

Het risico van LOPA en SIL Classificatie

Valkuilen bij procesveiligheid

NVVK Veiligheidscongres 2009

Ir. C.M. Pietersen
Safety Solutions Consultants BV
pietersen@safety-sc.com

1. Samenvatting

Risico evaluatie methoden worden in toenemende mate toegepast in de proces industrie. Dit vooral onder invloed van de wereldwijd ingevoerde internationale standaard NEN- EN- IEC 61511. Deze standaard vereist een risico benadering: hoe hoger het risico, hoe hoger de eisen zijn die gesteld worden aan (instrumentele) beveiligingen. Het risico niveau wordt uitgedrukt in een SIL: Safety Integrity Level. De risico analyse wordt wel SIL Classificatie of LOPA analyse (Layer Of Protection Analysis) genoemd. Het risico van Loss of Containment (LOC) scenario's (geïdentificeerd vanuit een HAZOP studie) dient te worden bepaald en te worden vergeleken met een door het bedrijf te definiëren risico acceptatie criterium. Daaruit volgt de noodzaak voor risicoreductie uitgedrukt in een SIL. Vervolgens dient een (combinatie van) beveiliging te worden ontworpen die kan voldoen aan de eisen die horen bij het SIL niveau. Hiermee is het risico van LOC scenario dus tot een acceptabel laag niveau terug gebracht.

Als de hier beschreven benadering correct wordt toegepast (gegeven de complexiteit van procesveiligheid) dan levert dit een consistente, verifieerbare benadering op voor procesveiligheid. Helaas is de praktijk van het toepassen van de SIL en LOPA benadering niet altijd zodanig dat dit het geval is. De benadering bevat de nodige valkuilen waardoor de veiligheid zelfs onder druk kan komen te staan. Het doel van dit paper is om deze te benoemen zodat de lezer die kan vermijden en uiteindelijk de veiligheid ermee gediend is.

In dit paper en de presentatie worden de verschillende aspecten van de SIL classificatie benadering die niet bijdragen aan de beoogde risico reductie besproken. Voorbeelden worden gegeven vanuit een grote praktische ervaring in de industrie. Het betreft onder andere:

- Het oneigenlijk gebruik van de SIL benadering om een inherent onveilig ontwerp te rechtvaardigen (bijvoorbeeld het afblazen naar atmosfeer)
- Het toekennen van onterecht grote risico reductie factoren aan de mogelijkheid van ingrijpen van een operator
- Het gebruik van generiek, niet verifieerbare risico reductie factoren voor beveiligingen met behulp van LOPA.
- Grote verschillen tussen SIL Classificatie met behulp van LOPA en ander methoden zoals een risicograaf of risico matrix.
- Het ontbreken van een correcte implementatie van de beveiligingen in het veiligheid management systeem.

2. Kwantificering van risico

Technisch opgeleide mensen willen in het algemeen graag de verschillende aspecten van het ontwerp en dus ook veiligheid in cijfers uitdrukken. Dat geeft de noodzakelijke rationele en objectieve basis voor een ontwerp van een technisch systeem zoals een procesinstallatie. Voor het beoordelen van het risico van een installatie is dat echter niet altijd mogelijk, c.q. wenselijk. Wat is de kans op onveilig handelen van een operator? Wat is de kans op falen van een dijk rond een opslagtank? Etc. Van de andere kant hebben we die kansen nodig, met alleen de (onzekere) bepaling van de effecten van een scenario hebben we geen basis voor risicoreducerende maatregelen. Het komt erop neer dat we het risico moeten kwantificeren en ons daarbij bewust moeten zijn van de valkuilen. Anders worden de verkeerde conclusies getrokken op basis van de risico analyse. Een te sterke focus op kwantificering is dan een risico.

