De Scenario audit

Voorstel voor een methode ter preventie van incidenten en rampen in de procesindustrie

Christo Zemering[1], Paul Swuste[2]

Samenvatting

Grote incidenten en rampen binnen de chemische industrie blijven zich voordoen, ondanks de invoering van veiligheidsmanagementsystemen en de omvangrijke wet- en regelegeving rond procesveiligheid. Bedrijven met Amerikaanse vestigingen dienen te voldoen aan het Process Safety Management System (PSM) programma van de Amerikaanse wetgeving. Als gevolg van recente incidenten en rampen is een studie gestart om de bestaande audit techniek te verbeteren. De huidige PSM audit techniek kent een aantal belangrijkste tekortkomingen, zoals een onvoldoende gevaarherkenning voor rampen en incidenten, een losstaande beoordeling van de elementen van het managementsysteem en beperkte beoordeling van de menselijke factor. In dit artikel wordt de 'scenario audit techniek' gepresenteerd. Het centrum van deze techniek is het zogenaamde 'vlinderdas model'. Een groot voordeel van dit model is de prominente plaats van het scenario met de mogelijkheid om meervoudige oorzaken van incidenten en rampen op te stellen. Voor ieder scenario worden barrières gedefinieerd en geaudit. Door het barrière concept niet alleen te beperken tot technische onderdelen, maar ook uit te breiden met management factoren, wordt een integrale beoordeling van management systemen mogelijk, inclusief de menselijke factor. De scenario audit techniek wordt geillustreerd aan de hand van een voorbeeld van een stofbrand/explosie binnen en buiten een installatie.

Het gepresenteerde onderzoek is een afstudeerproject geweest van de post graduate opleiding 'Management of Safety Health and Environment (MoSHE) van de Technische Universiteit Delft.

Summary

Despite the implementation of Safety Management Systems and many regulations on process safety, major chemical incidents and disasters continue to happen. The international operating process industry with American branches has to comply with the Process Safety Management System (PSM), according to OSHA law. Due to recent incidents and disasters, a study was conducted to improve the current PSM audit technique. Insufficient hazard recognition, a focus on the quality of individual elements of management systems, and an inadequate assessment of human factor aspects are the main shortcomings of this PSM audit.
A scenario-based auditing technique is presented in this paper, using the bow tie model as a centre of this technique. The major advantage of the bow tie model is the focus on scenarios and the possibility to consider multiple causes of incidents and disasters. Barriers are defined and audited, and by expanding the barrier concept not only to hardware issues, but also management factors an integral assessment safety management system becomes possible, including the human factor. The scenario-based audit is explained with an example of a dust fire/explosion in or outside an installation.

The research presented in this paper is based on a final report of the post-graduate master course 'Management of Safety, Health and Environment' of the Delft University of Technology.

Inleiding

Grote ongevallen en rampen blijven de industrie achtervolgen. Alleen al bij de chemische industrie is binnen de Europese Unie een gestage stijgende trend te zien en sloot het jaar 2001 af met 450 geregistreerde grote incidenten (European Commission, 2002). De explosie in de bestrijdingsmiddelenfabriek nabij het centrum van Toulouse in 2001, waarbij 30 mensen omkwamen en ongeveer 2500 gewond raakten, zal iedereen zich nog wel herinneren.

Ook Nederland wordt met enige regelmaat opgeschrikt door industriële rampen. In januari 2003 barstte een atmosferische opslagtank met ortho-cresol tijdens het vullen open, doordat de lasnaad aan de onderkant scheurde. De inhoud kwam vrij, de tank stortte in en een golf van stank verspreidde zich over de omgeving. De oorzaak van het incident was opvallend eenvoudig: een combinatie van een dertigjarige constructiefout en een reparatie, die niet goed was uitgevoerd. De fouten zijn nooit gedetecteerd bij enige inspectie en dit leidde uiteindelijk tot het bezwijken van de tank. Het bedrijf waar het incident gebeurde was geen kleine onderneming, maar een bedrijf met een veiligheidsmanagementsysteem en een kwaliteitssysteem. Er waren arbeidsveiligheidsrapporten en externe veiligheidsrapporten

[1] *General Electric Plastics, Plant Manager Lexan Chemops, Mt Vernon, Indiana. voormalig Environment, Health and Safety Leader Europe, christo.zemering@gep.ge.com*
[2] *Sectie Veiligheidskunde, Technische Universiteit Delft*

opgemaakt en er was uitgebreid geïnspecteerd (Ale, 2003). Vier maanden later ontplofte in een groot chemisch bedrijf een gasgestookte oven tijdens onderhoudswerkzaamheden. Tijdens de werkzaamheden bleven de toevoerkleppen van de gasleiding open staan en ontstond er een explosief mengsel. Deze ramp eiste drie slachtoffers. Ook bij dit bedrijf was een veiligheidsmanagement systeem actief en werden diverse veiligheidsaudits uitgevoerd. Schijnbaar zijn deze systemen en audits onvoldoende in staat om alle rampen te voorkomen. Dit artikel gaat nader in op procesveiligheidsaudits aan de hand van de onderstaande vragen:

1. Waarom zijn rampen en incidenten onvoldoende met procesveiligheidsaudits te signaleren?
2. Welke aanpassingen van procesveiligheidsaudits zijn nodig om in een vroegtijdig stadium ramp- en incidentscenario's te herkennen en te voorkomen?

De procesveiligheidsaudit uit dit artikel is uitgevoerd binnen de chemische tak van een multinationaal bedrijf. Vanwege de Engelse voertaal van het bedrijf zijn een aantal termen en figuren in de oorspronkelijke taal weergegeven.

