

BASF Veiligheidsfilosofie, gevolgen van IEC61508 en IEC61511

Symposium “SIPI, safety in de proces industrie”

6 november 2003, Ter Elst Edegem

Michel De Lannoy

Jan Luyts

BASF-producten zijn alomtegenwoordig

**Geneeskunde
& verzorging**



**Communicatie &
informatica**



**Sport &
vrije tijd**

**BASF...
een brede
waaier van
producten**

Verkeer



**Voedsel-
voorziening**

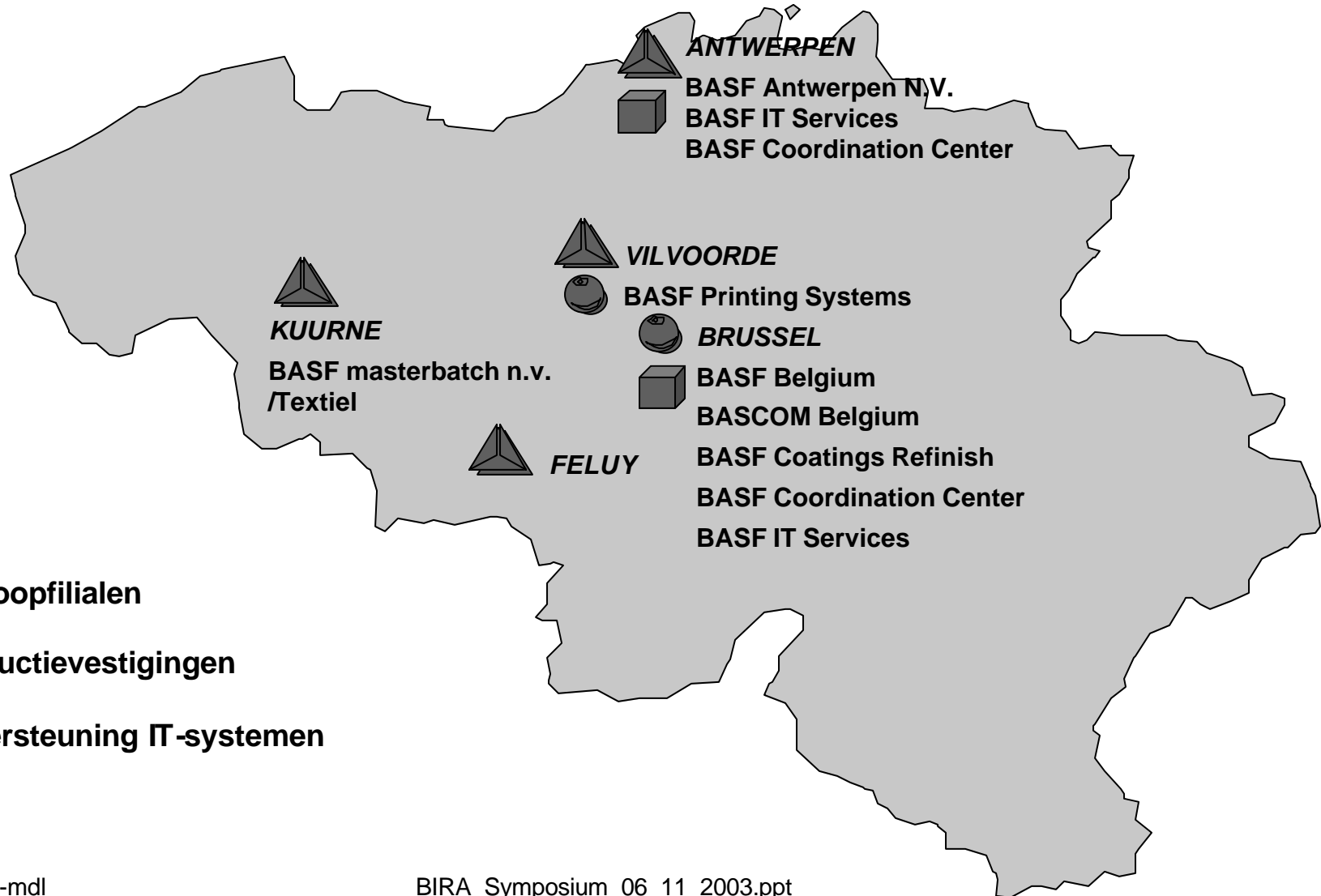


Bouw



BASF in België

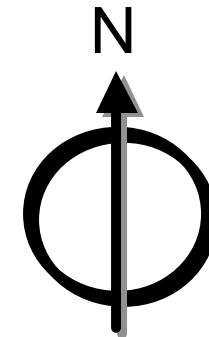
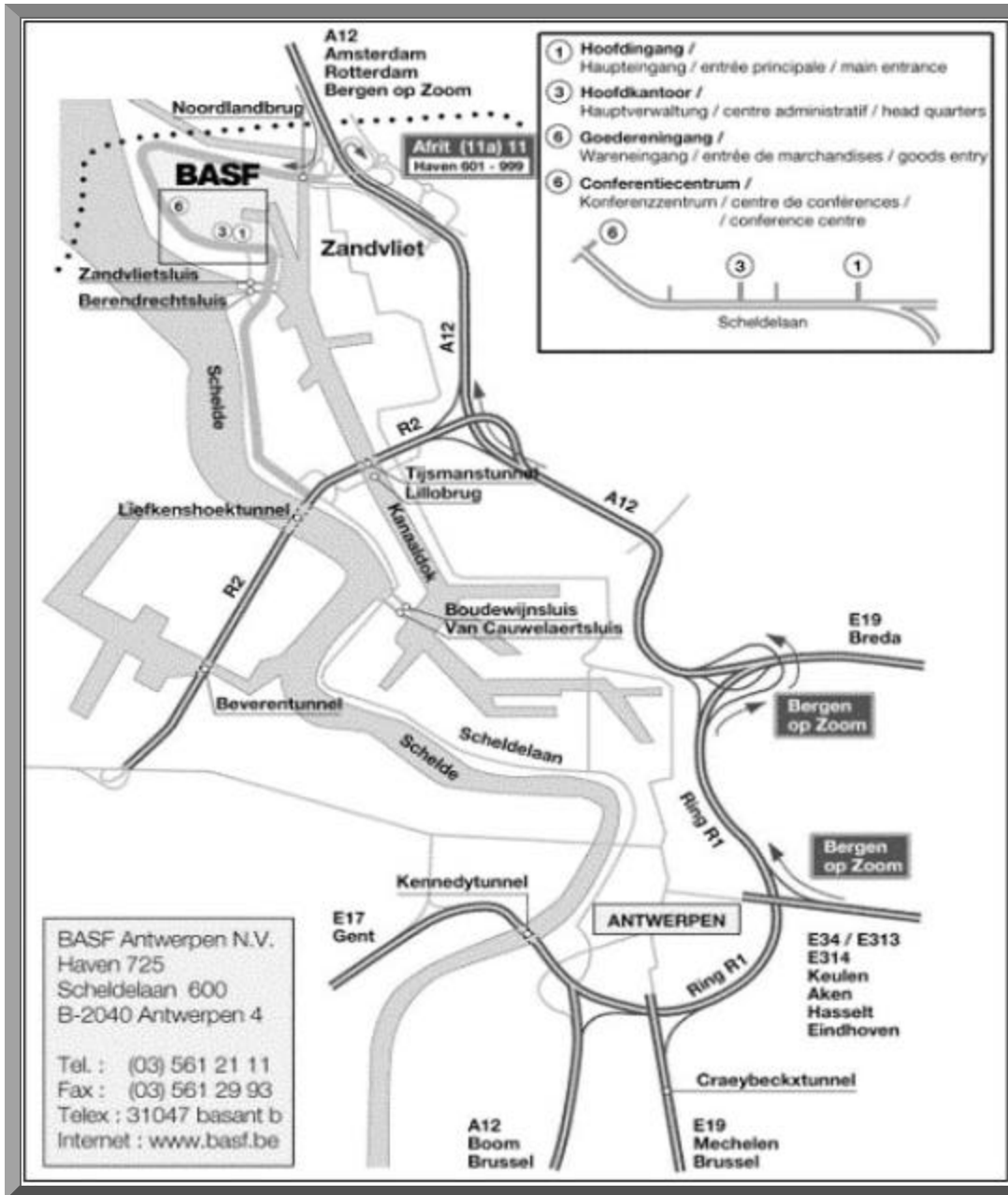
(2002)



