IEC 61508 en IEC 61511

Proces veiligheid & SIL

Er is al veel gesproken over SIL. In dit artikel legt Functional Safety Expert Herman Jansen uit hoe SIL in de praktijk bijdraagt aan een veiliger proces.

Herman Jansen
Consiltant BV

Uit de praktijk

In april jl. werd bij een gerenommeerd chemisch bedrijf een HAZOP studie uitgevoerd van één van de bestaande waterstof compressoren.

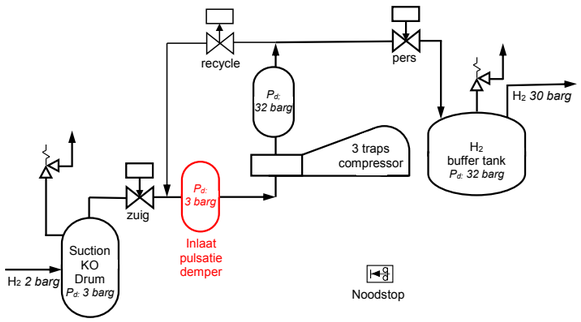

Fig. 1 Vereenvoudigd schema van een waterstof compressor

Voorzien is in een noodstopsysteem. Gelukkig is het nooit nodig geweest om deze tijdens bedrijf te activeren. Als de operator de noodstop bedient, wordt direct de compressor gestopt en worden de zuigafsluiter en de persafsluiter gesloten. De recycle-afsluiter gaat vertraagd open. Tijdens de brainstorm sessie kwamen we tot het besef dat door het indrukken van de noodstop, de inlaat pulsatiedemper catastrofaal zal bezwijken door overdruk vanaf de perszijde van de compressor.
Dit is een ernstig LOC scenario. Direct zijn door het bedrijf adequate maatregelen genomen.

Gevaren identificatie

Een goede gestructureerde methode teneinde zoveel mogelijk realistische gevaren te identificeren, is het uitvoeren van een HAZOP-studie. De installatie wordt in delen opgesplitst. Gedurende één of meerdere brainstorm sessies wordt door een multidisciplinair team ieder onderdeel onderworpen aan een lijst met standaard afwijkingen (zoals 'druk meer'). Hierdoor kwamen we tot het inzicht dat het met deze waterstof compressor 'goed fout' zat.
Wat heeft HAZOP met procesveiligheid en SIL te maken? Veel! Zonder kennis van de potentiële gevaren kan een proces installatie niet adequaat beveiligd worden. Een (instrumentele) beveiliging moet de ontwikkeling van zo'n geïdentificeerd gevaar stoppen. Voor 2000 werd er al ge-HAZOP-t (de methode is in 1974 ontwikkeld). Echter, door met name de SIL norm IEC 61511 is het risicoaspect tijdens de brainstorm sessies veel dominanter geworden.

Risico beheersing

Het risico van elk potentieel gevaar (de LOC scenario's) moet bepaald worden. Een veel gebruikte methode is de risicograaf.

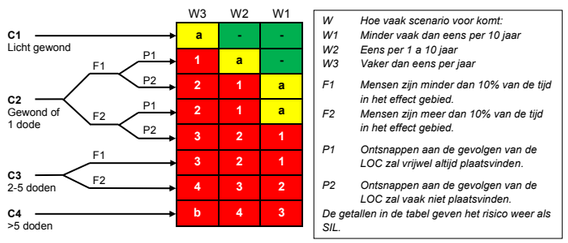

Fig. 2 De risicograaf

Een inschatting van de waterstof compressor LOC zou kunnen zijn:
- Lokale bediening van de noodstop; eens per 1 a 10 jaar (W2).
Mogelijke gevolgen; Zwaar gewonde/dode (C2). De operator is aanwezig (F2), Ontsnappen aan de gevolgen is vaak niet mogelijk (P2). Dit leidt tot een SIL 2 risico.

Dat houdt in dat een adequate SIL 2 beveiliging het risico in voldoende mate zal reduceren.
Een andere, populair geworden methode is LOPA. Een fout of een falen ('initiating event') kan leiden tot een incident. Van het 'initiating event' wordt de waarschijnlijkheid van optreden ingeschat. De ernst van de gevolgen van het incident moet bepaald worden. Vervolgens moet het bedrijf bepaald hebben welk restrisico zij acceptabel vindt. Deze informatie is bv. te ontlenen aan de risicomatrix van het bedrijf.

