

# Hoe wordt bepaald of een beveiliging SIL verificatie van

Herman Jansen



Ing. H. Jansen (jansen@safety-sc.com) is safety consultant bij Safety Solutions Consultants BV, Businesspark Apeldoorn, Laan van Westenenk 501, 7334 DT Apeldoorn, (055) 5493362, www.safety-sc.com

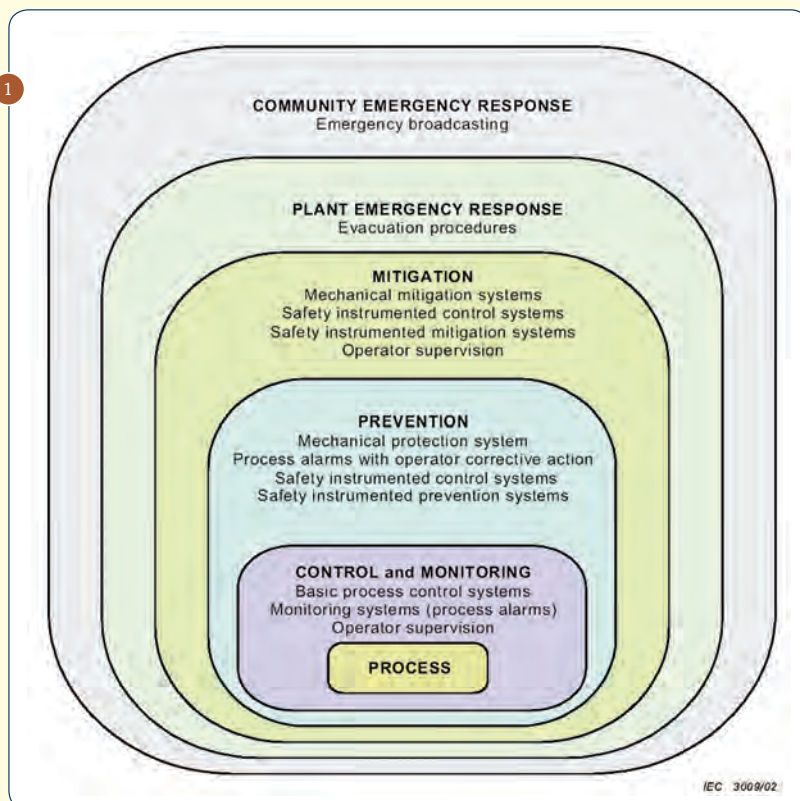
De (inter)nationale normen NEN-EN-IEC 61508 en NEN-EN-IEC 61511 bestaan dit jaar respectievelijk 10 en 5 jaar. Volgens deze normen moeten beveiligingen van gevaarlijke processen 'risk based' ontworpen zijn: hoe hoger het risico van het vrijkomen van een gevaarlijke stof, des te betrouwbaarder de beveiliging. Gesteld kan worden dat de methodiek van risk based ontwerpen inmiddels internationaal in de praktijk beproefd is. Wel blijkt dat zorgvuldig verifiëren of de beveiliging voldoet aan de normen, niet altijd volledig plaatsvindt. In dit artikel wordt uitgelegd op welke wijze de normen geverifieerd moet worden.

## Beveiligen, hoe doe je dat?

*Startpunt - Gevaaridentificatie: bepalen van potentieel te beveiligen scenario's*

Het moet helder zijn wat de potentiële gevaren zijn van een procesinstallatie of machine. In de procesindustrie wordt de HAZOP methodiek vaak toegepast teneinde te weten wat er mis kan gaan, wat de oorzaken en de gevolgen zijn en hoe beveiligd wordt of dient te worden. De gevaarsidentificatie wordt over het algemeen goed gedocumenteerd.

Fig. 1 'Protections layers' volgens IEC 61511



## 2e stap - Risicobepaling, SIL Classificatie

In de IEC 61508/61511 worden methodieken aangereikt om het risico te bepalen en uit te drukken als 'SIL': Safety Integrity Level. Er zijn vier niveaus: SIL 1 t/m SIL 4 (duidt op zeer hoog risico). Bij SIL classificatie worden op procesinstallatie zonder beveiligingen de risico's van de gevaarlijke scenario's bepaald.