Methoden en technieken

Ter beantwoording van de eerste vraag is een literatuuronderzoek uitgevoerd naar oorzaken van rampen en incidenten en naar wettelijke eisen voor procesveiligheidsaudits. Rampen zijn hierbij omschreven als gebeurtenissen waarbij ernstige of dodelijke slachtoffers te betreuren zijn in combinatie met grote materiële schade. Bij incidenten is er alleen sprake van grote materiële schade. Vervolgens zijn voor de periode 2000-2003 uit een bestand van totaal 100 ramp- en incidentrapporten uit de procesindustrie, 34 rapporten geselecteerd. Deze rapporten zijn ter beoordeling voorgelegd aan een groep van 4 experts; een ervaren veiligheidskundige van een afdeling Environment, Health and Safety en van een afdeling Proces Safety Management het hoofd, een ervaren ingenieur en een ervaren technicus. De selectie van de rapporten is gebaseerd op de mate van volledigheid van de aanwezige informatie. De rapporten behandelen een reeks van gebeurtenissen, variërend van chloorgasontsnappingen tot extruder branden en stofexplosies. Ieder rapport is eerst door de individuele experts becommentarieerd en vervolgens binnen de groep besproken. Aan iedere ramp of incident zijn één of meerdere primaire oorzaken toegekend die zijn onderverdeeld in fysische, organisatorische en mensgerichte oorzaken volgens de indeling van de Amerikaanse Occupational Safety and Health Administration wetgeving (OSHA Standard, 1992); het Process Safety Management System (PSM) (tabel 1).

De tekortkomingen van de procesveiligheidsaudits uit de eerste onderzoeksvraag hebben geleid tot aanpassingen en tot een voorstel voor een audittechniek waarbij mogelijke ramp- en incidentscenario's centraal staan. Eén toepassing van deze techniek, de zogenaamde 'scenario audit' zal als voorbeeld worden uitgewerkt.

Resultaten

Oorzaken van rampen en incidenten

Over oorzaken van rampen en incidenten bestaat al een uitgebreide bibliotheek aan literatuur (zie oa Hale ea, 1998). Tijdens de beginperiode, voor de Tweede Wereldoorlog, werd veiligheid sterk gedomineerd door ingenieurs, die de preventie vooral in technische aanpassingen zochten. In deze periode werd ook de 'accident-proneness theorie' geboren; sommige werknemers veroorzaken meer ongelukken en rampen dan anderen en die eigenschap was onlosmakelijk met bepaalde personen verbonden. Deze analyse van oorzaken leidde tot allerlei technische end-of-pipe maatregelen voor onderdelen van productieprocessen en tot selectieprocedures en trainingprogramma's voor werknemers. Uit deze tijd stamt ook de beroemde 80-20 regel; 80% van de ongevallen, incidenten en rampen zijn te wijten aan een menselijke fout (Heinrich, 1931). Omdat deze regel zo prettig eenvoudig is en de schuldvraag afdoende lijkt te beantwoorden is de 80-20 regel nog steeds een gevleugeld gezegde.

Tabel 1 Typering van oorzaken van incidenten en rampen volgens het Amerikaanse Process Safety Management System

Type oorzaken	Uitleg
Fysische oorzaken	
Gevaren	onvoldoende gevaar herkenning en evaluatie
Onderhoud	falende mechanische integriteit en
Opstarten	onvolledige pre-start-up veiligheidsreview
Noodsituaties	onvoldoende planning en response op noodsituaties
Heet werk	onderhoud onjuist uitgevoerd werk bij hoge temperaturen
Organisatorische oorzaken	
Procedures	incorrecte procedures
Informatie	ontbrekende of incorrecte veiligheidsinformatie
Training	gebrekkige of afwezige training
Ongevallen	herhaalde ongevallen volgens dezelfde scenario's
Audits	niet opgevolgde audit resultaten
Veranderingen	onvoldoende managen van aangebrachte proceswijzigingen
Mensgerichte oorzaken	
Werknemers	onvoldoende werknemers participatie
Mens	menselijke factor

Hoewel deze aanpak tot op zekere hoogte succesvol is geweest werd, onder invloed van psychologen en ergonomen, de mens-machine relatie steeds vaker als oorzaak gezien en minder de individuele werknemer. Vanaf de jaren zestig doet de 'menselijke factor' zijn intrede in de analyse. Onder invloed van de grote ramp in Flixborough (1974) in Groot-Brittannië ontstond er een groeiende aandacht voor managementaspecten van deze gebeurtenissen. De menselijke factor werd daarbij uitgebreid tot de beslissingen van managers en opzichters en de consequenties van deze beslissingen voor de veiligheid en integriteit van productieprocessen. Rond 1980 drong het besef door dat veiligheid een managementverantwoordelijkheid was, die in de lijn van de organisatie geplaatst moet worden in plaats van bij de stafafdeling veiligheid. De oorzaak van rampen uit deze periode (onder andere Bopal, Piper Alpha, Chernobyl, Challenger, Herald of Free Enterprise) werd gezocht in de nog spaarzaam begrepen interacties tussen technische en sociale aspecten van systemen en het management werd steeds meer als grote boosdoener gezien.

De laatste jaren is naast de directe fysische oorzaken van een ramp of incident een verdere verdieping te zien in de organisatorische oorzaken van rampen en incidenten. De grootste dreiging komt niet meer van een geïsoleerde menselijke fout van een werknemer vlak voordat de ramp zich voltrekt, maar in het vertraagde effect van menselijke beslissingen binnen de organisatie. Menselijke fouten worden niet meer opgevat als oorzaak, maar als consequentie van organisatorisch falen (Reason, 1997). Hierbij is de organisatie niet primair beperkt tot het managementsysteem van het lokale bedrijf, waar de ramp heeft plaatsgevonden, maar omvat eveneens het topmanagement, de wetgever en de inspecterende instanties. Een zeer lezenswaardig en goed voorbeeld van een dergelijke opvatting is de uitgebreide analyse van een gasexplosie in Longford, Australië, waar een aantal dodelijke en zwaar gewonde slachtoffers vielen en waar de gehele staat Victoria twee weken lang zonder gas kwam te zitten (Hopkins, 2000).