BASF in België 2002

		omzet (in mln euro)	aantal medew.
productiecentra:	BASF Antwerpen N.V. BASF Site Feluy	} 3.191,9	3.676
verkoopcentrum:	BASF Belgium N.V.	529	127
Coördinatiecentrum:	BASF Coordination Center N.V.	11,31	43
IT-vennootschap:	BASF IT Services N.V.	18,44	114

BASF



In het meest noordelijke punt van de Antwerpse Haven

Infrastructuur

totale oppervlakte.....	598 ha
daarvan bebouwd.....	60%
aantal installaties.....	54
capaciteit silo's.....	446.000 t
kaailengte.....	4.551 m
wegen.....	152 km
spoorwegen.....	41 km
bovengrondse leidingen.....	290 km
ondergrondse drukleidingen.....	230 km

Geïntegreerd productiecentrum

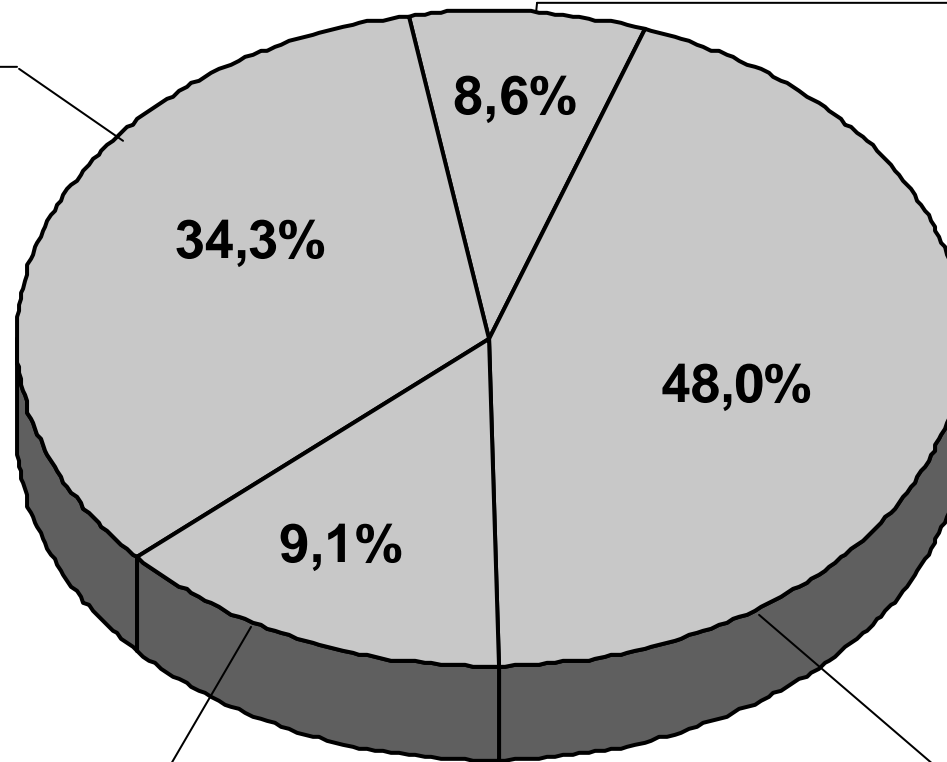
(54 productie-eenheden in 4 productiesectoren)

	BASF-producten	Toepassingen
Meststoffen & Anorganica	nitrofosforzuur, salpeterzuur, ammoniak, zwavelzuur samengestelde en enkelv.meststoffen	meststoffen
Kunststoffen en vezelproducten	polyurethaangrondstoffen, polystyreen, ethylbenzeen/styreen, Styrolux [®] , caprolactam, cyclohexanon, hydroxilamine...	huishoudtoestellen, speelgoed, sportartikelen, isolatiemateriaal, verpakkingsmateriaal, zetels, auto-onderdelen, tapijten, tandenborstels, nylonkousen...
Veredelingsproducten	ethyleenoxide, glycolen, tensiden, acrylzuur/acrylaten, SAP	antivriesmiddelen, detergenten, PET-flessen, ...
Chemicaliën en andere producten	ethyleen, propyleen, benzeen, pyrolysebenzine, PIB, formaldehyde, amines	gewasbeschermingsmiddelen, farmaceutische producten, additieven voor brandstoffen en smeeroliën, ...

Omzet per productiesector 2002

Chemicaliën en
andere producten

Meststoffen



Veredelingsproducten

Kunststoffen en
vezelproducten

Sustainable Development Responsible Care

Sustainable Development - *Duurzame ontwikkeling*

Doel is,

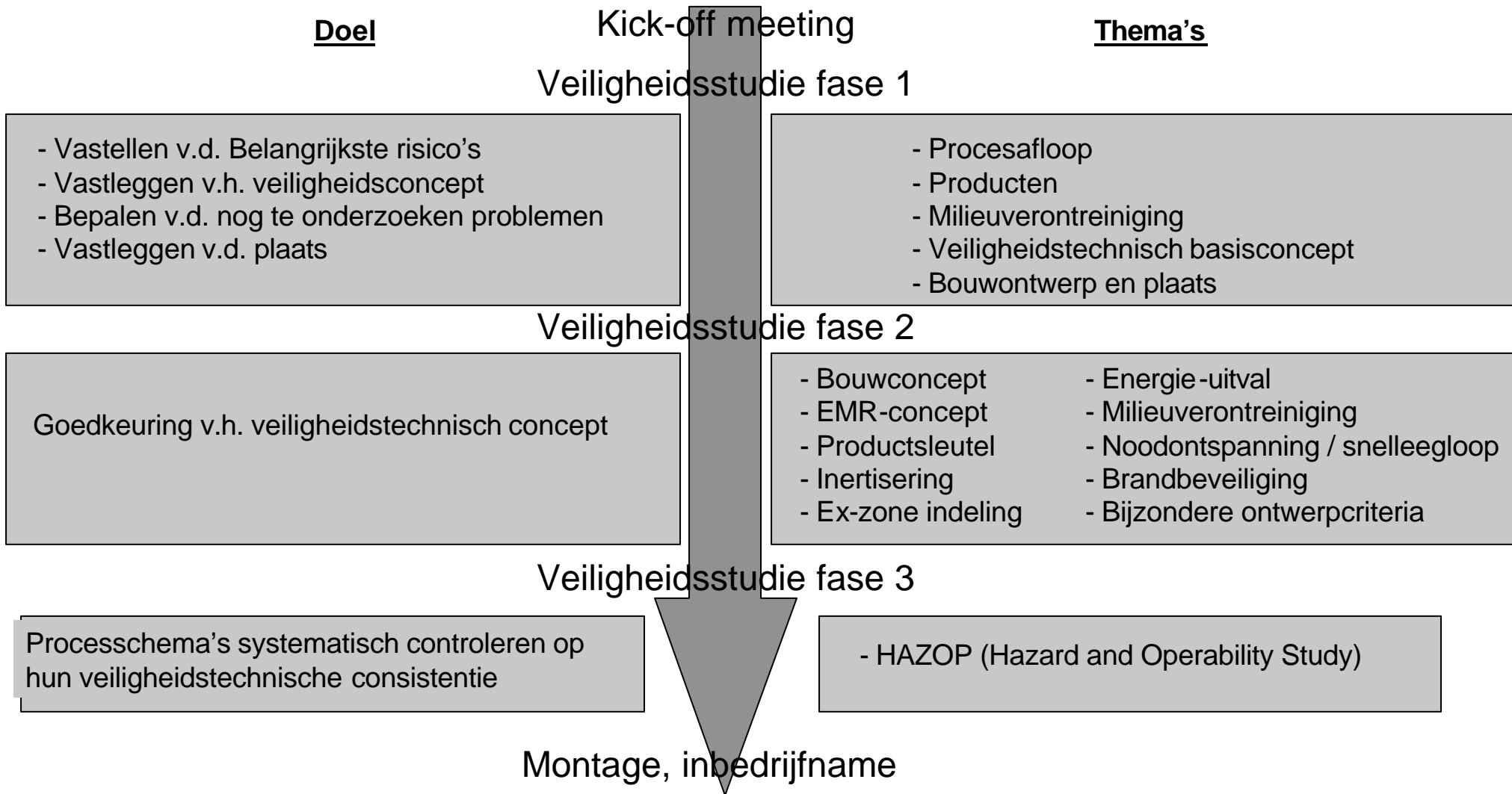
- aan de economische, ecologische en sociale behoeften van de actuele maatschappij te voldoen.
- De toekomstige generaties de mogelijkheid tot vrije ontplooiing te blijven bieden.

