KIVI Engineering Society Afdeling Meet-, Regel- en Besturingstechnologie CONSILTANT

Presentatie over

Procesveiligheid

- SIL

Ede, 9 juni 2016

Programma

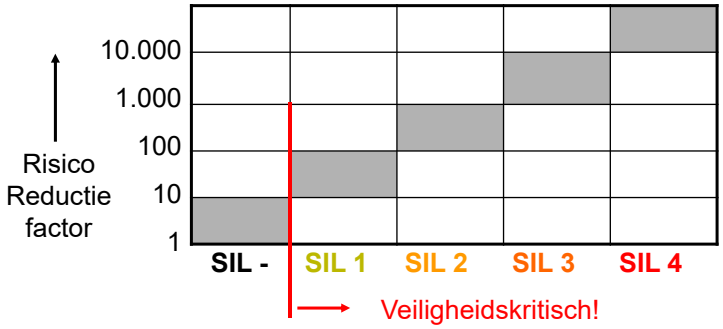
CONSILTANT

18:00 uur	Ontvangst met koffie/thee en broodjes
18:30 uur	Procesveiligheidsontwikkeling/HAZOP en LOPA
19:15 uur	Pauze
19:45 uur	SIL volgens IEC 61511 editie februari 2016
20:30 uur	Afsluiting met een drankje

Procesveiligheid: SIL 2

SIL

SIL (*Safety Integrity Level)* (-, 1, 2, 3, 4) geeft de betrouwbaarheid weer van een beveiliging