Rampen en incidenten hebben doorgaans meerdere fysische oorzaken. De gevaarsherkenning en -evaluatie is daarbij een essentieel instrument om dit type oorzaken te kunnen achterhalen. Dit geldt niet alleen voor de normale procesgang, maar ook voor speciale werkcondities zoals onderhoud, werk onder hoge temperaturen, storingen, opstartcondities van processen etc. Een gebrekkige of afwezige gevaarherkenning wordt in de literatuur regelmatig als oorzaak genoemd naast de technische maatregelen, die doorgaans veel te laat in de rampsequentie ingrijpen en alleen tot doel hebben om de topgebeurtenis, de feitelijke ramp of het incident, te voorkomen (zie onder andere Centre for Chemical Process Safety, 1994; Kletz, 1999; Rasmussen, 1993; Swuste ea., 2002; US Chemical Safety and Hazard Investigation Board, 2002).

De oorzaak van rampen en incidenten kunnen ook besloten liggen in de gebruikte technologie. Perrow (1999) heeft daar de vrij cynische term 'normal accidents' aan gegeven. Als de complexiteit van een proces groot is en de opeenvolgende processtappen kort in de tijd gekoppeld zijn, dan is de procesinformatie voor werknemers verwarrend en de tijd om bij storingen in te grijpen zeer beperkt. Onder deze procescondities zijn rampen en incidenten onvermijdelijk. In Nederland is dit model met succes toegepast bij een chocolade zoetwaren bedrijf (Blom en Swuste, 2002).

Een gebrekkige of afwezige gevaarherkenning en -evaluatie impliceert ook dat werkprocedures en training slechts beperkt zijn toegesneden op de feitelijke werkzaamheden. In de Longford fabriek waren storingen aan de orde van de dag. Onder druk van de markt en commerciële belangen werden deze condities geaccepteerd en op den duur als normaal beschouwd. Daardoor waren werknemers bij voorbaat al gedwongen om af te wijken van de gebrekkige procedures, omdat anders de fabriek direct stil zou komen te liggen. Dit plaatst de menselijke factor in een bijzonder licht en laat zien dat dit type knelpunten een oorsprong in de organisatie heeft.

Ook het topmanagement van de Longford vestiging heeft een dominante rol gespeeld in de aandacht voor veiligheid bij de locale fabriek. Het bedrijf beschouwde zichzelf als een van de veiligste bedrijven binnen de sector, door voortdurend te wijzen op de 'nul-ongevallen' doelstelling. De Australische vestiging had voor dat resultaat zelfs een nationale prijs ontvangen, een jaar voordat de ramp plaatsvond. Deze fixatie op ongevallencijfers, als enig meetpunt voor de veiligheid, is niet uniek voor dit bedrijf. Veel bedrijven hanteren direct meetbare empirische gegevens voor de optimalisatie van hun processen en daar is veiligheid geen uitzondering op. Een veiligheidsbeleid dat alleen gebaseerd is op ongevallencijfers en wedstrijdelementen inbouwt om de getallen zo laag mogelijk te houden, stimuleert tegelijkertijd een praktijk van onderrapportage. Nog afgezien van de vraag of een laag ongevallencijfer enige indicatie geeft over toekomstige ongevallen of rampen. Vooral dat laatste punt, de relatie tussen rampen en ongevallen is de laatste jaren onderwerp van discussie (zie onder andere Bari, 2000; Hale, 2002; Rasmussen, 1993; Salminen ea, 1992; Saloniemi en Oksanen, 1998; Visser, 1998). Deze vraag is terecht, omdat men tot op heden met de bestrijding van de hoge frequentie van de kleinere ongevallen nog weinig succesvol is geweest in het voorkomen van rampen en incidenten. Kleinere ongevallen, al dan niet met verzuim, zijn pas zinvolle indicatoren van grotere rampen, indien de ongevalscenario's onderdeel zijn van rampscenario's. Verder is er in veel bedrijven sprake van een selectiemechanisme, waardoor positieve boodschappen zoals een lage of afwezige ongevalfrequentie veel sneller tot het topmanagement doordringen dan tegenvallende resultaten van een veiligheidsaudit. Slecht nieuws baant zich doorgaans maar moeizaam een weg door de bedrijfshiërarchie heen. Resultaten van veiligheidsaudits zijn niet vaak onderwerp van vergaderingen van het managementteam van het hoofdkantoor, omdat deze rapportages doorgaans omvangrijk en technisch zeer gedetailleerd zijn en geen duidelijke informatie verschaffen over de kans op een ramp.

In reactie op Perrow's model van de 'normal accidents' is de theorie van de zogenaamde 'high reliability organisations' (hro) ontstaan. Deze hro's kunnen zich geen incidenten en rampen

veroorloven, omdat de gevolgen catastrofaal zijn en de bedrijfstak, de overheid en de publieke opinie eenvoudigweg dergelijke gebeurtenissen niet accepteren.
Luchtverkeersleidingen en nucleaire installaties zijn voorbeelden van hro's. Bij deze organisaties staat veiligheid in het centrum van hun bedrijfsvoering. Ze zijn nauwelijks geïnteresseerd in de goed nieuws boodschappen van nul-ongevallen, maar hebben een aantal indicatoren ontwikkeld om afwijkingen van de normale procesgang in een vroegtijdig stadium te signaleren (Weick ea, 1999). In de nucleaire industrie zijn ongeplande reactor shut downs voorbeelden van dergelijke indicatoren, of het aantal keer dat een veiligheidssysteem automatisch is geactiveerd (Rees, 1994). Deze gebeurtenissen zijn altijd aanleiding voor nader onderzoek, waarbij gekeken wordt of de sequentie van gebeurtenissen past in een groter ramp- of incidentscenario. De bedrijven zijn gericht op storingen en gaan a-priori niet van geïsoleerde gebeurtenissen uit. Het registratiesysteem voor storingen is zeer sterk ontwikkeld en de onderhoudsafdelingen van de hro's zijn locaties voor zogenaamd 'organisatorisch leren' (Carroll ea, 2002; Hale ea, 1997; Kjellen, 2000; Koornneef, 2000).