Responsible Care - *verantwoord handelen*

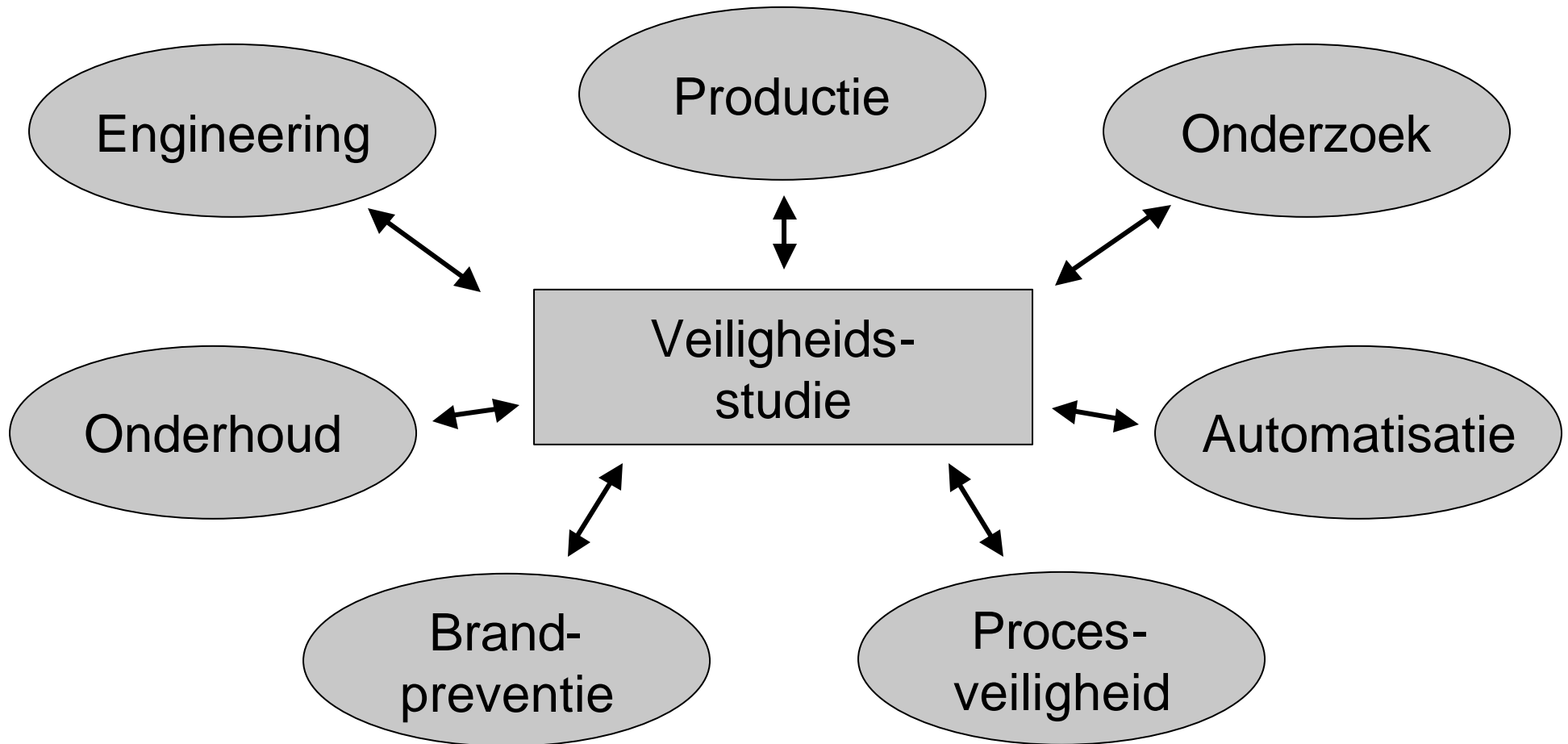
Doel is de voortdurende verbetering van

- milieubescherming
- veiligheid
- gezondheidszorg

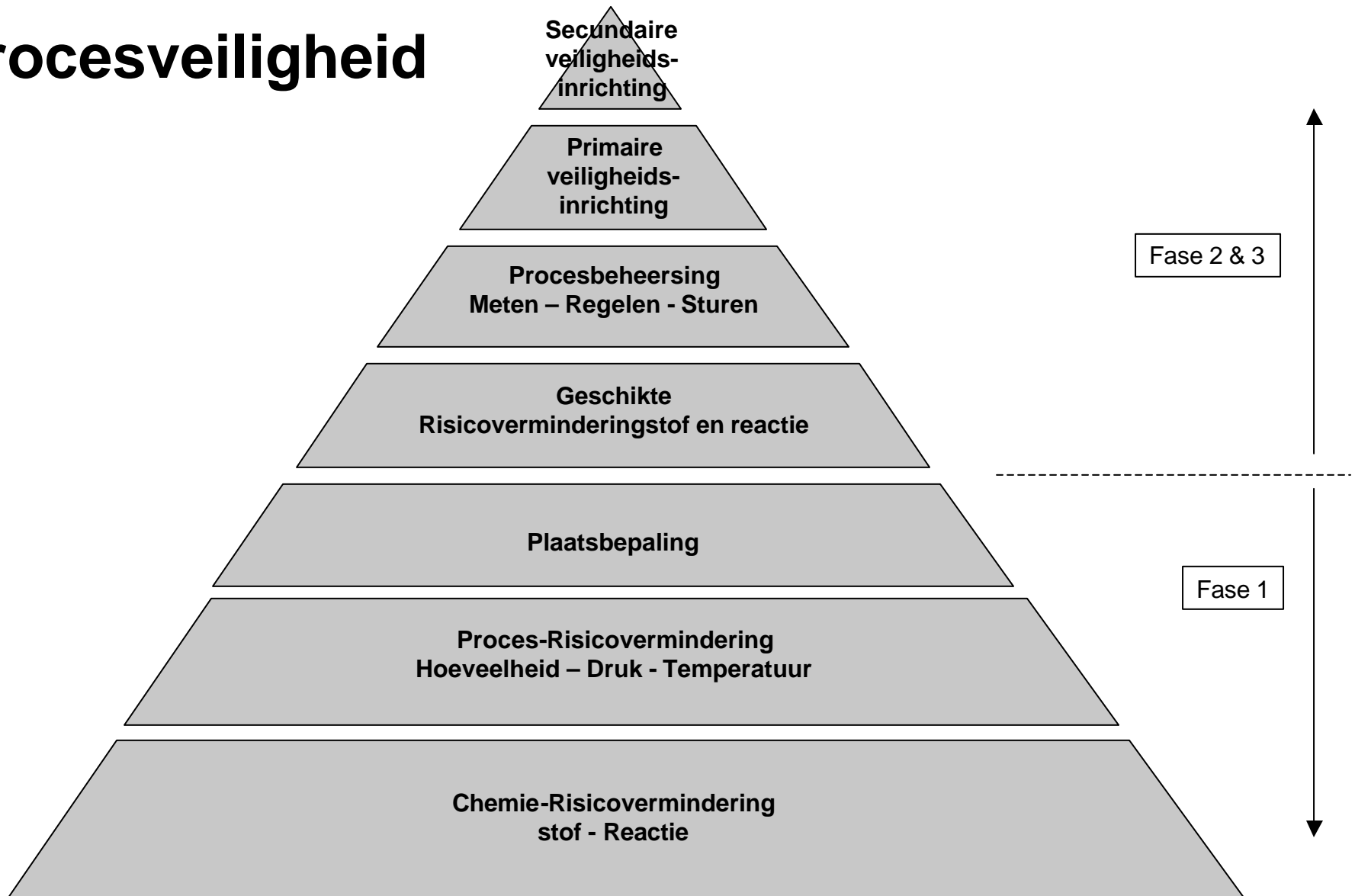
Veiligheidsstudies



Team



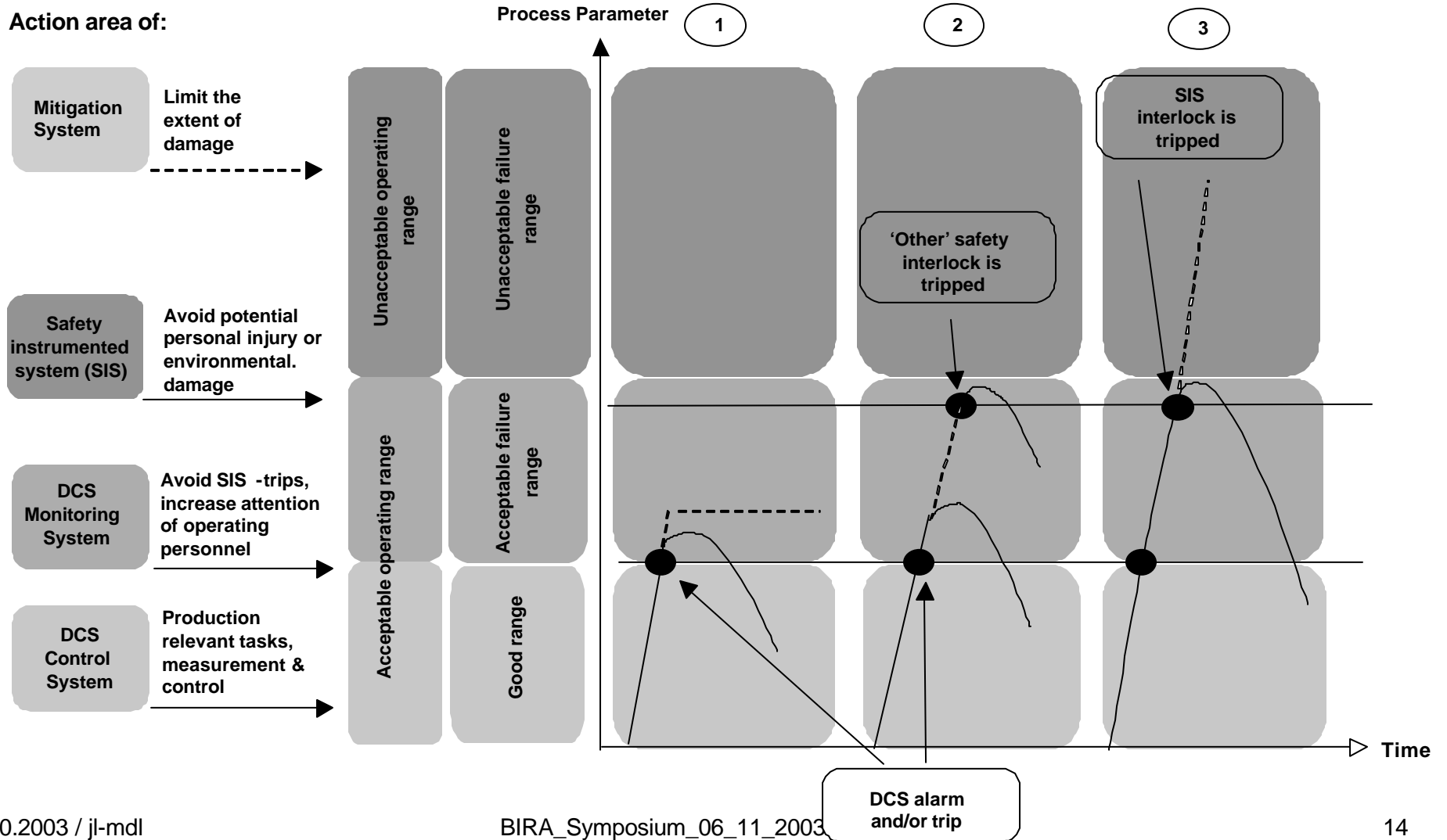
Procesveiligheid



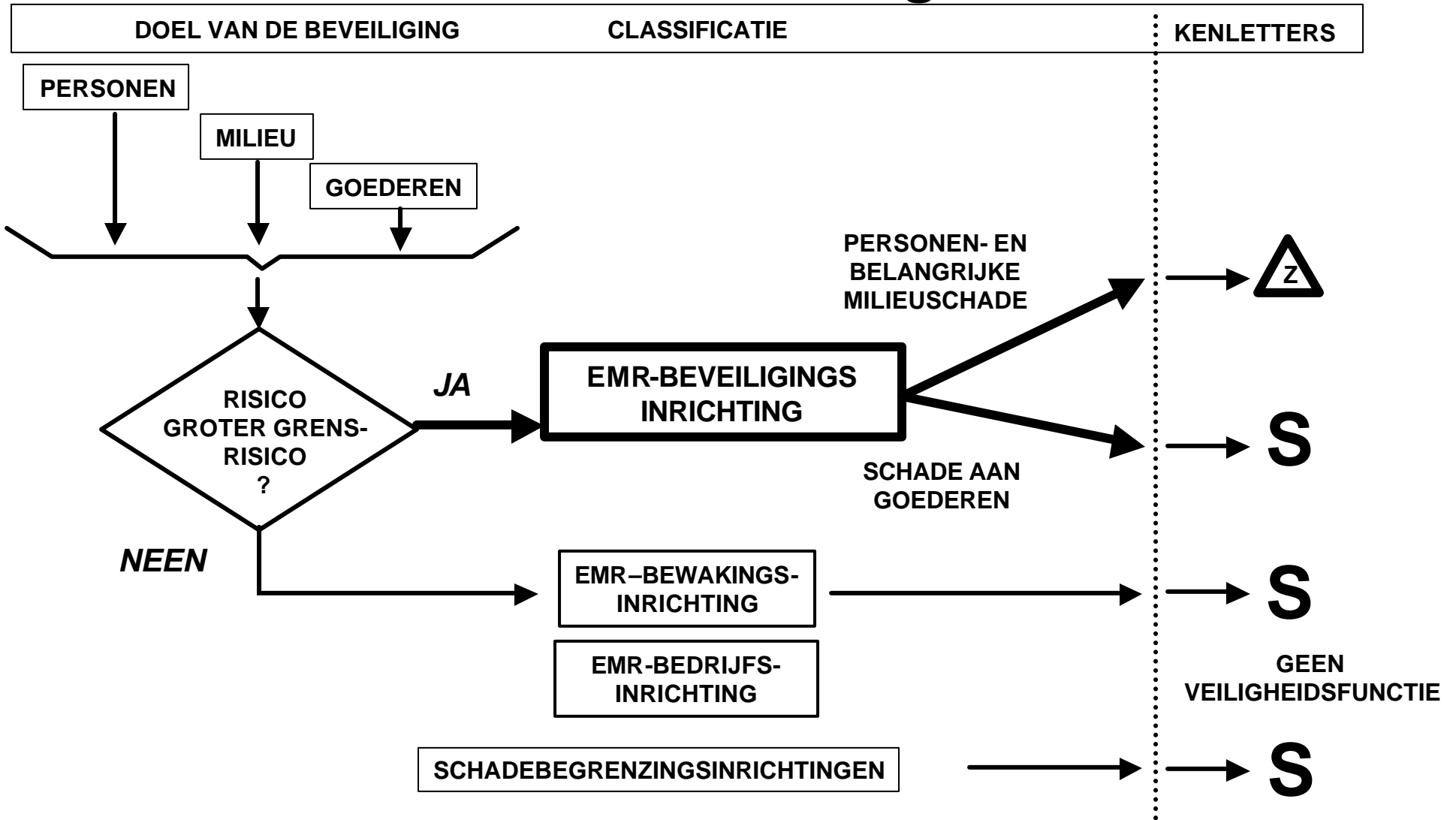
Voor IEC61508 & IEC61511

- RPI10 (Richtlinien für Planung und Instandhaltung):
 - › Gebaseerd op:
 - » VDI/VDE 2180 “Sicherung von Anlagen der Verfahrenstechnik”
 - » NE31 “Anlagensicherung mit Mitteln der Prozessleittechnik”
 - » DIN19250 “Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen”
 - » Andere erkende normen en richtlijnen
 - › De RPI10 heeft voor alle Europese BASF-dochterondernemingen een bindend karakter
 - » Verplichting
 - » Sterk aanbevolen
 - › Kwalitatieve benadering
 - NE = “NAMUR Empfehlung” NAMUR = “Norm Ausschuss Mess- und Regelungstechnik”

Classificatie volgens VDI/VDE 2180



Classificatie van EMR-inrichtingen



Vermijden en beheersen van passieve (functieremmende) fouten

LIJST VAN PASSIEVE FOUTEN

VERMIJDEN

- Gekeurde toestel- en installatietechniek
- Fail-safe-concept
 - ruststroomprincipe
 - stelorganen met veerterugstelling
- Construeren / voorzien voor verhoogde eisen overdimensionering
- Afgeschermd installatie

BEHEERSEN

Fouten herkennen	Tolereerbaar maken	Organisatorische maatregelen