## 3e stap - Allocatie en ontwerp van beveiligingen

Risico's kunnen gereduceerd worden door het proces aan te passen (inherent beveiligen; dit heeft de voorkeur) of door het aanbrengen van mechanische en/of instrumentele beveiligingen. Zie de Protection layer 'PREVENTION' in figuur 1. SIL verificatie zoals in dit artikel beschreven, heeft betrekking op instrumentele beveiligingen.

## 4e stap - SIL verificatie

SIL verificatie van SIL 1 t/m 4 beveiligingen is het toetsen van een instrumentele beveiliging aan de volgende eisen:

- Het moet functioneel voldoen.
- Het dient onafhankelijk van het regelsysteem gerealiseerd te worden.
- Het moet voldoen aan architectuur eisen (redundantie eisen).
- De faalkans op aanspraak van de beveiliging moet voldoende laag zijn met in acht name van periodiek testen.
- Om aan het gestelde SIL te voldoen, moet aan al deze eisen worden voldaan.

## Een voorbeeld

Aan de hand van een voorbeeld zal de SIL verificatie uitgelegd worden.

# voldoet aan de SIL eisen?

## instrumentele beveiligingen

### Procesbeschrijving

In V1 wordt een gas/vloeistof-mengsel gescheiden (zie figuur 2). De toevoer vanaf unit 100 is continu. Toevoer vanaf de Recovery unit vindt plaats op incidentele basis. Het niveau in Separator V1 wordt gemeten door transmitter LT-1 en geregeld door LC-2. De instrumentele overvulbeveiliging functioneert als volgt: bij hoog niveau, wordt de (continue) toevoer naar het vat V-1 gestopt.

Uit de HAZOP studie is naar voren gekomen dat het overvullen van V1 een risico is. Dit scenario is door het HAZOP/SIL team geclassificeerd als SIL 1.

### Voldoet deze beveiliging aan SIL 1?

Het is zinvol de beveiliging eerst schematisch zo volledig mogelijk weer te geven (zie figuur 3).

Er is voor gekozen om met een displacement transmitter het niveau te meten. Een isolator is toegepast in verband met explosiegevaar. De logische schakeling wordt in DCS ondergebracht. De veersluitende ballvalve wordt geopend door instrumentenlucht.

### SIL verificatiecriterium 1

De beveiliging moet *functioneel* voldoen. Dat wil zeggen: bij functioneren van de beveiliging dient (altijd) het ongewenste scenario voorkomen te worden. Dat is in dit voorbeeld niet het geval omdat de toevoer vanaf de 'Recovery unit' niet gestopt wordt. De pomp dient dus ook te stoppen.

### SIL verificatiecriterium 2

De SIL beveiliging moet *onafhankelijk* zijn van het regelsysteem. Dat is in het voorbeeld niet het geval: voor regelen én beveiliging is gebruikgemaakt van één transmitter. Een 2e leveltransmitter (LT-2) is nodig om de regelkring aan te sturen. Ook is het niet juist de logische schakeling in het DCS onder te brengen.

Na aanpassing zien het proces en de beveiliging er uit als in figuur 4 en 5.

### SIL verificatiecriterium 3

Beveiligingscomponenten moeten *voldoen aan de architectuureisen* van het betreffende SIL. De IEC normen geven aan wanneer een component enkelvoudig of redundant uitgevoerd dient te worden. Dat is afhankelijk van de complexiteit van de componenten: of er ervaring mee is, de verhouding tussen 'safe failures' (de beveiliging grijpt onnodig in) en 'dangerous failures' (de beveiliging grijpt niet in bij potentieel gevaar). Globaal

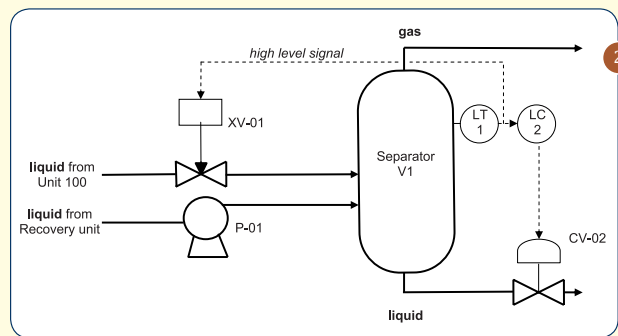
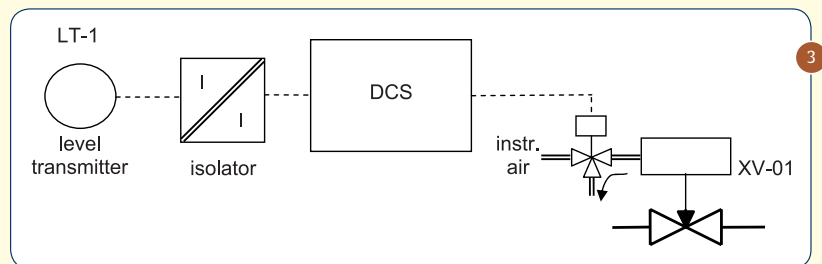