Wettelijke eisen aan procesveiligheidsaudits

In Amerika bestaan twee programma's van wet- en regelgeving die voor procesveiligheid relevant zijn; het Process Safety Management System (PSM) van OSHA en het Risk Management Program (RMP) van het Environmental Protection Agency (EPA) (OSHA Standard, 1992; EPA, 2004). De internationaal opererende procesindustrie met vestigingen in Amerika moet aan deze regelgeving voldoen. Bedrijven die toxische of brandbare chemicaliën gebruiken die op de lijst van de programma's voorkomen, dienen aan de eisen van de programma's te voldoen. Voor het PSM-programma geldt een grens in de omvang van het chemicaliëngebruik. Het programma is alleen van toepassing als deze grens wordt overschreden.

Het PSM-programma van OSHA bestaat uit 14 elementen die, wanneer correct geïmplementeerd, een bedrijf een hoge standaard moeten geven in de preventie van rampen en incidenten (tabel 2). De procesveiligheidsaudits van het PSM-programma worden regelmatig uitgevoerd door een team van onafhankelijke veiligheidsexperts. Binnen een gemiddeld tijdsbestek van een halve dag per element per fabriek controleert het auditteam aan de hand van vragenlijsten de aanwezigheid van de vereiste documentatie, interviewen zij enkele werknemers en beoordelen zij de feitelijke procescondities ter plekke. Voor deze 14 elementen zijn standaarden ontwikkeld en richtlijnen voor implementatie (Collins, 2004). De vragen van de procesveiligheidsaudit volgens PSM leidt tot een score op de elementen uit tabel 2. Deze score wordt als percentage gepresenteerd. De uniforme PSM audit maakt een vergelijk tussen bedrijven mogelijk. De scores zijn verbonden aan een oordeel en een tijdspad waarbinnen de geconstateerde tekortkomingen verholpen moeten zijn. Het RMP van de EPA is vergelijkbaar van opzet als het PSM-programma en omvat dezelfde elementen, alleen is dit programma gericht op de milieueffecten van een (on)geplande uitstoot van chemicaliën en vereist dat bedrijven worst case scenario's ontwikkelen.

In Europa reguleert de Seveso II richtlijn de rampen en incidenten met gevaarlijke chemicaliën (Oh, 2002). De audit, die op de richtlijn is gebaseerd, wordt in ons land uitgevoerd door een team, bestaande uit vertegenwoordigers van de provinciale overheid, de Arbeidsinspectie en de regionale brandweer. Anders dan het PSM-programma bevat de Seveso II richtlijn twee risiconiveaus voor bedrijven. Afhankelijk van de hoeveelheden, het aantal en de type chemische stoffen worden bedrijven ingedeeld in een lage of in een hoge risicocategorie. Bedrijven uit een lage risicocategorie moeten een preventiebeleid zware ongevallen (PBZO) voeren en over een veiligheidsbeheersysteem beschikken om dat PBZO-beleid uit te voeren. Bedrijven uit de hoge risicocategorie moeten daarnaast een veiligheidsrapport opstellen, een actuele stoffenlijst bijhouden en een intern noodplan maken dat regelmatig geoefend wordt. Binnen dit programma moeten eveneens worst case scenario's worden ontwikkeld en een aantal landen, waaronder Nederland, eisen een kwantitatieve risico beoordeling waarmee de risicocontouren worden vastgesteld, de zogenaamde 10^{-6} contouren. Europese vestigingen van internationale bedrijven, die reeds aan de PSA wetgeving voldoen, hoeven geen specifiek interne Seveso II audit uit te

Tabel 2 Overeenkomsten tussen de Amerikaanse Process Safety Management (PSM) en de Europese Seveso II Directive

OSHA 1910.119 Process Safety Management (PSM) of hHigly Hazardous Chemicals	Council Directive 96/82/EC SEVESO II
	Notification
	Major Accident prevention policy containing:
1 Employee participation	1 Organisation and Personel
2 Process safety information	2 Identification and evaluation of major hazards
3 Process hazard analysis	3 Operational controls
4 Operating procedures	4 Management of change
5 Training	5 Planning of emergencies
6 Contractors	6 Monitoring performance
7 Pre-start-up safety reviews	7 Audit and review
8 Mechanical integrity	
9 Hot work	Safety report
10 Management of change	
11 Incident investigation	
12 Emergency planning and response	
13 Compliance audit	
14 Trade secrets	

voeren, daar er veel overeenkomst bestaat tussen de elementen van de Amerikaanse en Europese programma's (tabel 2).

Maar een belangrijk onderscheid tussen het PSM-programma en de RMP/Seveso II richtlijnen zijn de scenario's. Het PSM-programma vereist geen ramp- en incidentscenario's, waardoor een bedrijf geen worst case hoeft te beschrijven en overeenkomstig geen scenario maatregelen te nemen. Verder kennen de programma belangrijke tekortkomingen. De implementatie van de elementen van de programma's worden tijdens audit losstaand beoordeeld in plaats van integraal, waardoor er nauwelijks een uitspraak over de kans op een ramp of een groot incident kan worden gedaan. Een tweede omissie is de stiefmoederlijke bedeling van de menselijke factor. In alle drie de programma's wordt de menselijke factor genoemd als een terrein waar aandacht aan besteed moet worden en veel verder komen de programma's niet.