<ul style="list-style-type: none"> <input type="checkbox"/> Automatisch melden van fouten <input type="checkbox"/> Zichzelfbewakende toesteltechniek <input type="checkbox"/> Gebruik van beveiligings-inrichtingen als bedrijfs-inrichtingen 	<ul style="list-style-type: none"> <input type="checkbox"/> Redundante instrumentering en installatie <input type="checkbox"/> Homogene/ diversitaire redundantie 	<ul style="list-style-type: none"> <input type="checkbox"/> Controle door operators, bv. Plausibiliteitstest <input type="checkbox"/> Regelmatig terugkerende functietest volgens VDI/VDE 2180

BASF Veiligheidsfilosofie, gevolgen van IEC61508 en IEC61511

- Procesveiligheid
- Instrumentatie

Instrumentele beveiligingen

Impact van IEC 61508 / 61511

Deel 1 - Procesveiligheid



General Requirements for Chemical Plants

BASF Group Directive

**Safety, Health and Environmental Protection (SHE)
at Planning and Construction of Process Plants**

(Competence Center Responsible Care)

General Requirements for Chemical Plants Basis

De vernieuwde “SHE”-richtlijnen zijn gebaseerd op:

- IEC 61508: “Functional Safety of electrical/electronic/programmable electronic safety related systems”
- IEC 61511: “Functional safety: Safety instrumented systems for the process industry sector”
- Men bespreekt de levenscyclus van de functies

In concreto - Nieuw

- Tot nu toe werd er enkel kwalitatief gewerkt, men zal nu ook kwantitatief te werk moeten gaan
- Men heeft een methodiek ontworpen om tijdens een veiligheidsstudie een risico-inschatting uit te voeren en het toepasselijk SIL-klasse te bepalen