Fig. 2 Processchets

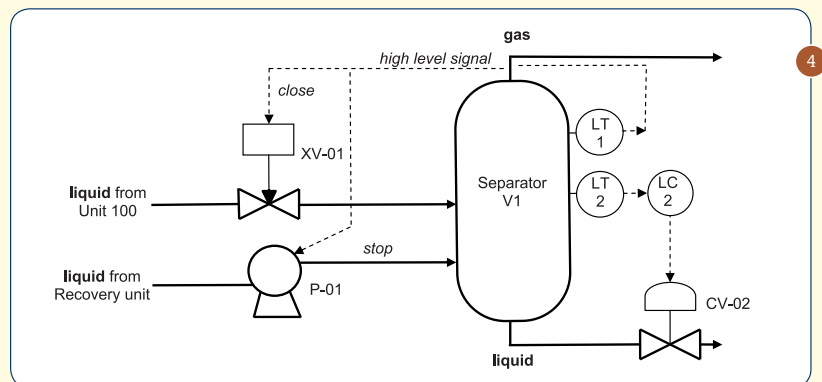
Fig. 3 De beveiliging

Fig. 4 Processchets met verbeterde beveiliging

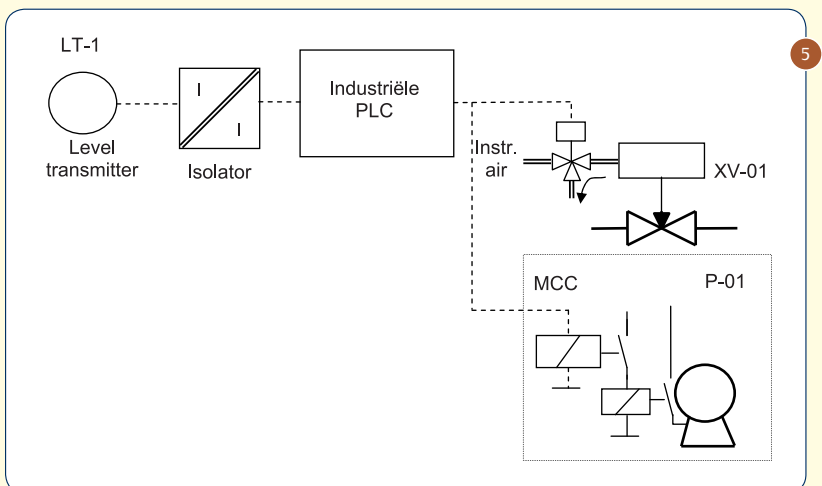
Fig. 5 De verbeterde beveiliging



3



4



5

blijkt het volgende: alle componenten van de beveiliging uit het voorbeeld voldoen aan de architectuureisen van SIL 1 (zie figuur 6).

**SIL verificatiecriterium 4**

De beveiliging moet een voldoende *lage faalkans* hebben. Met faalkans wordt bedoeld, de kans op falen van de beveiliging als deze aangesproken wordt. Dit wordt de 'Probability of Failure on Demand' genoemd, afgekort 'PFD'. De toelaatbare PFD waarden bedragen:

- SIL 1 PFD < 10<sup>-1</sup>
- SIL 2 PFD < 10<sup>-2</sup>
- SIL 3 PFD < 10<sup>-3</sup>
- SIL 4 PFD < 10<sup>-4</sup>

De PFD van de overvulbeveiliging dient dus kleiner dan 10<sup>-1</sup> te zijn.

PFD waarden worden bij voorkeur berekend met gebruikmaking van specifiek daarvoor ontwikkelde software (Markov modellering of foutenboom analyse). Om dat te kunnen bepalen, dienen we te beschikken over de faalgegevens van alle componenten van de beveiliging. Faalgegevens kunnen ontleend worden aan SIL certificeringsrapporten, OREDA / SINTEF, FMEDA rapporten (Exida), of door de planteigenaar zelf worden bepaald.