Expert mening over oorzaken van rampen en incidenten

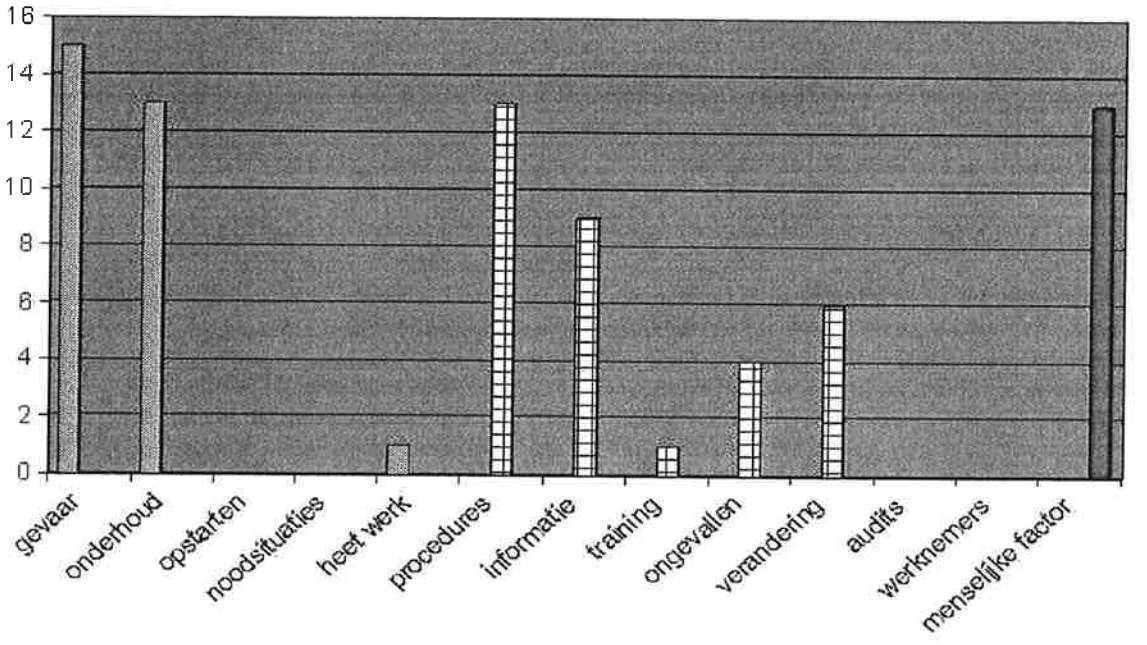
De resultaten van de mening van experts naar oorzaken van 34 rampen en incidenten staan weergegeven in figuur 1. Per rapport is meer dan één oorzaken aangegeven, waardoor de som van oorzaken veel hoger uitkomt dan het aantal bestudeerde rapporten.

ren die als achterliggende oorzaak voor de menselijke factor kunnen dienen.

Scenario Audit

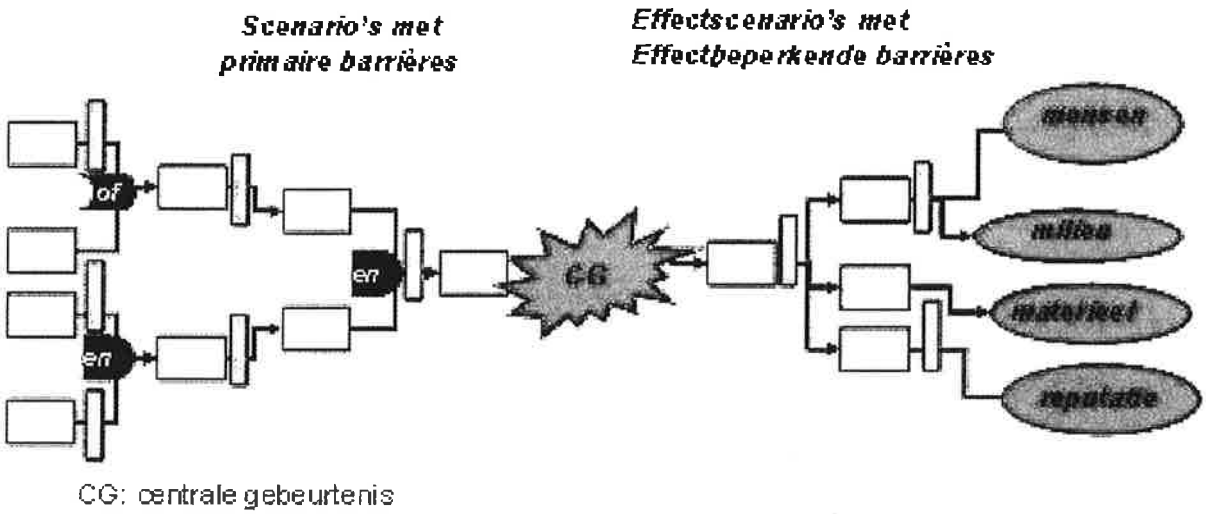
Om tegemoet te komen aan het commentaar op de veiligheidsaudit van het PSM-programma is een auditmethode ontwikkeld, de zogenaamde 'scenario audit'. De kern van de audit zijn één of meerdere scenario's met verschillende deelscenario's die tot een ramp of een groot incident kunnen leiden. De uitbreiding met deelscenario's is een belangrijke toevoeging, daar bij de meeste rampen meerdere scenario's betrokken zijn en de bestaande wetgeving en bijbehorende audits een dergelijke multicausale benadering onvoldoende onderzoeken. Het rampscenario wordt gepresenteerd volgens het 'vlinderdas-model' (figuur 2). Het vlinderdas-model is een bestaand model, dat reeds jaren gebruikt wordt bij de analyse van rampen en incidenten (Zuijderduijn, 1999; Petrolekas, 2001). Tot op heden is het model nog nauwelijks voor audit doeleinden gebruikt.

