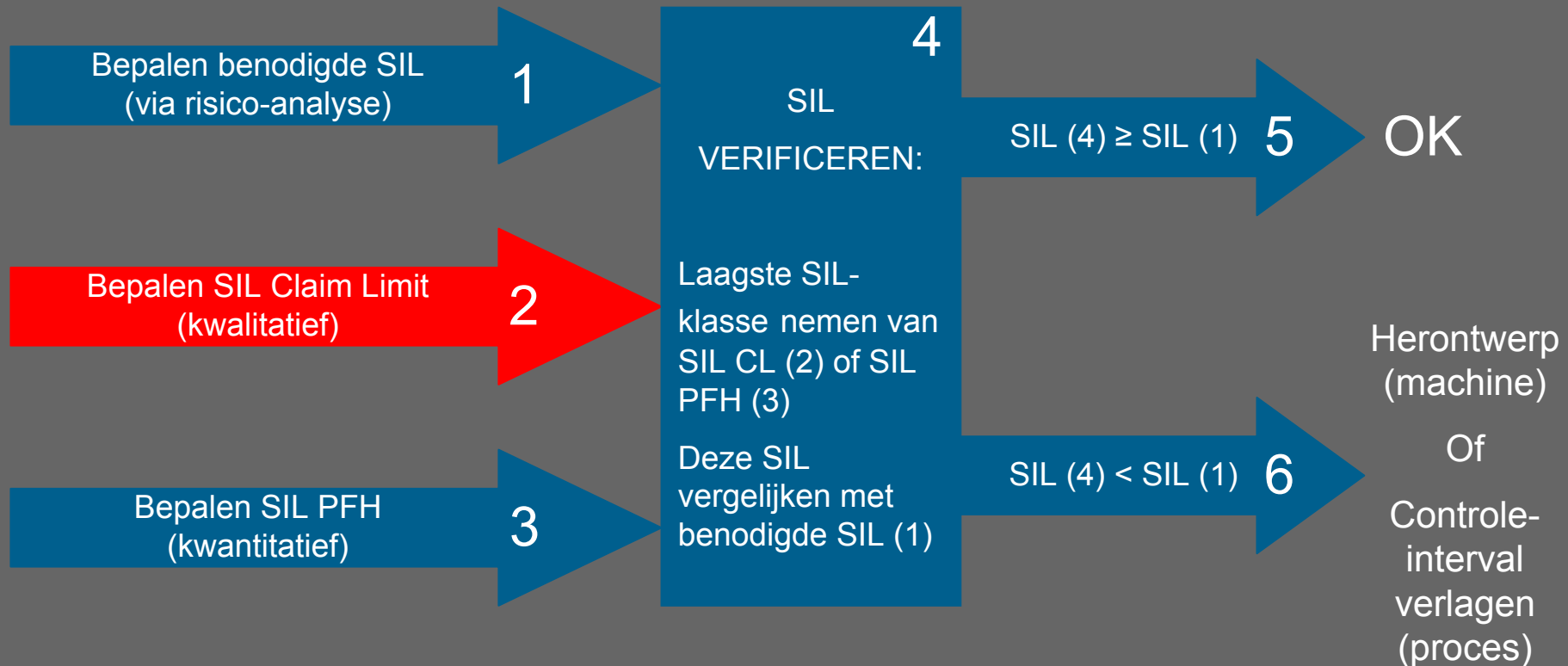
$$\text{CLASS} = Fr + Pr + Av$$

$$\text{CLASS} = 5 + 3 + 3 = 11$$

Severity (SE)	Class (CL)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

2. Bepalen SIL Claim Limit

- Hoe wordt SIL bepaald:



2. Bepalen SIL Claim Limit

- Het bepalen van de SIL Claim Limit is een kwalitatieve bepaling de SIL en wordt bepaald door 2 parameters:
 - HFT: Hardware Fault Tolerance = mate van redundantie
 - SFF: Safe Faile Fraction = mate van diagnose

2. Bepalen SIL Claim Limit

- HFT:
 - Het minimum aantal fouten in een subsysteem (sensor, logic solver, output), die optreden door willekeurige hardwarefouten, dat een verlies van de veiligheidsfunctie kan veroorzaken, min 1.