Toch is de nadruk op kwantificering voor procesveiligheid sterk. Dit mede onder invloed van de SIL normen (die kwantificatie trouwens zelf sterk nuanceren) in opkomst. Het wordt ons ook 'gemakkelijk' gemaakt. Zo vinden we de cijfers die we nodig hebben zonder veel moeite in de literatuur. Die vinden we bijvoorbeeld in het LOPA boek van de CCPS¹. Wat is echter de basis ervan? Die zou transparant en verifieerbaar dienen te zijn. Zo wordt bijvoorbeeld geponeerd dat een pomp seal (afdichting) falen plaats vindt met een frequentie van 0,1 per jaar en dat een dijk rond een opslagtank een kans op falen op aanspraak heeft van 0,01. Natuurlijk wordt erbij gemeld dat het voorbeelden zijn en dat er voorzichtig mee moet worden omgesprongen. Er wordt echter in de praktijk veel naar gerefereerd in risico analyses. We hebben nu eenmaal cijfers nodig. Kwantificering van faalkansen wordt vereist door de NEN- EN IEC 61508/ 61511 in het kader van de SIL risico benadering. Deze normen geven daarbij aan dat de faalkansen onderbouwd moeten worden met faalgegevens uit de praktijk, en met name de praktijk van de eigen installaties. Verder wordt gewaarschuwd dat we op deze manier uitsluitend technisch (random) falen meenemen. De minstens even belangrijke aspecten van systematisch falen (bv menselijke fouten) dienen dus op een andere wijze in de beschouwing te worden meegenomen. Kwantificeren daarvan is nog lastiger en wordt vaak niet meegenomen. Dat is een belangrijke omissie, menselijk handelen is immers een belangrijke risico factor (zowel in het veroorzaken als het herstellen). We moeten ons dus realiseren dat kwantificeren slechts een deel is van een beschouwing over risico en risico reductie.

Het probleem met kwantificeren

Dit probleem wordt mooi geïllustreerd in *The Hitchhiker's Guide to the Galaxy* (Douglas Adams). In het boek hebben hyper intelligente wezens de grootste computer ooit van het hele universum gebouwd. Deze computer heet 'Deep Thought'. De computer is gebouwd om eindelijk het ultieme antwoord te geven op de 'Grote kwestie van Leven, het Universum and Alles'. Men verzoekt om een simpel antwoord. De computer heft 7,5 miljoen jaar van rekenen nodig om het antwoord te geven. Daar wordt met spanning naar uitgekeken.

De teleurstelling is echter groot als het antwoord 42 blijkt te zijn.



"Tweeënveertig?!" Is dat alles wat je ons kan tonen na zeven en een half miljoen jaar rekenen? "Ik heb het antwoord zorgvuldig gecontroleerd" zegt Deep Thought dan, "en ik weet zeker dat dit het antwoord is. **Om eerlijk te zijn, ik denk dat het antwoord niet het probleem is. Misschien hebben jullie nooit goed nagedacht over de vraag**".

¹ Layer Of Protection Analysis- Simplified Process Risk Assessment; CCPS 2001

We vragen niet naar een cijfer, het gaat om procesveiligheid in zijn totaliteit. Als je niet de juiste vraag stelt krijg je ook niet het juiste antwoord! Hoe interpreteer je een cijfermatig resultaat voor veiligheid? Wat worden de maatregelen als bv 42 het resultaat is? Zie het kader hierboven.

3. Oneigenlijk gebruik van de SIL benadering voor inherent onveilige situaties

Dit kan het best geïllustreerd worden door een tweetal (gesimplificeerde) praktijk voorbeelden.

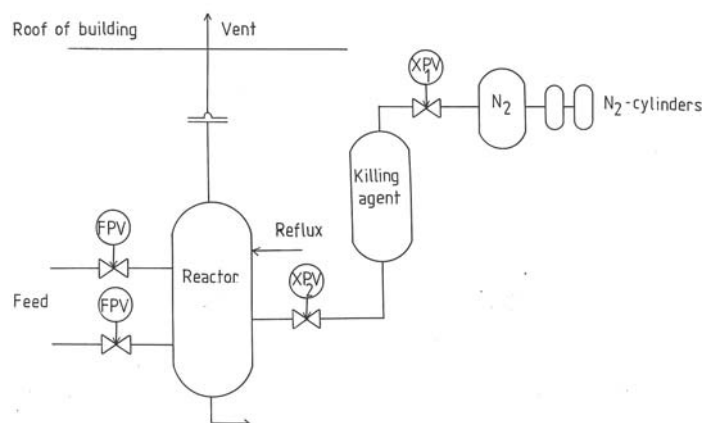
Reactor runaway beveiliging

De case betreft een reactor overdruk beveiliging (breekplaat) die aflaat naar atmosfeer op het dak van het reactorgebouw. Zie figuur 1. Het scenario is een mogelijke runaway reactie. Om te voorkomen dat de breekplaat moet aanspreken is er een 'reactie killing' systeem geïnstalleerd. Er is hier dus in feite sprake van twee scenario's :

- Het barsten van de reactor bij hoge druk door een runaway reactie. Daarvoor is de breekplaat de beveiliging.
- Het barsten van de breekplaat met als gevolg dat de reactorinhoud naar buiten komt op het dak. De beveiliging daartegen is het killing systeem.