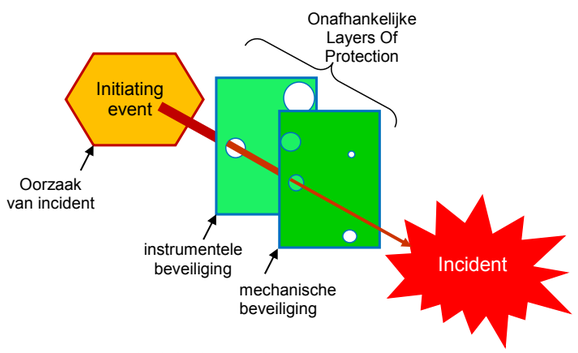

Fig. 3 De LOPA methodiek schematisch weergegeven

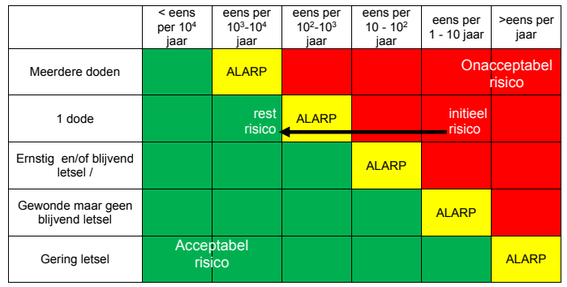

Fig. 4 Een risicomatrix

In geval van het waterstof scenario is een forse risico reductie benodigd om te komen tot acceptabel rest risico. Door het bedrijf is gekozen voor een combinatie van een SIL 1 instrumentele beveiliging (noodstop stuurt een nieuw aan te brengen afblaasafsluiter open) en een mechanische veerveiligheid op de inlaat pulsatiedemper.
Wat heeft risicobepaling met procesveiligheid en SIL te maken? Veel! Zonder risicobepaling kan een proces installatie niet adequaat beveiligd worden. Een beveiliging moet voldoende betrouwbaar zijn. Een SIL 1 beveiliging reduceert het risico met een factor tussen 10 en 100, een SIL 2 beveiliging reduceert het risico met een factor tussen 100 en 1000.

De instrumentele beveiliging

Als we weten wat de instrumentele beveiliging moet doen (functie) en hoe integer deze moet worden uitgevoerd, kan deze ontworpen worden. Tijdens het ontwerp zijn de volgende aspecten relevant:

1. De documenten die volgens het management systeem opgesteld dienen te worden.
2. Betrokkenen moeten competent zijn.
3. De beveiliging moet de installatie veiligstellen.
4. De beveiliging moet snel genoeg zijn.
5. De beveiliging zal onafhankelijk van het regelsysteem gerealiseerd moeten worden.
6. Mogelijk moeten onderdelen van de beveiliging redundant worden uitgevoerd.
7. De PFD van de beveiliging moet laag zijn.
8. Het PLC programma moet correct zijn.
9. De beveiliging moet te testen zijn.
10. Het ontwerp van iedere beveiliging zal geverifieerd moeten worden.

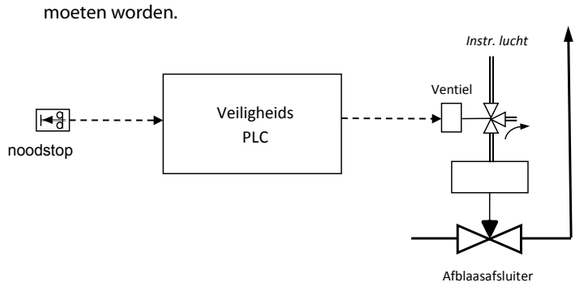

Fig. 5 De SIL 1 beveiliging schematisch weergegeven

Nadat een instrumentele beveiliging gerealiseerd is volgens het ontwerp, zal zeker gesteld moeten worden dat deze helemaal goed functioneert. Essentieel is dat voor iedere SIF een gedegen en gedetailleerde test beschrijving beschikbaar komt. Volgens het bepaalde interval zal periodiek getest moeten worden.

Wat 15 jaar SIL heeft gebracht:

- Uiteraard betrouwbare instrumentele SIL 1/2/3 beveiligingen die aantoonbaar bijdragen aan procesveiligheid.
- Leveranciers hebben integere instrumenten/sensoren/veiligheid besturingen op de markt gebracht.
- Veiligheidkritische voorzieningen worden bepaald. SIFs worden op P&ID's en in het veld visueel gekenmerkt.
- Veiligheidkritische voorzieningen worden periodiek getest.

De invloed van de SIL normen strekt verder dan alleen instrumentele beveiligingen

20 jaar geleden kon het zijn dat bij een HAZOP-studie van een potentiële grote calamiteit geconcludeerd werd: Een alarm zal actief worden en de operator heeft voldoende tijd voor correctieve acties. Aanvullende acties zijn niet nodig.
LOPA is mede ontwikkeld op basis van de SIL-normen. Aan een operator wordt nu over het algemeen niet meer risicoreductie toegekend dan een factor 10.
Is SIL nu uitontwikkeld? Neen. De SIL-norm voor de procesindustrie, IEC 61511 uit 2003 zal op korte termijn opnieuw uitgebracht worden. Diverse internationale teams zijn al jaren bezig met de verbeteringen. Doordat de norm zó in een behoefte voorziet, is er erg veel participatie en drive om de norm nóg beter te maken dan deze al is!

< Fig 6 Wijze waarop Dow Benelux B.V. SIFs visueel kenmerkt

Fig 7. Voorblad IEC 61511 >

Uitleg van de afkortingen

ALARP	As Low As Reasonably Practible
HAZOP	Hazard & Operability study
H_2	Waterstof
KO	Knock Out
LOPA	Layer Of Protection Analysis
LOC	Loss Of Containment
P_d	Design Pressure
PFD	Probability Of Failure on Demand
PLC	Programmable Logic Controller
P&ID	Piping & Instrumentation Diagram
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SRS	Safety Requirements Specification