Procesveiligheid: SIL 3

SIL normen

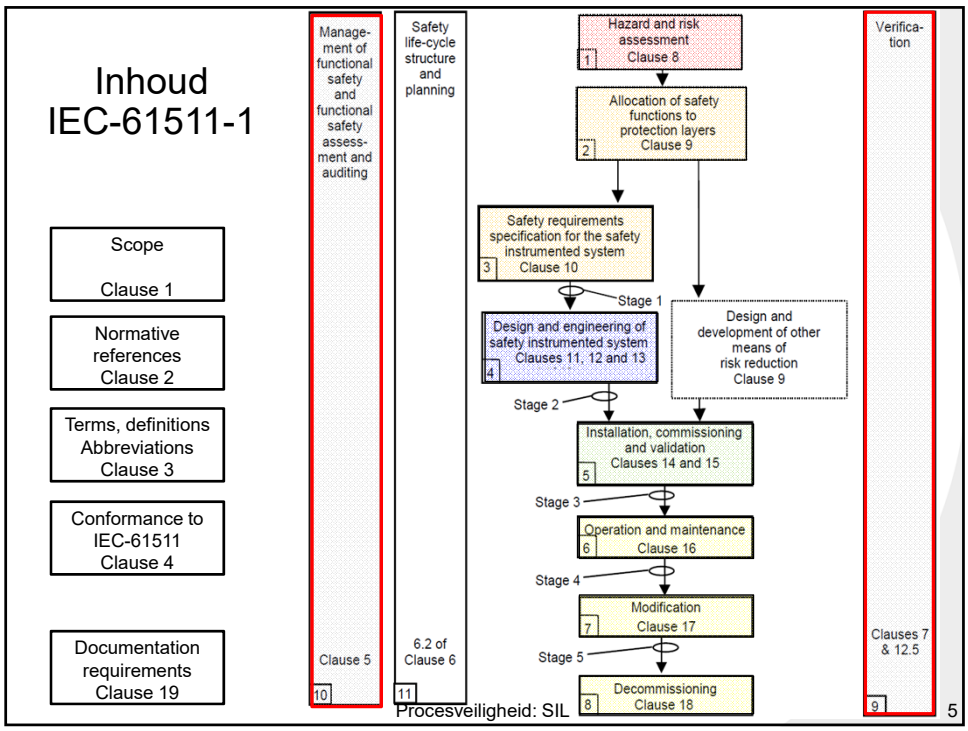
IEC 61511 *Proces industrie*

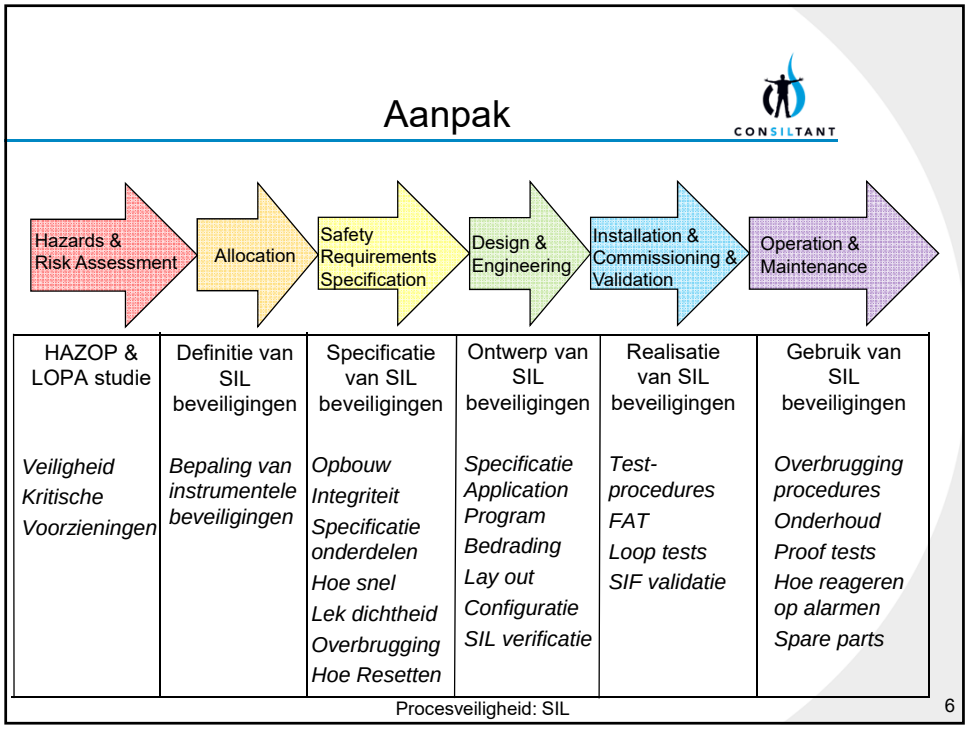
- Deel 1 - Algemene eisen *Normatief*
- Deel 2 – Guidelines for the application of IEC-61511-1
- Deel 3 – Guidance for determination of the required SIL

IEC 61508 *Algemeen*

- Deel 1 - Algemene eisen *Normatief*
- Deel 2 - Richtlijnen voor 'beveiligingen' (hardware) *Normatief*
- Deel 3 - Eisen voor programmatuur (software) *Normatief*
- Deel 4 - Definities en afkortingen
- Deel 5 - Voorbeelden 'SIL classificatie' methoden
- Deel 6 - Richtlijnen voor toepassing van deel 2 en 3
- Deel 7 - Overzicht van technieken en voorzieningen

Procesveiligheid: SIL 4


Inhoud
IEC-61511-1
Scope
Clause 1
Normative references
Clause 2
Terms, definitions
Abbreviations
Clause 3
Conformance to IEC-61511
Clause 4
Documentation requirements
Clause 19
Manage-ment of functional safety and functional safety assess-ment and auditing
Clause 5
10
Safety life-cycle structure and planning
6.2 of Clause 6
11
Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clause 10
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11, 12 and 13
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Verifica-tion
Clauses 7 & 12.5
9
Procesveiligheid: SIL
5