M.a.w. als $HFT = 0$, dan is er bij $N+1$ fouten een verlies van de SIS & SRECS

2. Bepalen SIL Claim Limit

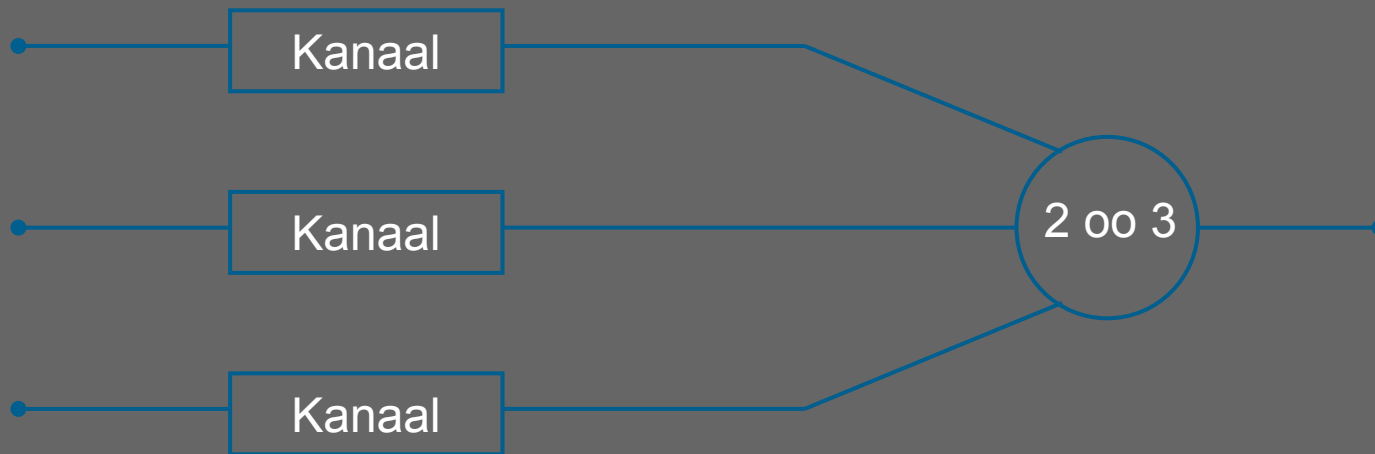
- HFT:
 - Ontwerp en architectuur van SRECS & SIS

Aantal gevaarlijke fouten	Betekent	Architectuur
0	1 fout geeft een gevaarlijke toestand	1 out of 1
1	1 fout en het systeem is nog veilig	1 out of 2; 2 out of 3
2	2 fouten en het systeem is nog veilig	1 out of 3
3	3 fouten en het systeem is nog veilig	1 out of 4