In het centrum van het model staat de centrale gebeurtenis (CG) met links een foutenboom en rechts een gebeurtenisboom. In de foutenboom van figuur 2 zijn twee deelscenario's aangegeven met 9 failures, of storingen. Falende apparatuur is een voorbeeld van een dergelijke storing. Deze deel-



Figuur 1 Oorzaken van 34 rampen en incidenten

De indeling in oorzaken in figuur 1 is overeenkomstig de typering van tabel 1. Oorzaken, die hun oorsprong in de organisatie hebben zijn in de meerderheid. Van de individuele oorzaken zijn de scores op sub-optimale gevaarherkenning, naast onderhoud en procedures het hoogst. Ook de menselijke factor heeft een hoge score. De informatie uit de rapporten laat een nadere analyse van de menselijke factor niet toe en er is geen onderscheid te maken tussen bijvoorbeeld een sub-optimaal niveau van ontvangen training, tijds- of productiedruk of andere factoscenario's geven aan hoe het gevaar, of de energie, via verlies van beheersing vrij kan komen. Een CG wordt ook wel met 'loss of control' of 'loss of containment' aangeduid. Voorbeelden van een CG zijn: een scheur in een tank, een emissie van een toxisch gas, een explosief mengsel in een reactor. In de foutenboom staan twee soorten poorten, de EN- en de OF-poort. Bij een OF poort is één storing voldoende voor de propagatie van het deelscenario. Indien meerdere storingen tegelijkertijd noodzakelijk zijn wordt een



Figuur 2 Vlinderdas model

EN-poort gebruikt. De balkjes in de figuur zijn de barrières. Deze barrières zijn op te vatten als blokkades, die de energiestroom van het gevaar reduceren of stoppen (Goossens, 2003). Aan de linkerkant zijn deze barrières de zogenaamde primaire barrières; zij voorkomen de propagatie van het deelscenario. Falende primaire barrières leiden tot de centrale gebeurtenis. Veiligheidskleppen in pijpleidingen is een voorbeeld van een primaire barrière. Aan de rechterkant van de figuur zijn de 'effect beperkende barrières', die de effecten van de centrale gebeurtenis beperken. De ramp of het incident staat aan het einde van de gebeurtenissenboom. Tijdens een scenario audit wordt alleen de linkerkant van het model tijdens groepssessies uitgewerkt, waarin naast leden van het auditteam zowel uitvoerenden, onderhoudspersoneel, als managers en ontwerpers van het locale bedrijf zitting hebben.

Voorbeeld van een scenario audit

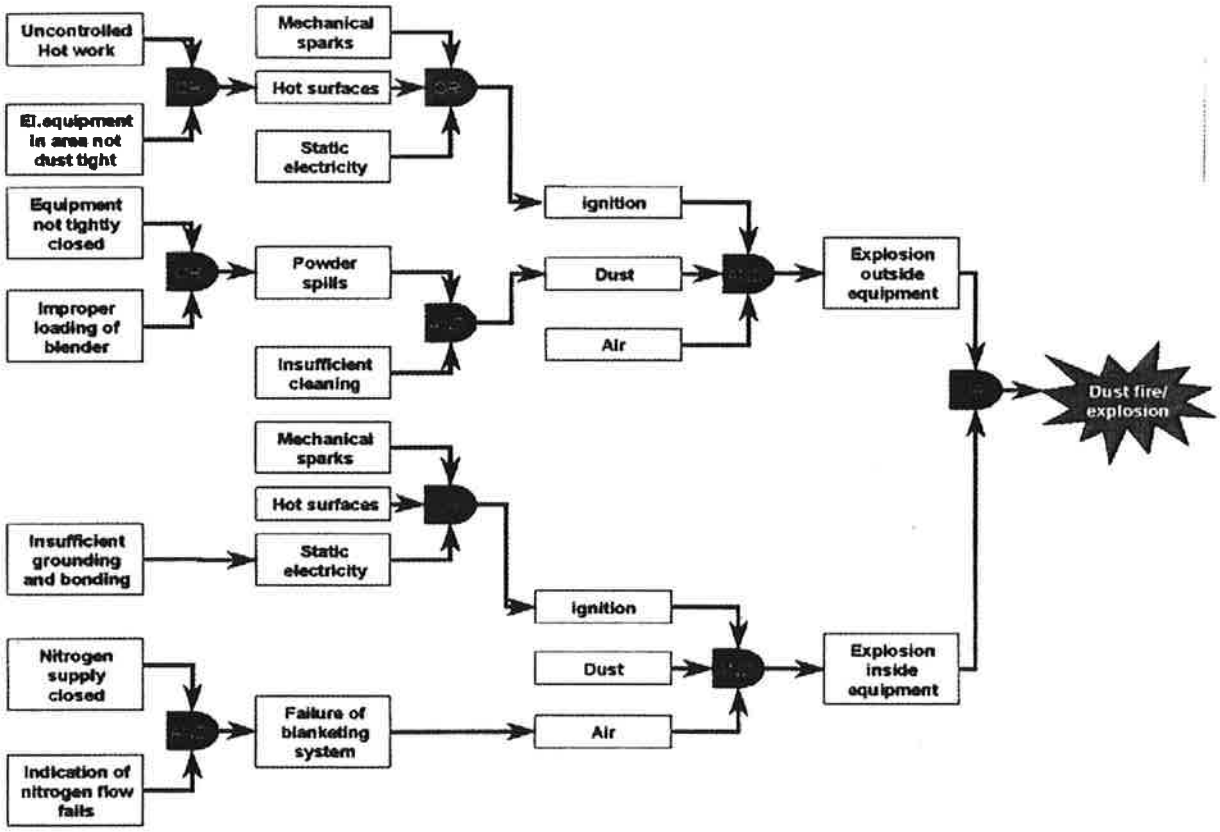
De groep, die de scenario audit uitvoert, doorloopt vijf stappen:

1. Het scenario start met de bepaling van de relevante centrale gebeurtenis (CG), of gebeurtenissen uit de bow tie. Cru gezegd wordt aan het team gevraagd de gebeurtenissen te benoemen waardoor een fabriek opgeblazen kan worden. Veelal betekent dit dat de installatie met het hoogste 'energieniveau' wordt geselecteerd. Andere bronnen, waarop de selectie kan berusten, zijn de veiligheidsrapporten volgens de Seveso II richtlijn, de ervaring van de aanwezigen, Process Hazard Analysis documenten, of historische rapportages van processtoringen. Indien de groep meerdere CG's kiest, dan dienen de scenario's in de volgende stappen separaat te worden opgesteld. Het is van belang de CG zo specifiek mogelijk te kiezen om tot realistische scenario's te komen in de tweede stap. Een CG als 'stofexplosie' is bijvoorbeeld minder specifiek dan 'stofexplosie in en buiten de installaties bij extruderlijn A'.