Als verstopping van impulsleidingen waarschijnlijk is, dient dit meegenomen te worden in de gekozen faalsnelheid. Soort medium (bijv. vervuild of agressief) is van belang bij afsluiters evenals het al dan niet 'tight shut-off' moeten zijn.

Iedere beveiliging moet periodiek getest (kunnen) worden. Het kan zijn dat de kwaliteit en volledigheid van het testen niet 100% zijn. Dat wordt uitgedrukt met de 'Proof test Coverage' factor PC.

**Bepaalde faalsnelheden**

- Level transmitter  $\lambda_{DU} = 6,0 \times 10^{-7} / h$  Bron: Sintef
- Isolator  $\lambda_{DU} = 1,5 \times 10^{-7} / h$  Bron: Exida
- PLC PDF = 5,0 × 10<sup>-3</sup> Bron: Leverancier
- MCC relais  $\lambda_{DU} = 2,0 \times 10^{-7} / h$  Bron: Sintef
- Solenoid valve  $\lambda_{DU} = 9,0 \times 10^{-7} / h$  Bron: Sintef
- Afsluiter+ actuator  $\lambda_{DU} = 2,1 \times 10^{-6} / h$  Bron: Exida

Fig. 6

Component	Minimaal benodigde aantallen		
	voor SIL 1	voor SIL 2	voor SIL 3
Druk Schakelaar	1	2	3
Transmitter	1	2	2
SIL 2 gecert. Transm.	1	1	2
Relais	1	1	2
Industriële PLC	acceptabel	niet acceptabel	niet acceptabel
SIL 3 gecert. PLC	acceptabel	acceptabel	acceptabel
Pilot/Solenoid valve	1	1	2
Afsluiter met actuator	1	1 à 2	2 à 3
Motorafschakeling	1	1	2

*Overige gegevens*

- Proof test interval T 4 jaar
- Proof test Coverage factor PC 95%

Voor de bepaling van de PFD van de transmitter kan de volgende formule gebruikt worden:

$$PFD_{transmitter} \approx [0,5 \times \lambda_{DU} \times T] / PC = [0,5 \times 6 \times 10^{-7} \times 4 \times 24 \times 365] / 0,95 = 1,1 \times 10^{-2}$$

De overige PFD's kunnen op identieke wijze berekend worden.

$$PFD_{beveiliging} = PFD_{trans.} + PFD_{isolator} + PFD_{PLC} + PFD_{Sol.valve} + PFD_{afsluiter} + PFD_{MCC} = 8,2 \times 10^{-2}$$

De beveiliging voldoet aan de faalkans eis.

**Overall conclusie**

De uiteindelijke beveiliging voldoet aan alle integriteitseisen van SIL 1 wanneer 4-jarlijks getest wordt.

**Algemene aanbevelingen**

- Het SIL goed documenteren, onder andere ten behoeve van 'Management of Change'.
- Beveiligingen onderbrengen in een separaat onderhoud/periodiek testprogramma.
- De HAZOP studie wordt in de praktijk niet altijd gevolgd door een SIL classificatie (in geval van niet te tolereren risico's) en SIL verificatie van alle eisen in geval van SIL scenario's. Audits en (overheids)inspecties zijn daar nog niet voldoende voor ingericht. SIL classificatie en verificatie dienen echter aantoonbaar te worden uitgevoerd. ●

**Referenties**

- IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems
- IEC 61511: Functional Safety - Safety Instrumented Systems for the Process Industry Sector
- Reliability Data for Safety Instrumented Systems PDS Data Handbook, 2006, SINTEF
- Safety Equipment Reliability Handbook third edition, 2007, Exida
- Artikel 'Juist omgaan met industriële veiligheid', NPT Proces-technologie okt. 2004 (www.safety-sc.com)

**Afkortingen**

- DCS Distributed Control System
- h hour
- HAZOP Hazard & Operability (study)
- MCC Motor Control Center
- PC Proof test Coverage Factor
- PFD Probability of Failures on Demand
- PLC Programmable Logic Controller
- SIL Safety Integrity Level
- T Proof test interval
- $\lambda_{DU}$  Dangerous undetected failure rate