Twee scenario's, geclassificeerd als SIL 2 and SIL 1 respectievelijk. Wat is het probleem? Enigszins zwart-wit gesteld: de SIL benadering wordt hier gebruikt om een inherent onveilige situatie (gaswolk over het dak naar de omgeving) te rechtvaardigen. Het alternatief, bv afblazen naar fakkel of een gesloten systeem wordt zo vermeden en de nodige kosten bespaard².

Figure 1 Reactor met beveiligingen



Het overvullen van een LPG opslag bol

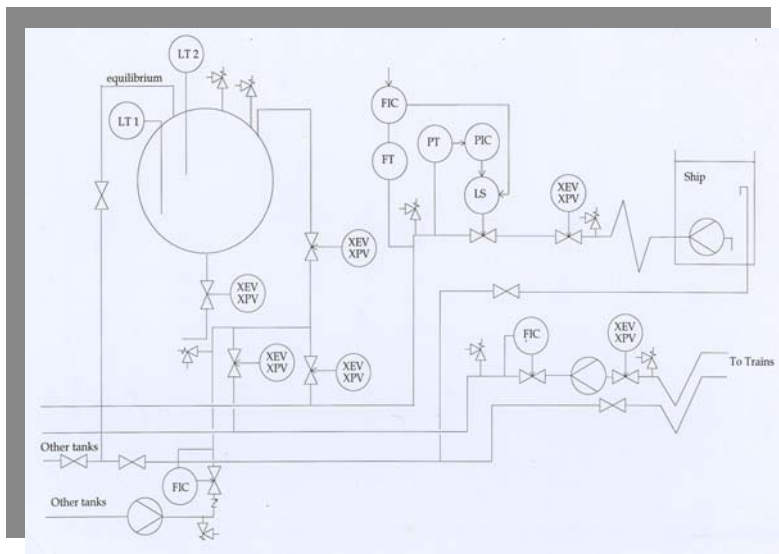
Zie figuur 2. De bol kan worden gevuld vanuit drie locaties: een schip, een spoorketel wagen en vanuit een andere LPG opslagtank. Vanuit de HAZOP studie is geconcludeerd dat in het geval van overvullen (het volledig vullen) van de bol er een zodanige overdruk ontstaat dat er kleinere (flenzen) en zelfs grotere lekken (scheuren

² Een vergelijkbaar probleem is naar voren gekomen in de analyse van de BP Texas ramp (VS, 2005): onveilig afblazen naar atmosfeer. Budgetten om dat aan te passen sneuvelden verschillende malen.

bol) kunnen optreden. Dit scenario wordt veroorzaakt door de hoge persdruk van de toeleverende pompen. Het scenario is vervolgens door het HAZOP team

geclassificeerd als SIL 3. Dit betekent dat het risico van dat scenario een factor 1000 - 10.000 te hoog wordt geacht. Om het risico te reduceren naar een aanvaardbaar niveau is er een SIL 3 overvulbeveiliging voorgesteld en geïnstalleerd. Ook hier rechtvaardigt deze beveiliging schijnbaar een inherent onveilige situatie die niet acceptabel is: de bol kan worden beschadigd door de pompdruk, leidend tot een ramp. De enige juiste beveiliging hier is dat er zodanige pompen worden geïnstalleerd dat dit probleem geheel verdwenen is. Inherent veilig (wat dit aspect betreft).

Figure 2 LPG opslag en vul systeem



4. Het risico van een SIL geclassificeerde Instrumentele Beveiliging.

Het bepalen van de noodzakelijke risicoreductie via de SIL Classificatie dient gevolgd te worden door het ontwerpen van een beveiliging die aan de eisen die behoren bij het SIL voldoet. Voor bestaande beveiligingen dient geverifieerd worden of er aan voldaan wordt. De SIL verificatie vereist specialistische kennis en bruikbare faalgegevens. Beiden zijn in de praktijk vaak een probleem. Als de verificatie niet goed wordt uitgevoerd kan dat leiden tot een installatie die onder- of over beveiligd is. Beide situaties zijn ongewenst.