→ “BASF Risico Matrix”

- Men zal moeten aantonen dat de veiligheidsrelevante beschikbaarheid van de instrumentele beveiligingsinrichting voldoet aan de opgelegde SIL

Pressure equipment directive (PED) - Nieuw

- Geldigheidsbereik van PED (DGRL 97/23/EG) :
 - › Deze richtlijn geldt bij het uitleggen, vervaardigen en het beoordelen van de conformiteit van drukapparatuur met een toegelaten druk van meer als 0,5 bar.
 - › Drukapparatuur in dit kader zijn vaten, buisleidingen en drukhoudende uitrustingsdelen (armaturen, ventielen, instrumentele-apparatuur met drukhoudend huis,...), evenals uitrustingsdelen met veiligheidsfunctie (breekschijven, veiligheidskleppen en instrumentele-veiligheidsinrichtingen)
- De regelgeving van PED met betrekking tot instrumentele beveiliging werd opgenomen in de richtlijnen

De KWM-studies

- Wij hadden:

KWM studie fase 1, 2 en 3 waarin de instrumentele beveiligingsinrichtingen werden vastgelegd

- Nieuw:

KWM-studie fase 4 : Controle van de implementatie voor opstart

Vastleggen van de instrumentele beveiligingsinrichtingen - Nieuw

- Van ieder potentiële gebeurtenis: risico-inschatting → risicoklasse
 - Voor elke instrumentele beveiliging : SIL-klasse
 - De PED-relevantie wordt voor iedere beveiligingsfunctie vastgelegd
 - De testperiodiciteit wordt vastgelegd
 - De nodige beschikbaarheid van het bedrijf wordt vastgelegd
- Er wordt een dossier samengesteld die de basis zal vormen voor de verdere designfase.

