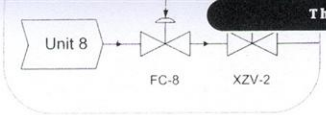


Wanneer is de beveiliging voldoende?

Juist omgaan met industriële veiligheid

Herman Jansen

Ing. Herman Jansen is werkzaam als safety consultant bij TNO Safety Solutions Consultants BV in Apeldoorn.
E-mail: jansen@safety-sc.com.
Internet: www.safety-sc.com

Goed beveiligen is van levensbelang. Te licht beveiligen is gevaarlijk. Te zwaar beveiligen is met name economisch onaantrekkelijk. Welke beveiligingsprincipes en -componenten kunnen worden gekozen? Moet periodiek worden getest? In dit artikel wordt een praktische methode aangereikt hoe op een verantwoorde wijze met veiligheid kan worden omgegaan, gebaseerd op de internationale normen IEC 61508 en IEC 61511.

Risico's

In ons dagelijks leven hebben we voortdurend met risico's te maken: in het verkeer, in onze huizen, door criminaliteit, door onze voeding, het weer, het milieu et cetera. Meestal gaat het goed, soms gaat het fout... En ook al zouden we dat misschien willen, het uitsluiten van alle risico's is onmogelijk. Leven is nu eenmaal een risicovolle onderneming.
In het bedrijfsleven is het niet veel anders. Het volledig *uitsluiten* van risico's is alleen mogelijk door productieprocessen stil te leggen, de procesinstallatie af te breken en de fabriek te sluiten. Een realistischer benadering is daarom risico's te *beheersen*. Maar hoe gaat dat, beheersen van risico's?

Aanpak

Het reduceren van risico's tot een aanvaardbaar niveau houdt meer in dan even ergens een beveiliging plaatsen. Aandacht voor veiligheid is noodzakelijk gedurende de volledige levensduur van de installatie: tijdens het ontwerp, tijdens de productiefase, bij aanpassingen, tijdens onderhoud, maar ook tijdens het afbreken van de installatie.
Een goede procedure is:

1 identificatie van gevaren en noodzakelijke beveiligingsfuncties (bijvoorbeeld door HAZOP);
2 inschatten van de risico's (SIL-classificatie);
3 integratie van de SIL-classificatieresultaten in het ontwerp;
4 verificatie of de beveiligingen functioneel en integer zijn (SIL-verificatie);
5 in werking stellen van procedures voor operatie, onderhoud en periodieke tests;
6 functionele afnametest en inbedrijfstelling van de beveiligingen;
7 uitvoeren van periodieke tests en onderhoud;
8 optimalisatie (bijvoorbeeld ten gevolge van betere inzichten of modificaties in de installatie);
9 implementatie in een veiligheidsmanagementsysteem (inclusief auditing).

In het vervolg van dit artikel zal worden ingegaan op de eerste vier genoemde aspecten.

Gevarenidentificatie en noodzakelijke beveiligingsfuncties

Waar gaat het om? Het gaat om te weten waar de potentiële gevaren zitten. Uitgangspunt is natuurlijk dat het ontwerp van de installatie solide is. Ontworpen door ervaren procestechnologen en engineers, en zo inherent veilig mogelijk, waardoor minimale additionele beveiligingen nodig zijn. Een leiding bijvoorbeeld niet uitvoeren met een hoge-drukbeveiliging, maar bij voorkeur deze zodanig specificeren dat die leiding tegen de hoogst mogelijk voorkomende druk bestand is.
Een HAZOP (Hazard and Operability Study) kan vervolgens worden uitgevoerd om het ontwerp door te lichten. Dat moet dan gebeuren door een team van specialisten, in bezit van kennis over en ervaring met de HAZOP-methode, het proces, de procesinstallatie, de operatie en het onderhoud. Het is niet ongebruikelijk hierbij gebruik te maken van externe deskundigen.