Voorbeelden van aspecten die regelmatig over het hoofd worden gezien.

Een belangrijk aspect bij SIL verificatie is de controle op functionaliteit: voorkomt de beveiliging met 100% zekerheid het scenario (bij functioneren, er wordt wel een zekere faalkans geaccepteerd). Worden de juiste en voldoende acties uitgevoerd (bv sluiten van *alle* relevante afsluiters). Een ander aspect is dat een nieuw ontworpen beveiliging een nieuw gevaar introduceert (als bv een van de afsluiters die dicht moet faalt). Dit dient in een HAZOP beschouwd te worden.

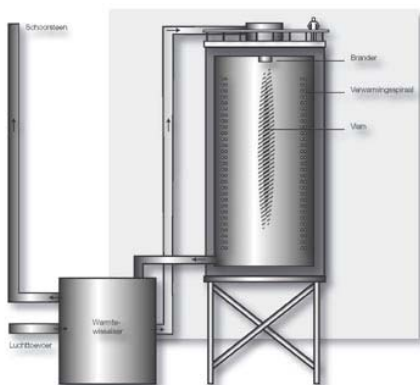
De eerste stap bij het beoordelen van beveiligingen van een procesinstallatie dient altijd een systematische gevaaridentificatie studie (meestal HAZOP) te zijn. Dit is ook conform de IEC 61511 standaard. Als dit niet of onvoldoende plaatsvindt kunnen scenario's over het hoofd worden gezien en is de installatie onderbeveiligd. Anders gezegd: Het risico is dan hoger dan door het bedrijf zelf acceptabel wordt geacht.

5. Onvoldoende implementatie in een SIL Safety Management Systeem

De NEN- EN- IEC 61511 standaard betreft het borgen dat de risico's voldoende worden gereduceerd en dat ook te handhaven over de levensduur van de installatie. De SIL Classificatie en –Verificatie is slechts een onderdeel ervan. Het vereist dat de beveiligingen 'fit for purpose' blijven en bv niet worden overbrugd (of onder strikte voorwaarden). SSC onderzocht destijds met behulp van de Tripod methode het incident dat hieronder wordt beschreven. Daarbij speelde het niet correct overbruggen van essentiële beveiligingen een rol. Bij de start-up van de installatie was de overbrugging onterecht nog niet terug genomen.

Explosie in a gas gestookte installatie (DSM , 1 April 2003)³.

Het incident betrof een explosie tijdens de start-up van in de installatie (zie de figuur hieronder). Het werd een ramp doordat er op dat moment drie mensen boven op stonden. Die hebben dat helaas niet overleefd. De explosie kon plaatsvinden omdat de start-up werkinstructies niet volledig gevolgd werden. Dit resulteerde in het feit dat de beveiliging niet functioneel was: De beveiligingsafsluiters waren nog open/ overbrugd. Dat maakte het mogelijk om gas naar de installatie te sturen onder onbeveiligde omstandigheden. Het betrof hier dus niet een probleem met de SIL Classificatie en/of SIL verificatie van de beveiliging maar een onderdeel van het 'SIL' beheerssysteem. Ook volgens de IEC 61511 is dit een vitaal aspect. Het betreft o.a. onderdelen van menselijk handelen zoals de kwaliteit van de werkinstructie en het toezicht op het volgen ervan.



6. Conclusie

De door de NEN –EN IEC 61508/61511 normen gegeven risico benadering ('SIL') is een belangrijke doorbraak bij het 'fit for purpose' beveiligen van procesinstallaties. Mede doordat de SIL/ LOPA benadering relatief nieuw is zijn er echter de nodige problemen bij een juiste implementatie ervan. Daarmee wordt het gevaar gelopen dat de installatie niet juist beveiligd is, met alle gevolgen van dien. In dit paper zijn verschillende aspecten van de risk evaluatie/ SIL Classificatie benadering gepresenteerd vanuit onze praktijkervaring op dit gebied. Door het vermijden van de genoemde valkuilen wordt de veiligheid beter gediend. Tot slot: Methoden als SIL/ LOPA zijn geen doel maar middel, veiligheid blijft het centrale doel.

³ De gegevens zijn door DSM openbaar gemaakt zodat breed in de industrie lessen kunnen worden geleerd.