Eerste inbedrijfsnamecontrole - Nieuw

- Nazicht en controle van de implementatie van de concepten - opbouw versus SIL - vóór inbedrijfname
- Controle van de aanwezigheid van de nodige documentatie
- Controle van de conformiteits-verklaring en - attesten(PED)

Risico-inschatting - Nieuw

De internationale veiligheidsdienst van BASF heeft een concept ontwikkeld voor risico-inschatting:

“The BASF Risk Matrix”

Dit is een semi-kwantitatieve methode waarin:

Risico = Waarschijnlijkheid x Ernst

→ Hieruit volgen de risicoklassen

BASF Risicomatrix - Nieuw

Risk Matrix

	Risk Matrix			
Probability	Severity			
	S ₁	S ₂	S ₃	S ₄
P ₀	A	B	D	E
P ₁	A/B*	B	E	E
P ₂	B	C	E	F
P ₃	C	D	F	F
P ₄	E	F	F	F

* Determined on a case by case basis decision whether A or B is needed

Probability:

P ₀ : Happened a couple of times	1/year or more often
P ₁ : Happened once	Approx. 1/10 years
P ₂ : Almost happened, near miss	Approx. 1/100 years
P ₃ : Never happened, but is thinkable	Approx. 1/1000 years
P ₄ : Not plausible	Less than 1/10000 years

Severity:

- S₁: On site: potential for one or more fatalities
- S₂: On site: potential for one or more serious injuries (irreversible)
- S₃: On site: potential for one or more lost time injuries
- S₄: On site: potential for minor injuries, or irritation

Risicoklasse en het vastleggen van de SIL - Nieuw

<u>Risicoklasse</u>	<u>Risico niveau</u>	<u>Risico reductie</u>	<u>SIL</u>
A	Extreem, totaal onaanvaardbaar	Wordt niet gebouwd bij BASF → Verandering van het ontwerp of proces noodzakelijk	4
B	Zeer groot, onaanvaardbaar risico	Verandering van het ontwerp of proces, of een mechanische veiligheidsinrichting of een Instrumentele beveiligingsinrichting	3
C	Groot, onaanvaardbaar risico	Verandering van het ontwerp of proces, of een mechanische veiligheidsinrichting of een Instrumentele beveiligingsinrichting	2
D	Medium, accepteerbaar risico dat verder onderzocht moet worden	Een Instrumentele bewakingsinrichting van hoge kwaliteit met gedocumenteerde testen of een organisatorische maatregel volgens procedure van hoge kwaliteit	(1)
E	Klein accepteerbaar risico, dat eventueel verder onderzocht moet worden	Een Instrumentele bewakingsinrichting of een organisatorisch maatregel via een procedure	(1)
F	Zeer klein, accepteerbaar risico	Geen. Dit zijn de Instrumentele bedrijfsinrichtingen	(1)

Opmerking : SIL 1 wordt bij BASF niet gebruikt

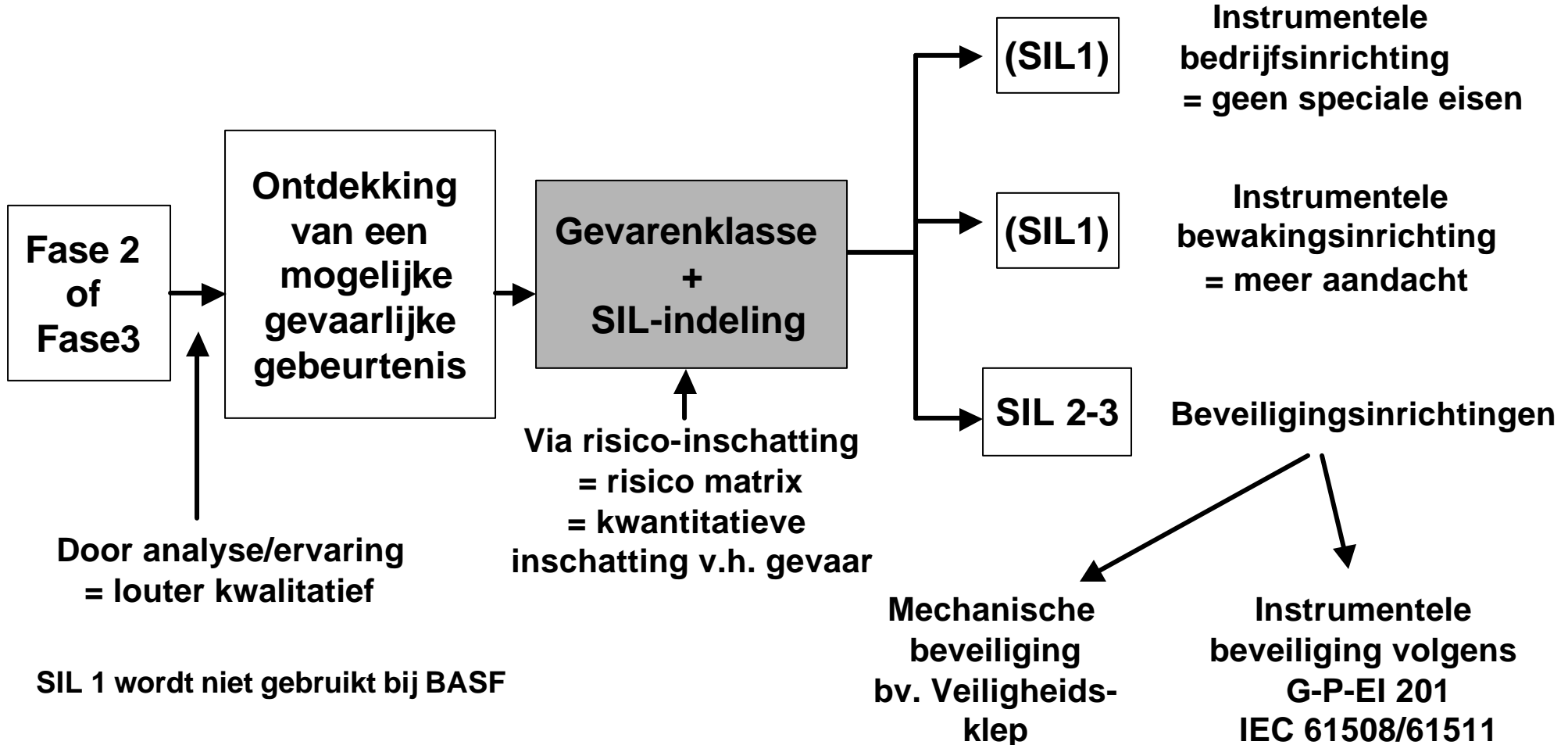
Prioriteit van de maatregelen

Nu nog geldt wat betreft de prioriteit van de risicoreducerende maatregelen (in volgorde van belang) :

- Proces of ontwerp intrinsiek veilig (bv. Andere chemische stoffen)
- Passief ontwerpelementen (bv. Drukvast ontwerp)
- Mechanische beveiligingsinrichtingen (bv. Veiligheidsklep)
- Instrumentele beveiligingsinrichtingen

Ontstaan van een procesbeveiliging

Volgens de nieuwe richtlijnen



Instrumentele beveiligingen Impact van IEC 61508 / 61511

Deel 2 – Instrumentatie



Classificatie van de instrumentele-inrichtingen

Men onderscheidt :

- bedrijfsinrichtingen
- bewakingsinrichtingen
- Schadebegrenzingsinrichtingen
- beveiligingsinrichtingen

De classificatie is deze van VDI / VDE 2180 (niet veranderd)

Beveiligingsinrichtingen

Dit zijn de SIL 2 en SIL 3 inrichtingen

- Ze voorkomen een gevaarlijke situatie in het proces
- Ze worden opgebouwd in een separaat hoogwaardig systeem
- De aanspreekfrequentie van deze functies moet zeer laag blijven
- Zij, en zij alleen zijn onderworpen aan de vernieuwde richtlijnen

Foutengedrag van een systeem (IEC)

Soorten fouten

Men onderscheidt:

- Veilige fouten: (= Actieve fouten) Fouten die zich manifesteren en actief het systeem in veiligheid brengen
- Gevaarlijke fouten: (= Passieve fouten) Fouten die zich niet manifesteren en het veilig gedrag van het systeem tegenwerken

Foutengedrag van een systeem (IEC)