SIL-classificatie

Kort samengevat behelst SIL-classificatie het inschatten van risico's. SIL staat voor Safety Integrity Level. Er zijn vier niveaus, namelijk SIL1 tot en met SIL4: hoe hoger het ingeschatte risico, hoe hoger ook het SIL-niveau en de daarmee samenhangende eisen die worden gesteld aan de beveiligingen. De hoogte van het risico van een 'Loss Of Containment' (LOC) wordt bepaald door de ernst en de frequentie van optreden (bij afwezigheid van beveiligingen). Principieel gaat het daarbij om veiligheid (preventie van letsel bij mensen).
Het SIL classificeren ten behoeve van het voorkomen van milieuverontreiniging (bijvoorbeeld door emissie van een toxische stof) en financiële gevolgen (door equipmentschade en operationele derving) is geen 'eis' van de genoemde internationale IEC-normen. Het is echter wel zeer aan te bevelen.
De beste resultaten worden verkregen als de risico's brainstormend in teamverband worden ingeschat, waarbij de samenstelling van zo'n team overeenkomt met het voornoemde HAZOP-team.

Hoe gaat nu zo'n SIL-classificatie in zijn werk?
Een voorbeeld kan dit verduidelijken.
Stel, er is een project geïnitieerd om een vat (V-100) toe te voegen aan een bestaande installatie.

1

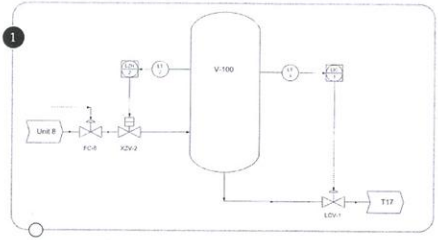


Fig. 1. Processchets

Na de HAZOP wordt een SIL-classificatie gehouden. Daaraan nemen deel: een externe facilitator (die leiding geeft aan het classificeren en ter plekke notuleert met behulp van laptop en beamer), de verantwoordelijke procestechnoloog, een ervaren operator en een instrumentatie-engineer.
Het geïdentificeerde gevaar (ook wel scenario genoemd) is: 'Overvullen van vat V-100'. Door de procestechnoloog is al een instrumentele hoogniveaubeveiliging ontworpen, die bij te hoog niveau de inlaatafsluiter sluit.

Het risico wordt ingeschat door het team diverse vragen te laten beantwoorden:

- *Waardoor kan het scenario optreden?* Door het (dicht) falen van niveau regelafsluiter LCV 1.
- *Hoe vaak zal het scenario optreden?* Bij afwezigheid van de instrumentele beveiliging circa eens per vijf jaar.
- *Wat zijn de gevolgen?* De gasleiding naar C101 zal zich vullen met vloeistof. Deze leiding (50 meter lang) is daar niet voor ontworpen. Er kan/zal een breuk ontstaan waardoor in tien minuten circa 1000 kg van de gevaarlijke stof vrij zal kunnen komen.
- *Hoe snel kan het scenario zich ontwikkelen?* Circa drie uur na het open falen van de regelafsluiter.
- *Wat zijn de gevolgen voor mensen?* Zij kunnen worden blootgesteld aan de gevaarlijke stof en die gedurende enige tijd inhaleren. Mensen die zich in de directe nabijheid bevinden, kunnen zwaar gewond raken, er kunnen zelfs doden vallen.
- *Bevinden zich mensen in de nabije invloedsfeer van de calamiteit?* Ja, circa tien mensen zijn regelmatig in de buurt.
- *Is het mogelijk aan het gevaar te ontkomen?* Alhoewel het gevaar zich langzaam ontwikkelt, zullen de aanwezigen toch verrast worden. Ontsnappen aan het gevaar zal vaak niet mogelijk zijn.
- *Wat zullen de gevolgen zijn voor het milieu?* Een emissie van circa 1.000 kg is een ernstige milieubelasting.
- *Wat zijn de economische gevolgen?* Schade aan de leiding inclusief ondersteuningen: circa € 50.000, productiederving gedurende vijf dagen: circa € 100.000.
  Totaal: € 150.000.