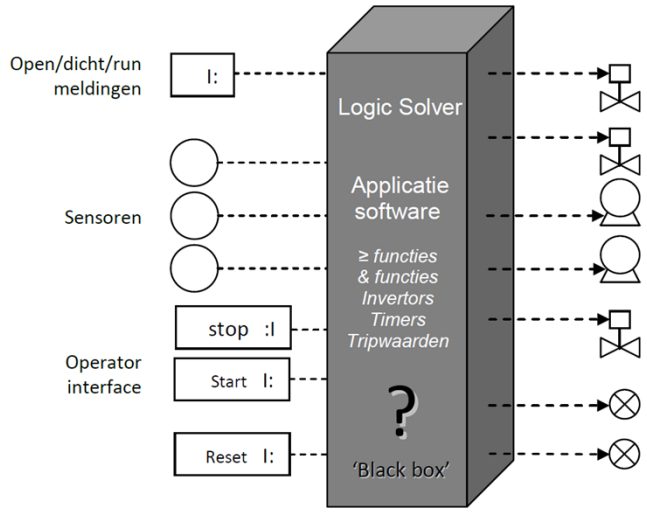

Aanpak
CONSILTANT
Hazards & Risk Assessment
Allocation
Safety Requirements Specification
Design & Engineering
Installation & Commissioning & Validation
Operation & Maintenance
HAZOP & LOPA studie
Veiligheid Kritische Voorzieningen
Definitie van SIL beveiligingen
Bepaling van instrumentele beveiligingen
Specificatie van SIL beveiligingen
Opbouw
Integriteit
Specificatie onderdelen
Hoe snel
Lek dichtheid
Overbrugging
Hoe Resetten
Ontwerp van SIL beveiligingen
Specificatie Application Program
Bedrading
Lay out
Configuratie
SIL verificatie
Realisatie van SIL beveiligingen
Test-procedures
FAT
Loop tests
SIF validatie
Gebruik van SIL beveiligingen
Overbrugging procedures
Onderhoud
Proof tests
Hoe reageren op alarmen
Spare parts
Procesveiligheid: SIL
6

IEC-61511 2e editie

- Verduidelijkingen, aanscherpingen, meer voorbeelden
- Minder vrijblijvend. ‘Should’ is vaak veranderd in ‘shall’
- ‘Architectuur eisen’ zijn anders dan in 1e editie
- Meer aandacht voor systematische fouten
- Meer eisen ‘Applicatie Program’
- Meer eisen m.b.t. testen
- Safety manual vereist
- Strengere eisen projectuitvoering en competentie van mensen

Procesveiligheid: SIL 7

Meer aandacht voor Application Program



Procesveiligheid: SIL 8

SIL verificatie

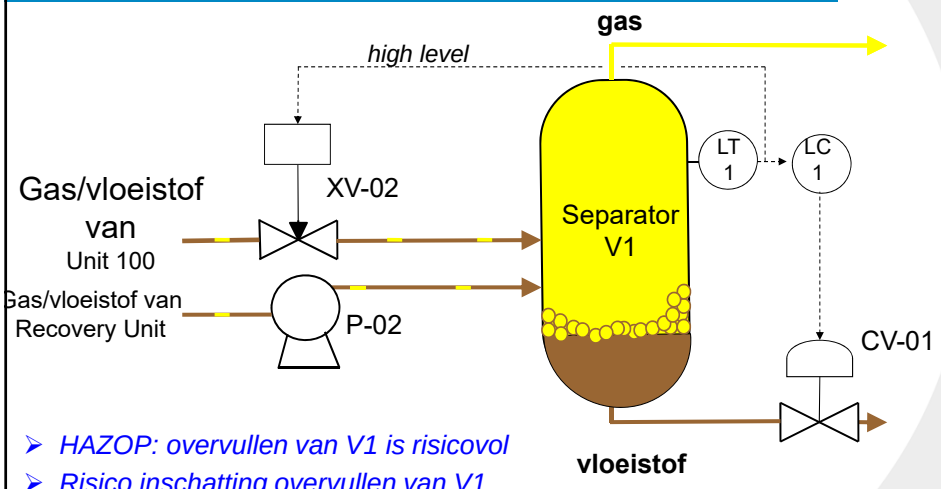
Aantonen dat het ontwerp van de beveiliging voldoet aan de SIL eisen.

1. *Identificatie van de beveiliging*
2. *Juiste functie (gebaseerd op SRS)*
3. *Onafhankelijk van regeling*
4. *Geen systematische fouten*
5. *Architectuur (redundantie) correct*
6. *Faalkans voldoende laag*

In 2e editie van IEC 61511 is item 4 toegevoegd.