2. Bepalen SIL Claim Limit

- HFT:
 - Ontwerp en architectuur van SRECS & SIS

$$n \text{ oo } k: \text{HFT} = k - n$$



$$\text{HFT} = k - n = 3 - 2 = 1$$

$$1 \text{ oo } 1: \text{HFT} = 0$$

$$1 \text{ oo } 2: \text{HFT} = 1$$

$$1 \text{ oo } 3: \text{HFT} = 2$$

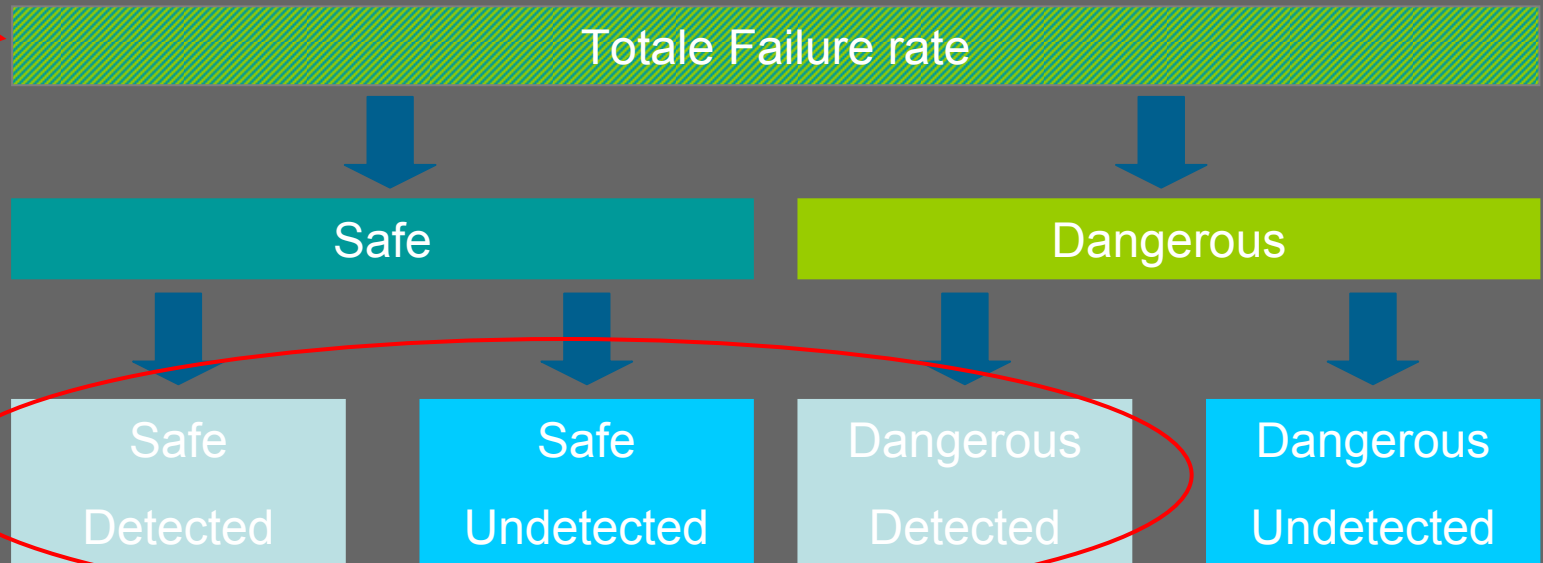
$$1 \text{ oo } 4: \text{HFT} = 3$$

$$2 \text{ oo } 3: \text{HFT} = 1$$

$$2 \text{ oo } 4: \text{HFT} = 2$$

2. Bepalen SIL Claim Limit

- SFF:
 - De fractie van de totale faalfrequentie van een subsysteem dat niet resulteert in gevaarlijk falen



2. Bepalen SIL Claim Limit

- SFF:
 - De fractie van de totale faalfrequentie van een subsysteem dat niet resulteert in gevaarlijk falen

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_{totaal}}$$

$$SFF = \frac{\lambda_S + \lambda_D \times DC}{\lambda_S + \lambda_D}$$

2. Bepalen SIL Claim Limit

- DC = Diagnostic Coverage = parameter die staat voor de mate van automatische diagnose.

Algemene formule voor bepalen DC:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$$

2. Bepalen SIL Claim Limit

- De SIL Claim Limit kan in de tabel afgelezen worden als een combinatie van de Safe Failure Fraction en de Hardware fault tolerance

Bv: SFF = 55% en HFT = 1

Safe Failure fraction	Hardware fault tolerance (see Note 1)		
	0	1	2
< 60%	Not allowed	SIL1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4 (Note 2)
≥ 99 %	SIL 3	SIL 4 (Note)	SIL 4 (Note 2)

NOTE 1: A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function
NOTE 2: Not in IEC 62061

3. Bepalen van SIL PFH

- Hoe wordt SIL bepaald?:



3. Bepalen van SIL PFH

- Meest complex en wiskundig gedeelte voor het bepalen van de SIL
- Is afhankelijk van de:
 - De architectuur (1oo1; 1oo3; ...)
 - De faalkans welke zorgt voor gevaarlijk falen
- Berekenen van de faalkans van het totale systeem
- Eveneens rekening houden met optredende transmissiefouten (P_{TE}) tussen componenten

$$PFH_D = PFH_{D1} + \dots + PFH_{Dn} + P_{TE}$$

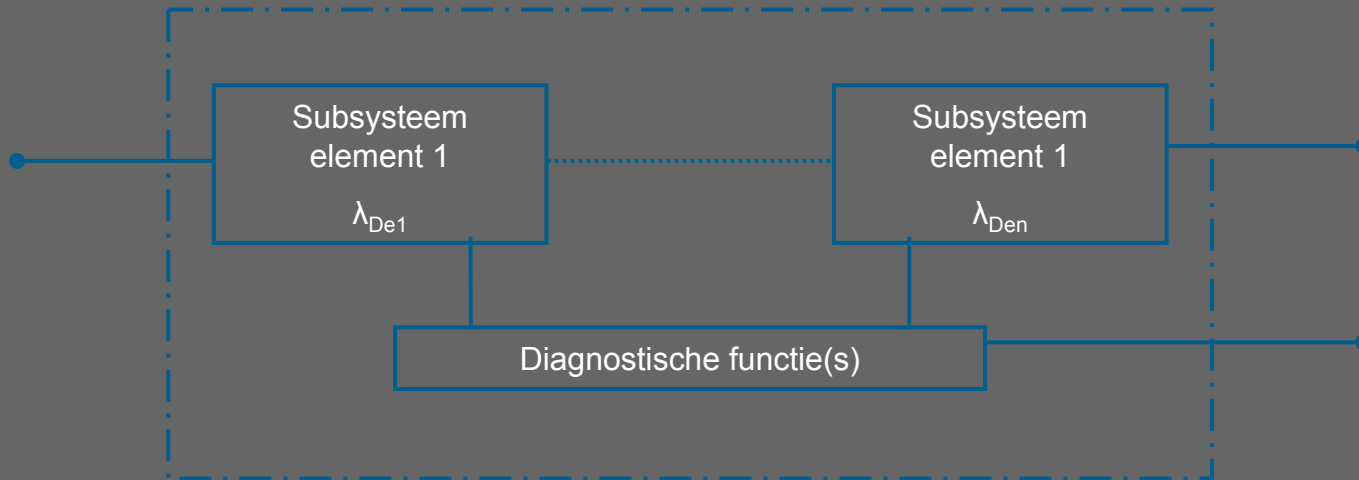
3. Bepalen van SIL PFH

UITGANGSPUNTEN:

- $\lambda = 1 / \text{MTTF}$
- $\lambda = \lambda_S + \lambda_D$
- $\text{PFH}_D = \lambda_D \times 1\text{h}$ (Gemiddelde kans op gevaarlijk falen per uur)
- $T_2 = \text{Diagnostic test interval}$
- $T_1 = \text{Proof test Interval} / \text{levensduur}$ (welke de kleinste is)
- $\text{DC} = \text{Diagnostic Coverage}$
- $\beta = \text{Common Cause factor}$ (kans dat meerdere componenten tegelijkertijd falen; bv 1, 5 of 10%)

3. Bepalen van SIL PFH

- Moeilijkheidsgraad is volledig afhankelijk van de architectuur: bv eenvoudige 1oo1 met diagnose



$$\lambda_{DssC} = \lambda_{De1} (1 - DC_1) + \dots + \lambda_{Den} (1 - DC_n)$$

$$PFH_{DssC} = \lambda_{DssC} \times 1h$$

3. Bepalen van SIL PFH

Na van elke component de PFHD berekend te hebben, kan de totale PFHD bepaald worden:

$$PFH_D = \sum PFH_{Dsensor} + \sum PFH_{Dlogicsolver} + PFH_{Douput} + P_{TE}$$

3. Bepalen van SIL PFH

Samenvattend: hoe bepalen PFH?