Invloed van de verschillende fouten

Invloed op de beveiligingsinrichting	
Veilige fouten	Onveilige fouten
<ul style="list-style-type: none"> • (Af)schakeling spreekt ten onrechte aan (= “spurious trip”) • Installatie gaat in een veilige toestand <p>→ Vermindering van de Beschikbaarheid</p>	<ul style="list-style-type: none"> • (Af)schakelfunctie wordt geblokkeerd • Installatie draait verder ook indien een (af)schakeling noodzakelijk zou zijn <p>→ Vermindering van de Veiligheid</p>

Foutengedrag van een systeem (IEC)

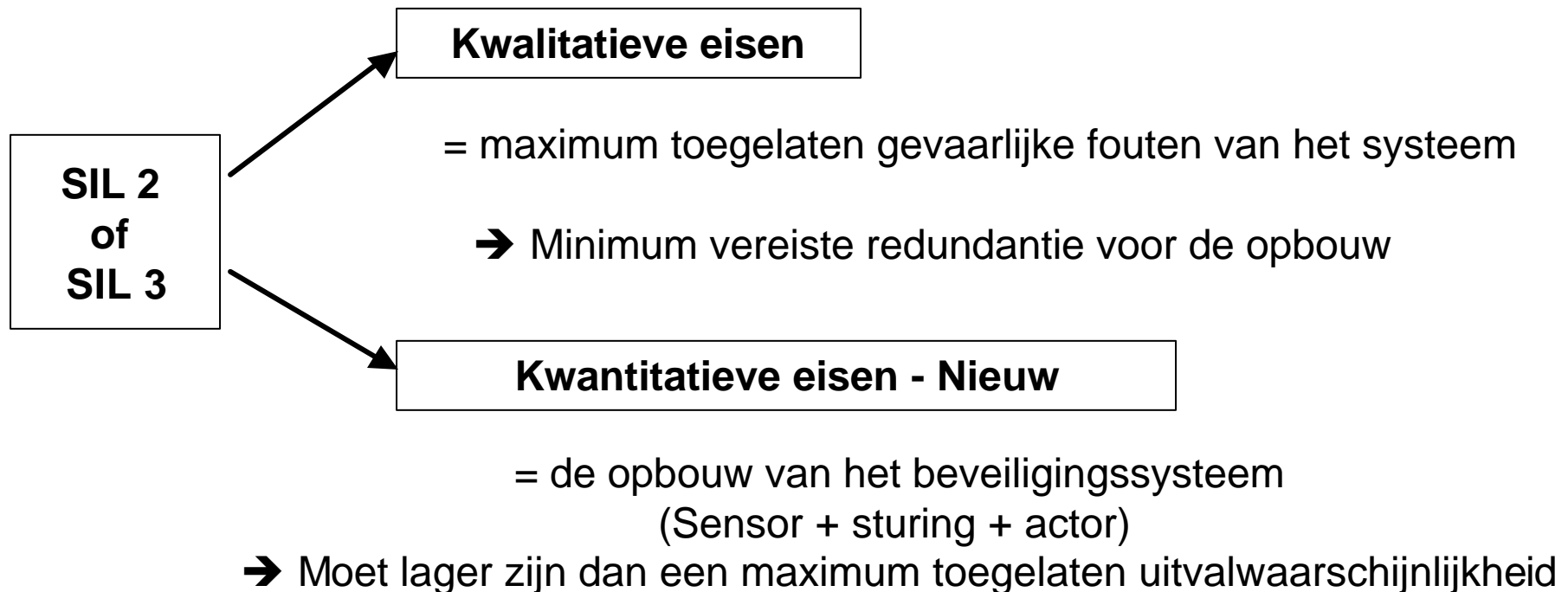
Te volgen doel

Het doel dat nagestreefd moet worden is het opsporen van gevaarlijke fouten

Dit wordt gerealiseerd door:

- Analyse in de designfase
- Automatische foutdetectie in het systeem
- Periodieke functietesten van het geheel, zonder nieuwe systematische fouten in te brengen

Kwalitatieve eisen versus kwantitatieve eisen (IEC)



Kwalitatieve eisen van SIL (IEC)

Fouttolerantie

Fouttolerantie van een systeem

- De hoogste SIL van een systeem wordt beperkt door de hardware fouttolerantie van de subsystemen.
- De hardware fouttolerantie (X) van een functionele unit is de mogelijkheid om verder de functie te kunnen garanderen in de aanwezigheid van X fouten.
- Het gaat om gevaarlijke fouten !

Kwalitatieve eisen van SIL (IEC)

Aantal gevaarlijke fouten

Aantal gevaarlijke fouten	Betekent	Architectuur
0	1 fout geeft een gevaarlijke toestand	1v1
1	1 fout en het systeem is nog veilig	1v2 of 2v3
2	2 fouten en het systeem is nog veilig	1v3
3	3 fouten en het systeem is nog veilig	1v4

Kwalitatieve eisen van SIL (IEC)

A-, B-, proven in use toestellen

- A-toestellen: gedrag bij fouten bekend. Eenvoudige analoge techniek → lagere eisen
- B-toestellen: gedrag bij fouten minder bekend. Complexere toestellen, microprocessor gestuurde toestellen → hogere eisen
- “Proven in use”: toestellen die zich bewezen hebben
- IEC 61511 laat het gebruik toe van “proven in use” toestellen. Een proven in use B-toestel kan beschouwd worden als een A-toestel waardoor de eisen naar de architectuur toe verminderen.

Kwalitatieve eisen van SIL (IEC)

Hardware fouttolerantie

SFF (safe failure fraction)	Hardware fouttolerantie		
	0 (A/B) (1v1)	1 (A/B) (1v2 of 2v3)	2 (A/B) (1v3)
Geen (< 60%)	SIL 1 / Verboden	SIL 2 / SIL 1	SIL 3 / SIL 2
Laag (60% - 90%)	SIL 2 / SIL 1	SIL 3 / SIL 2	SIL 4 / SIL 3
Medium (90% - 99%)	SIL 3 / SIL 2	SIL 4 / SIL 3	SIL 4 / SIL 4
Hoog (> 99%)	SIL 4 / SIL 3	SIL 4 / SIL 4	SIL 4 / SIL 4

SFF laag = klassiek in ruststroomprincipe opgebouwd systeem

SFF = verhouding van het aantal veilige fouten tot het totaal aantal fouten

Kwantitatieve eisen van SIL (IEC)

$$PFD_{AVG} = \lambda$$

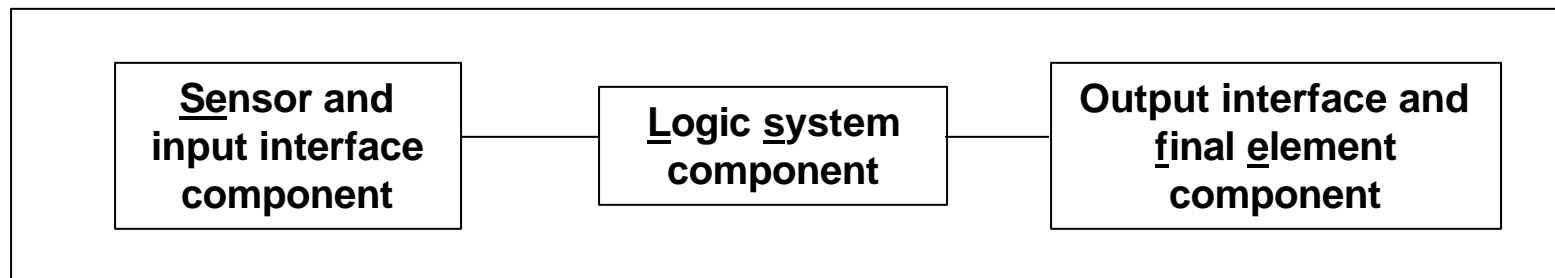
SIL	Weinig belaste bedrijfswijze ("on demand mode") Gemiddelde uitvalwaarschijnlijkheid van de functie bij werking (PFD_{AVG})	Sterk belaste bedrijfswijze of continu belast ("continuous mode") Waarschijnlijkheid van een gevaarlijke uitval per uur (?)
4	$10^{-5} = PFD_{AVG} = 10^{-4}$	$10^{-9} = 1 = 10^{-8}$
3	$10^{-4} = PFD_{AVG} = 10^{-3}$	$10^{-8} = 1 = 10^{-7}$
2	$10^{-3} = PFD_{AVG} = 10^{-2}$	$10^{-7} = 1 = 10^{-6}$
1	$10^{-2} = PFD_{AVG} = 10^{-1}$	$10^{-6} = 1 = 10^{-5}$