Integratie SIL-classificatie in het ontwerp

Heeft het team de risico's geïnventariseerd, dan is het zaak een voldoende betrouwbare beveiliging te ontwerpen. Dat doet men door:

1 het geïnventariseerde risico 'te vertalen' in een SIL-klasse;
2 vervolgens de beveiliging te laten voldoen aan de eisen die horen bij die SIL-klasse.

Een beproefde methode om tot het juiste SIL-niveau te komen is het gebruik van de risicograaf.
De gevolgen voor milieu en economie kunnen worden 'vertaald' naar een SIL-klasse door gebruik te maken van de conversietabellen 1 en 2.
De beveiliging moet voldoen aan de betreffende SIL-klasse met betrekking tot veiligheid. Het is aan te bevelen de beveiliging te laten beantwoorden aan de hoogstbepaalde SIL-klasse (veiligheid, milieuschade, economische schade).

Voor het behandelde voorbeeld ziet dat, bij toepassing van de risicograaf (fig. 2) en de conversietabellen (tabellen 1 en 2), er als volgt uit:

$SIL_{veiligheid}$: SIL 2 SIL_{milieu} : SIL 1 SIL_{geld} : SIL 2

Gesteld kan dus worden dat het risico van overvullen beveiligd dient te worden met een SIL-2-beveiliging.

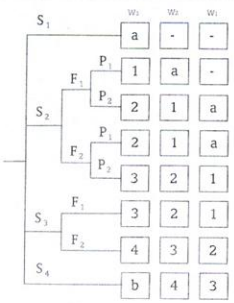
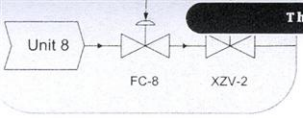


Fig. 2. Risicograaf ter bepaling van de SIL-klasse ten behoeve van de menselijke veiligheid

2

Gevolgen voor mensen		Aanwezigheid van mensen		Frequentie van optreden		Ontsnappen aan gevaar	
S1	lichtgewonde(n)	F1	minder dan 1 uur per dag	W1	minder dan 1x per 10 jaar	P1	zal vaak mogelijk zijn
S2	zwaargewonde(n), 1 dode	F2	vaker dan 1 uur per dag	W2	1x per 1 à 10 jaar	P2	zal vaak niet mogelijk zijn
S3	enkele doden			W3	meer dan 1x per jaar		
S4	vele doden						



Tabel 1.
Bepaling van de SIL-klasse om milieuvervuiling te voorkomen

	Milieugevolgen	***F3*** *>1x per per jaar*	***F2*** *1x per 1-10 jaar*	***F1*** *<1x per 10 jaar*
S0	geen	0	0	0
S1	beperkt	SIL 1	a	0
S2	gering, ernstig	SIL 2	SIL 1	a
S3	tijdelijke effecten	SIL 3	SIL 2	SIL 1
S4	langetermijneffecten	SIL 4	SIL 3	SIL 2

Tabel 2.
Bepaling van de SIL-klasse om economische schade te voorkomen

	Economische gevolgen	***F3*** *>1x per jaar*	***F2*** *1x per 1-10 jaar*	***F1*** *<1x per 10 jaar*
S0	0	0	0	0
S1	< 5.000 euro	SIL 1	a	0
S2	5.000-50.000 euro	SIL 2	SIL 1	a
S3	50.000-500.000 euro	SIL 3	SIL 2	SIL 1
S4	>500.000 euro	SIL 4	SIL 3	SIL 2