2. Vervolgens wordt de linkerkant van de bow tie, de foutenboom geconstrueerd. Hier worden de directe storingen en condities benoemd die leiden tot de gedefinieerde CG, de locaties van de storingen inclusief de EN- en OF-condities. In deze fase is de input van zowel uitvoerenden als onderhoudspersoneel van belang om alle condities, die noodzakelijk zijn voor een CG, te kunnen vaststellen. Het gevaar bestaat dat deze bow tie zeer uitgebreid en ingewikkeld wordt. Het risico van een uitdijende bow tie wordt beperkt door de storingen te beperken tot zogenaamde 'hardware failures' en 'failure conditions'. In figuur 3 is de linkerkant van de bow tie uitgewerkt voor een stofbrand/explosie, die zowel binnen als buiten de installatie kan plaatsvinden. De CG is in dit voorbeeld niet nadere gespecificeerd. Om deze CG te laten plaatsvinden is de gelijktijdige combinatie van lucht (zuurstof), stof en een ontstekingsbron noodzakelijk en daarom zijn deze drie voorwaarden met een EN-poort verbonden met de CG. Als één van deze condities of voorwaarden ontbreekt, dan zal de CG niet plaatsvinden. De ontstekingsbron kan bestaan uit een vonk, veroorzaakt door een mechanische of elektrostatische ontlading, of door hete oppervlakten.

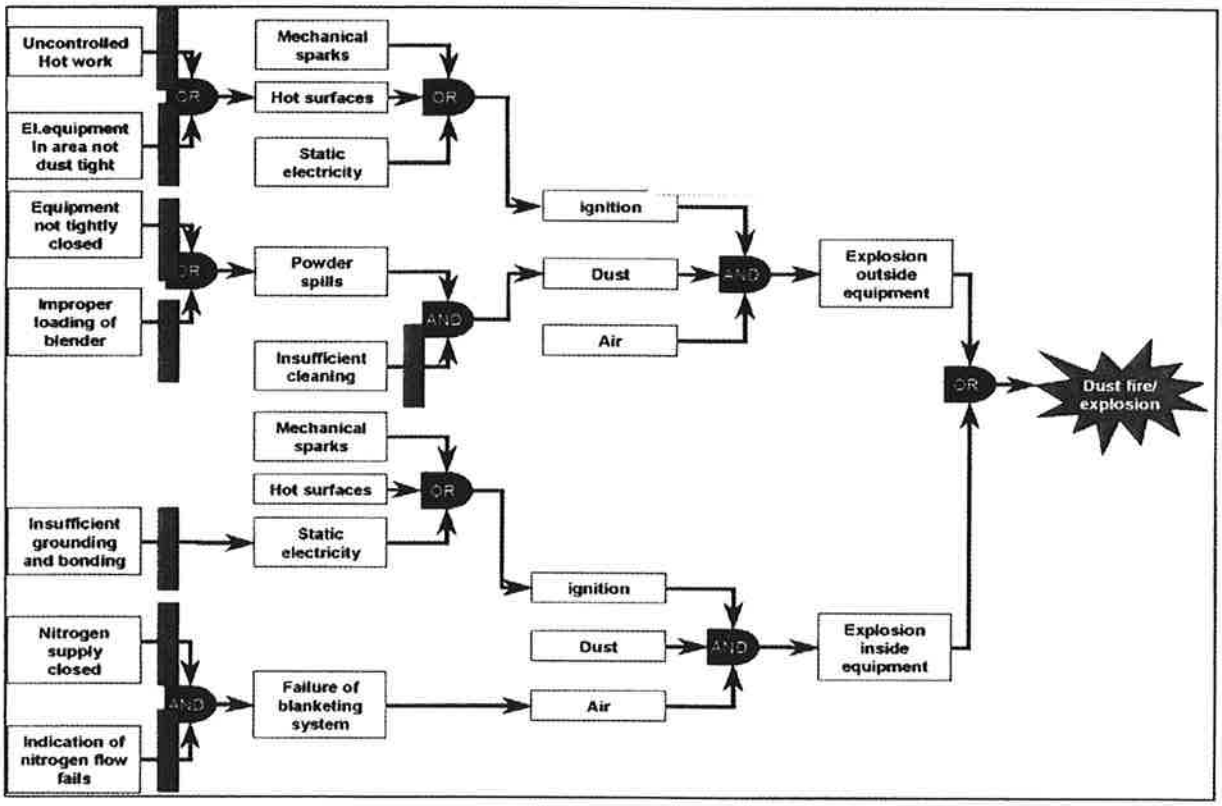
3. In deze stap worden de primaire barrières vastgesteld, die ervoor moeten zorgen dat scenario's gestopt worden. Primaire barrières zijn onder te verdelen in actieve of passieve barrières. Bij een passieve barrière beweegt er niets of komen werknemers niet in de buurt van de gevaarszones. De wanddikte van een reactorvat is een voorbeeld van een passieve barrière, evenals afgeschermde gevaarsgebieden en veiligheidszones. Bij actieve barrières nemen operators of de hardware actief maatregelen door in te grijpen in een gevaarlijke productielijn. Deze laatste type barrières zijn vaak software gestuurd en vereisen geen ingrijpen van een operator. Een automatische shut down is een voorbeeld van een actieve hardware barrière.