Procesveiligheid: SIL 9

Voorbeeld Hoog niveaubeveiliging

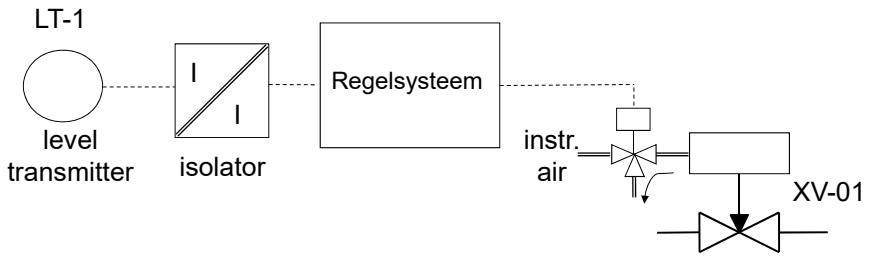


- *HAZOP: overvullen van V1 is risicovol*
- *Risico inschatting overvullen van V1*
- *Een SIL 1 beveiliging is nodig*

Procesveiligheid: SIL 10

SIL verificatiecriterium 1 - Identificatie

Identificatie van de beveiliging



Procesveiligheid: SIL 11

SIL verificatiecriterium 2 - Functie

Juiste functie?

De toevoer vanaf de ‘Recovery unit’ wordt niet gestopt. Als de pomp in bedrijf is, dient deze ook te stoppen.

Belangrijk:

- Applicatie software (application program)
- Proces Safety Time
- Afsluiter ‘Tight Shut-off’?

Procesveiligheid: SIL 12

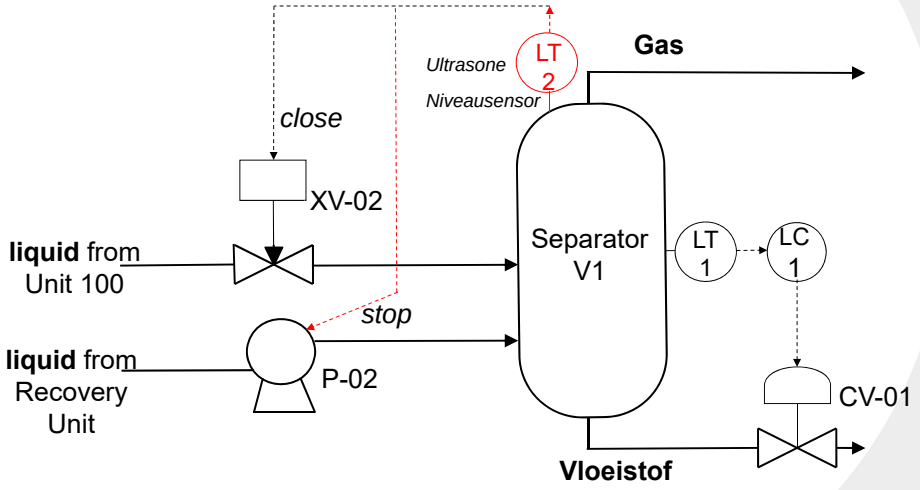
SIL verificatiecriterium 3 - Onafhankelijk

Onafhankelijk van de regeling?

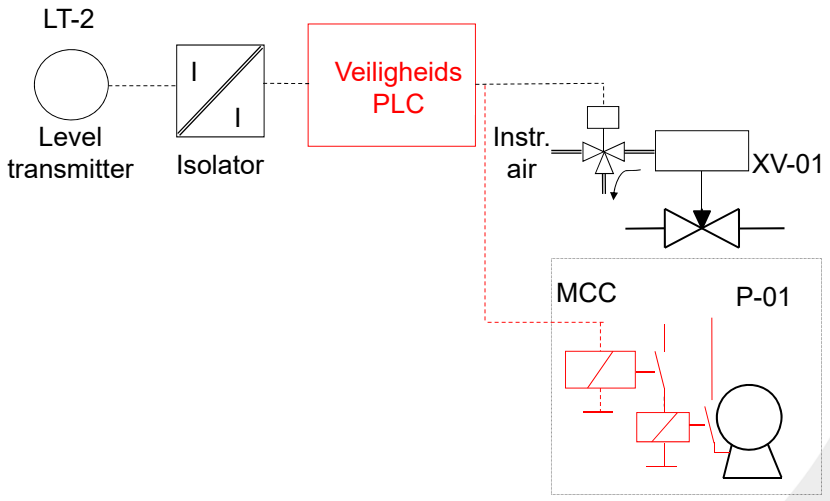
Voor regelen en beveiligen is gebruik gemaakt van één transmitter en een regelsysteem.