SIL-verificatie

SIL-verfificatie houdt in het toetsen van instrumentele beveiligingen aan de gestelde SIL-eisen. Hoe kan nu worden vastgesteld of een beveiliging voldoet?
Belangrijk is vast te stellen dat de beveiliging functioneel correct is. Een beveiligingsloop moet (bij voorkeur) volgens het fail-to-safe principe worden opgezet. Maar ook de kwaliteit en het faalgedrag van de gebruikte beveiligingscomponenten spelen een rol. Evenals de mate waarin redundanties zijn toegepast, waardoor bij falen van een component de beveiligingsfunctie toch intact blijft.
Terugkerend naar het 'overvul'-beveiligingsvoorbeeld kan dan het volgende worden geconcludeerd: de instrumentele beveiliging die ervoor zorgt dat bij te hoog niveau de inlaatafsluiter sluit, is functioneel gezien een juiste beveiliging om het overvulscenario te voorkomen.
De beveiligingsloop is als volgt ontworpen (zie fig. 3): een verschildruk-transmitter wordt gebruikt om het niveau te meten, de analoge stroomuitgang wordt rechtstreeks verbonden met een SIL 2 gecertificeerde beveiligings-PLC (Programmable Logic Controller). Deze PLC stuurt een solenoid valve aan die de lucht aflaat van de actuator van toevoerafsluiter XZV-2 waardoor deze sluit. Bij uitval van elektrische spanning of lucht sluit de toevoerafsluiter (dat is dus volgens het fail-to-safe principe).

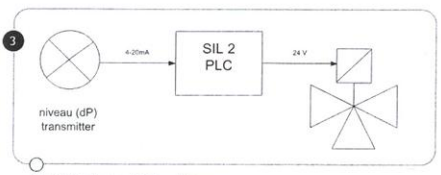


Fig. 3. De instrumentele beveiliging

Voldoet deze instrumentele beveiliging nu aan SIL 2? De integriteit van de beveiliging is afhankelijk van de integriteit van alle relevante onderdelen: de niveausensor, de PLC alsmede de toevoerafsluiter.

- *PLC:* is gecertificeerd voor gebruik in SIL 2 beveiligingen;
- *niveaumeting:* er wordt gebruik gemaakt van een beproefde verschildruk-transmitter van een gerenommeerde leverancier waarvan het operationele faalgedrag bekend is;
- *afsluiter:* ook voor de afsluiter wordt gebruik gemaakt van een bekend type waarvan de operationele faaldata bekend is.

De waarschijnlijkheid dat de toevoerafsluiter *niet* sluit wanneer het niveau te hoog is, wordt bepaald door de som van de waarschijnlijkheden van falen van alle betreffende onderdelen. Deze waarschijnlijkheid wordt vaak uitgedrukt als 'Probability of Failure on Demand' (afgekort als PFD). Bij een SIL-2-beveiliging mag de berekende PFD niet groter zijn dan 0,01. De PFD van een component is afhankelijk van de kwaliteit van die betreffende component (uitgedrukt als faalkans per tijdseenheid), hoe vaak en hoe goed er wordt getest, of er automatische diagnosefaciliteiten zijn en hoeveel jaar de beveiliging moet functioneren. De PFD kan berekend worden met speciale software. Ook is het mogelijk hiervoor de tabellen te gebruiken zoals vermeld in IEC 61508-6, annex B.

Op basis hiervan kunnen we een uitspraak doen over de beveiliging in ons 'overvul'-voorbeeld: de berekende PFD blijkt groter te zijn dan 0.01. De beveiliging is dus onvoldoende betrouwbaar. Om de betrouwbaarheid te verhogen is gekozen voor enkele aanpassingen. De meetwaarde van de beveiligingstransmitter LT-2 wordt in het regelsysteem continu vergeleken met de identieke meetwaarde van de regeltransmitter LT-1. Bij een verschil wordt een discrepantiealarm geïnitieerd. Daarnaast wordt in de luchtaansturing van de regelafsluiter FC-8 een solenoid valve geplaatst dat bij te hoog niveau in V-100 naast XZV-2 ook regelafsluiter FC-8 laat sluiten.

Met deze aanpassingen en een testfrequentie van eens per vier jaar voldoet deze instrumentele hoogniveaubeveiliging wel aan de SIL-2-eisen.

Referenties:

- IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems (2000).
- IEC 61511: Functional Safety - Safety Instrumented Systems for the Process Industry Sector (2003).