1. Teken het schema waarin de componenten te zien zijn van elk onderdeel
2. Bepaal het proof-test interval
3. Bepaal voor elke component:
 - » Architectuur
 - » Diagnostic Coverage factor
 - » De failure rate van het element
 - » De Common Cause Factor
4. Bereken de PFH van elke component
5. Bepaal de kans op transmissiefouten tussen componenten
6. Bereken de totale PFH

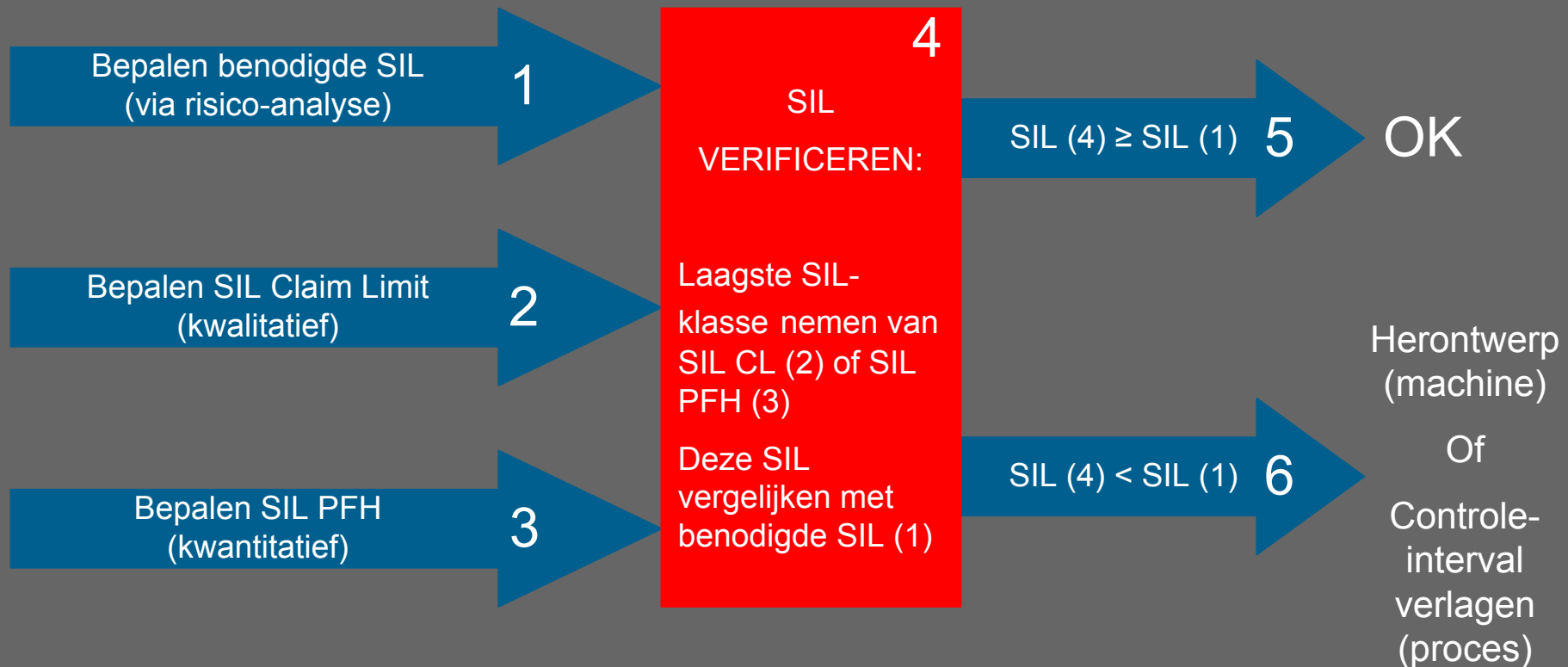
3. Bepalen van SIL PFH

Kans op falen per uur (PFH)	SIL klasse
$10^{-6} \leq \text{PFH} < 10^{-5}$	SIL 1
$10^{-7} \leq \text{PFH} < 10^{-6}$	SIL 2
$10^{-8} \leq \text{PFH} < 10^{-7}$	SIL 3
$10^{-8} \leq \text{PFH} < 10^{-9}$	SIL 4*

* SIL 4 is niet van toepassing bij de machinebouw

4. SIL verificeren

- Hoe wordt SIL bepaald?:

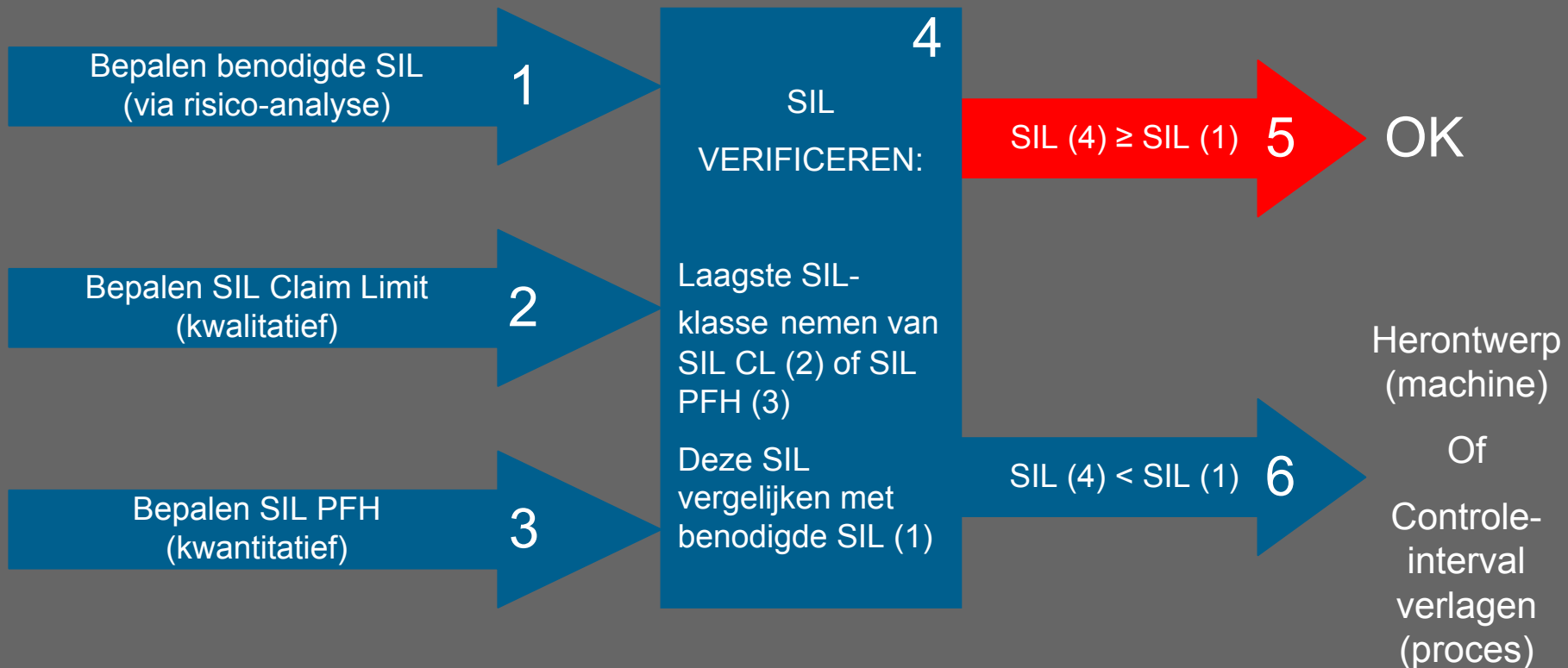


4. SIL verificeren

- Men bekomt 2 SIL klassen:
 - SIL Claim Limit
 - SIL PFH
- Van beide bekomen SIL klassen neemt men de laagste SIL klasse om deze met de SIL klasse, gekomen uit de risicoanalyse, te vergelijken

5. SIL (4) ≥ SIL (1)

- Hoe wordt SIL bepaald?:



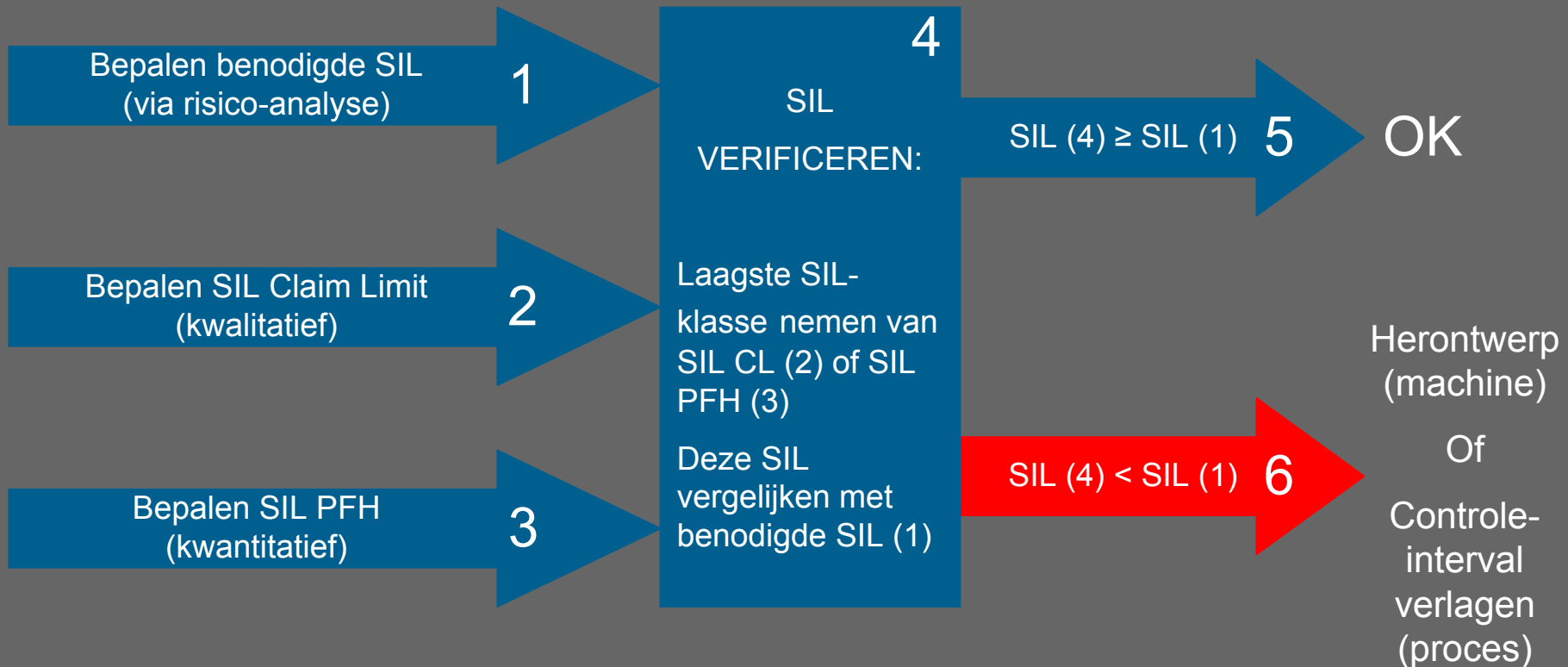
5. SIL (4) \geq SIL (1)

Indien de geverificeerde SIL klasse hoger is dan deze die gekomen is uit de risicoanalyse, wil dit zeggen dat het ontwerp van het veiligheidscircuit voldoende is om aan de risico's te voldoen



6. SIL (4) < SIL (1)

- Hoe wordt SIL bepaald?:



6. SIL (4) < SIL (1)

Als de geverificeerde SIL klasse lager is dan deze uit de risicoanalyse, voldoet het ontwerp van het veiligheidscircuit NIET om de optredende risico's m.b.t. veiligheid op te vangen

6. SIL (4) < SIL (1)

Hoe oplossen?:

In de meeste gevallen zijn er 2 zeer algemene oplossingen:

- Herontwerp van het veiligheidscircuit:
 - Componenten met een lagere failure rate
 - Meer redundantie bij de componenten
- Het verkleinen van het inspectieinterval

6. SIL (4) < SIL (1)

Na aanpassen van het inspectieinterval of de herontwerp van het veiligheidscircuit (of beiden) begint de ganse berekeningscyclus opnieuw tot het veiligheidscircuit aan het gewenste beveiligingsniveau voldoet

Safety Integrity Level

VRAGEN OF OPMERKINGEN ?