Dus niet onafhankelijk van de regeling.

Verbeterd ontwerp



Verbeterde beveiliging



Procesveiligheid: SIL 15

SIL criterium 4 – Geen systematische fouten

Devices hebben een 'low likelihood of systematic faults' hebben.

Systematic Failures
Fouten in het ontwerp, software (bug), menselijke fouten, veroorzaakt door externe invloeden.
Moeilijk te kwantificeren.

'A qualitative approach is preferred for systematic failures'.

Random Hardware Failures
Fouten door verouderingsprocessen.
Relatief makkelijk te kwantificeren.

Procesveiligheid: SIL 16

Systematic failures

IEC-61511: Pas '**prior use**' instrumenten/componenten toe!!
Process interface failures are very prominent in sensors, including plugged process lines, frozen lines, corrosion and gas permeation and valves, including seat damage, plugging, deposition and corrosion.

In IEC-61508 wordt 'Systematic Capability' gebruikt wat eigenlijk aangeeft dat de leverancier zijn werk goed heeft gedaan.

SIL verificatiecriterium 4

In deze applicatie wordt het niveau gemeten met een ultrasone niveausensor.

De gekozen sensor kan niet goed door 'schuim' kijken en is derhalve voor deze applicatie niet/minder geschikt.

Een radarmeting wordt gekozen.

SIL verificatiecriterium 5 - Architectuur

Architectuur (redundantie) correct?
Enkel of dubbel uitvoeren?

Drie methoden:
- *volgens IEC 61511 (met prior use componenten)*
- *volgens IEC 61508 route 1H (type A&B, SFF, HFT)*
- *volgens IEC 61508 route 2H*

Aanbeveling Consiltant BV: Gebruik de rood aangegeven methode als bedrijf niet 'prior use' kent.

'The route developed in IEC 61511 is derived from route 2H'.

SIL verificatiecriterium 5 - Architectuur

SIL	Mode	Minimum required HFT
1	All	0
2	Demand mode	0
2	Continuous mode	1
3	All	1
4	All	2

IEC-61511-1:2016

All devices shall be suitable for the operating environment as determined through consideration of the manufacturer's documentation, the constraints within the SRS and reliability parameters. Suitability of the selected devices shall always be considered in the context of the operating environment.
Devices selected for use as part of a SIS shall be in accordance with IEC 61508-2/3:2010 or shall be 'Prior Use'.

SIL verificatiecriterium 6 - Faalkans

Vereenvoudigde formules:

1oo1 $PFD \approx \frac{1}{2} \lambda_{DU} \cdot T$

1oo2 $PFD \approx \frac{1}{3} ([1- ß] \cdot \lambda_{DU})^2 \cdot T^2 + ß \cdot \frac{1}{2} \lambda_{DU} \cdot T$

2oo2 $PFD \approx \lambda_{DU} \cdot T$

2oo3 $PFD \approx ([1- ß] \cdot \lambda_{DU})^2 \cdot T^2 + ß \cdot \frac{1}{2} \lambda_{DU} \cdot T$

PFD = *Probability of failure on demand*

λ_{DU} = *Dangerous undetected failure rate*

T = *Test periode, tests zijn 100% perfect*

ß = *Common Cause Factor*

SIL	*PFD*
1	$< 10^{-1}$
2	$< 10^{-2}$
3	$< 10^{-3}$
4	$< 10^{-4}$

Procesveiligheid: SIL 21

SIL verificatie

1. Identificatie van de beveiliging ✓

2. Juiste functie ✓

3. Onafhankelijk van regeling ✓

4. Geen systematische fouten ✓

5. Architectuur (redundantie) correct ✓

6. Faalkans voldoende laag ✓

Conclusie:

de uiteindelijke beveiliging voldoet aan alle integriteiteisen van SIL 1 gebaseerd op een proof test interval van x jaar.

Procesveiligheid: SIL 22

Als u meer wilt weten:

CONSILTANT

Trainingen met open inschrijving;

HAZOP	*4 oktober 2016*
LOPA en SIL classificatie	*21 september 2016*
SIL verificatie en SIF validatie	*22 september 2016*

Locatie: Apeldoorn www.consiltant.com

Procesveiligheid: SIL 23