Instrumentele beveiligingsinrichtingen vallen meestal onder de "on demand mode"

Kwantitatieve eisen van SIL (IEC)

Invloeden

Een volledig systeem ziet er in principe als volgt uit:



Voor ieder subsysteem (element) houdt men rekening met:

- De architectuur (bv. 2 van 3 structuur)
- De foutdetectiegraad DC (“Diagnostic Coverage”)
- De faalwaarschijnlijkheid van de elementen λ
- Het aandeel aan gemeenschappelijke fouten b (“Common Cause Failure”)
- Het testinterval T_I

Kwantitatieve eisen van SIL (IEC)

Berekeningen (1)

- Men berekent de totale faalwaarschijnlijkheid van ieder subelement (Sensor – Logic System – Final element)
- Dit noemt men de “Probability of failure on demand = PFD”

$$\begin{array}{l} \rightarrow \text{PFD}_{SE} = \sum \lambda_i \\ \text{PFD}_{LS} = \sum \lambda_i \\ \text{PFD}_{FE} = \sum \lambda_i \end{array} \quad \begin{array}{l} \rightarrow \\ \rightarrow \\ \rightarrow \end{array} \quad \begin{array}{l} \text{som van alle faalfrequenties van de} \\ \text{verschillende componenten} \end{array}$$

- Hieruit volgt de gemiddelde faalwaarschijnlijkheid voor het systeem

$$\text{PFD}_{AVG} = \sum \text{PFD}_{SE} + \sum \text{PFD}_{LS} + \sum \text{PFD}_{FE}$$
- PFD_{AVG} moet aan de vereiste SIL-klasse voldoen

Kwantitatieve eisen van SIL (IEC)

Berekeningen (2)

- Deze PFD - berekeningen worden bij het ontwerp van de beveiliging gemaakt en worden later bevestigd met het statistisch materiaal verzameld in de loop der jaren
- De berekeningen eisen een volledig nieuwe aanpak:
 - › Men moet over exacte statistische data beschikken en deze zijn zelden aanwezig daar het medium in de welke een instrument werkt bepalend is voor zijn betrouwbaarheid.
 - › Ieder project moet apart berekend worden
 - › Tijdrovend, hoge kosten, niet praktisch

➔ BASF besloot over te gaan naar standaard oplossingen

Standaard oplossingen

Eerste stap

Inzet van betrouwbare instrumentatie

- Doelbewuste keuze van toestellen :
- › Sturing: Gecertificeerd SIL 3
 - › Instrumenten: Gestandaardiseerd = “proven in use”
 - › Onze standaard toestellen:
 - » Getest in labo
 - » Minimum één jaar praktische ervaring in industriële omgeving met een relevant aantal exemplaren

Standaard oplossingen

Tweede stap

Maatregelen treffen die tot automatische foutdetectie leiden met als doel :

- “Conservatief” statistisch materiaal te gebruiken in plaats van exacte data daar deze laatste op het ogenblik ontbreken
- De testintervallen te maximaliseren

Standaard oplossingen

Inschatting, maximalisatie van het testinterval

Men weet dat :

$$\rightarrow \text{PFD}_{\text{AVG}} = f(l^{\text{DU}}, \text{TI}, b)$$

indien men ervan uit gaat dat de niet ontdekte fouten alle gevaarlijke fouten zijn, wat een conservatieve benadering is dan :

$$l^{\text{DU}} \gg l^{\text{U}} \rightarrow l^{\text{DU}} \gg l^{\text{U}} = l \cdot (1 - \text{DC}) \text{ en } \text{SFF} = \text{DC}$$

$$\rightarrow l^{\text{DU}} = l \cdot (1 - \text{SFF}) = (1/\text{MTBF}) \cdot (1 - \text{SFF})$$

$$\rightarrow \text{PFD}_{\text{AVG}} = f(\text{MTBF}, \text{SFF}, \text{TI}, b) - \text{conservatief}$$

Bij het vastgelegde SIL is $\text{PFD}_{\text{AVG}} = \text{cte}$; $b = \text{cte}$ (kan goed ingeschat worden)

$$\rightarrow \text{TI} = f(\text{MTBF}, \text{SFF}) - \text{conservatief}$$

= basis voor de “Typicals”

→ MTBF meestal bekend en hoog vermits standaard “proven in use”

→ SFF moet zo groot mogelijk zijn wat betekent dat zoveel mogelijk gevaarlijke fouten gedetecteerd moeten worden

“Typicals”

- Keuze van een typical in functie van: de opgelegde SIL, en de beschikbaarheid van het bedrijf
- Testinterval kan door middel van automatische foutdetectie tot 5 jaar verhoogd worden.
- Automatische foutdetectie wordt gerealiseerd door software die de verschillende metingen bewaakt, zoals :
 - Onderlinge verschillen, het niet meer “leven” van het signaal, enz... Deze worden in eerste instantie gealarmeerd en kunnen eventueel in tweede instantie tot een afschakeling leiden
- Opmerking : Een hoge automatische foutdetectie is enkel mogelijk indien de metingen ANALOOG in de veiligheidssturing binnen komen!

Formele organisatorische maatregelen (IEC)

De norm eist ook organisatorische maatregelen voor de verschillende acties in de levenscyclus van de beveiliging waarvan wij de volgende verscherpt hebben :

- Opstellen van een grondig dossier over de beveiligingen (wat, waarom, hoe, ...)
- Goede definitie van de verantwoordelijkheden en de “workflows”
- Testspecificaties (vooral bij de eerste inbedrijfname)
- Opbouw van een databank (statistiek)
- Systematisch toepassen van het “4-ogen” principe
- Validaties en extra studies voor complexe functies met eventueel tussenkomst van experts volgens het V-model
- Audits over de materie in alle vestigingen
- Opleiding en sensibilisatie acties

Kosten

- Analyse van de norm, uitwerken van alle technische en organisatorische aspecten ervan
- Opstellen / uitwerken van een volledige vernieuwde richtlijn op groepsniveau
- Invoeren van de nieuwe richtlijnen, invoeren van nieuwe “workflows”
- Mensen opleiden
- Organiseren van interne audits om de huidige toestand te toetsen met de gewenste toekomstige toestand en hieruit eventueel acties voorzien

Baten

- Betere totale conceptuele aanpak van de materie
- Door een grondige analyse van de mogelijkheden is men op een verscherpte standardisatie beland
- Optimalisatie van opbouw en testintervallen gesteund op een kwantitatieve en korrektere benadering dan in het verleden
- Aanpak is pragmatischer dan eerst gedacht
- De audits hebben aangetoond dat wij destijds met onze zuivere kwalitatieve aanpak architecturen hebben opgebouwd die de berekeningen kunnen doorstaan