4. Tijdens de vierde stap worden de primaire barrières geaudit. De te auditen installatie wordt daarbij onderverdeeld in verschillende segmenten en ieder segment wordt door een klein groepje van 2-3 personen ter plaatse onderzocht. Deze groepjes bestaan uit één lid van het auditteam en één of twee medewerkers van het betreffende bedrijf. De resultaten van deze stap worden in de bow tie verwerkt, waarbij de



Figuur 3 Bow tie stofexplosies, zonder barrières

barrières als balkjes in de scenario's van de bow tie verschijnen. In figuur 4 zijn de barrières voor de stofbrand/explosie aangegeven. De aanwezigheid van lucht (zuurstof) is één van de noodzakelijke condities voor de CG. Binnen de installatie is deze conditie te beheersen, door de installatie onder een stikstofatmosfeer te houden. Voor stofbranden/explosies buiten de installatie is voor deze conditie geen barrière aanwezig.



Figuur 4 Bow tie stofbrand/explosie, barrières

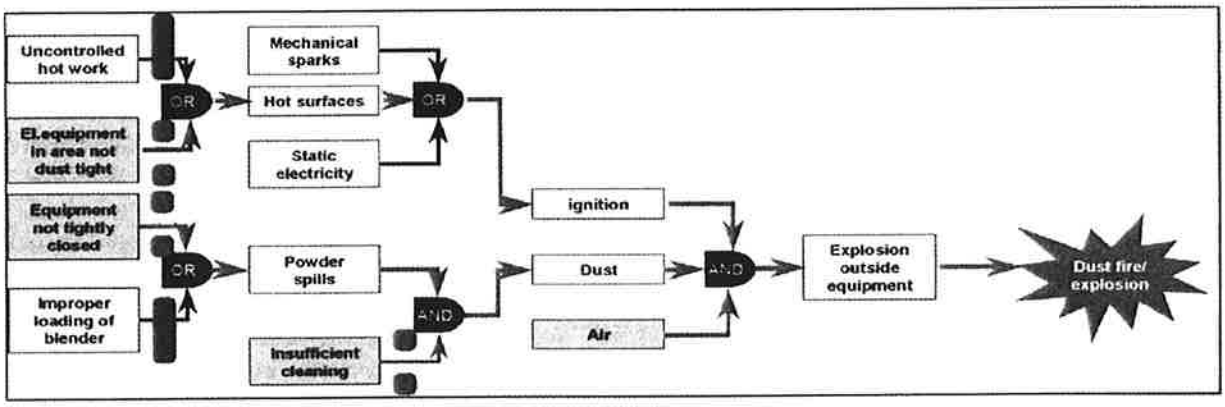
5. Als laatste stap wordt de kwaliteit van de barrières bepaald en de relatie gelegd met specifieke onderdelen van het management systeem. Daarvoor zijn de zogenaamde 'managementfactoren' van belang, evenals de informatie van procesverstoringen. Managementfactoren beïnvloeden de kwaliteit van de primaire barrières als volgt. Wanneer de primaire barrières via geëigende methoden zijn geïdentificeerd en gedefinieerd, dan dient het management vervolgens ervoor te zorgen dat het ontwerpproces en de installatie van de barrières optimaal wordt uitgevoerd. Er dienen procedures opgesteld te worden voor de barrières en de beschikbaarheid van voldoende en competente werknemers moet gegarandeerd zijn zodat de procedures onder alle omstandigheden uitgevoerd kunnen worden. Dit laatste stelt eisen aan de training en de opleiding van werknemers die de activiteiten uitvoeren. Als de barrières zijn geplaatst, dan is de inspectie en het onderhoud van de barrières noodzakelijk, evenals de betrokkenheid van werknemers om de relevante procedures te volgen. Wanneer meerdere werknemers betrokken zijn bij werkzaamheden, dan speelt communicatie een belangrijke rol als ook regels bij conflicten tussen veiligheid en andere bedrijfsdoelen, zoals productiedruk en levertijd. Als laatste is de registratie van storingen en ongevallen een onderdeel van het veiligheidsmanagementsysteem, met als doel om te leren van deze gebeurtenissen en om primaire barrières zonodig bij te stellen (Hale en Guldenmund, 2003; Hale ea., 2004; Guldenmund ea., 2005). Een aantal van deze managementfactoren zijn terug te vinden in tabel 1 onder het kopje 'organisatie'. Samengevat bestaan de managementfactoren uit:

- ontwerp en installatie van barrières
- procedures;
- beschikbaarheid van competente werknemers;
- inspectie en onderhoud;
- competentie (geschiktheid en training)
- betrokkenheid van werknemers, inclusief regels voor conflicten tussen veiligheid en andere bedrijfsdoelen;
- communicatie;
- registratie van storingen en ongevallen.

In figuur 5 zijn de resultaten van deze stap weergegeven. De informatie van processtoringen is een belangrijke indicator voor het functioneren van de primaire barrière en dit vormt de start voor een nader onderzoek naar relevante managementfactoren. In het voorbeeld zijn de barrières voor het scenario van een stofbrand/explosie binnen de installatie effectief gebleken. Er zijn geen storingen bekend van een geblokkeerde stikstof toevoer of van een falende indicator van deze toevoer. Het bedrijf heeft deze onderdelen van het proces, samen met de inspectie van de aarding van installatieonderdelen, opgenomen in een inspectie- en onderhoudprogramma, dat regelmatig wordt uitgevoerd. Een stofbrand/explosie buiten de installatie blijft in dit voorbeeld echter een waarschijnlijk scenario, omdat aan de drie eerder genoemde voorwaarden voor een CG wordt voldaan. In de figuur zijn de falende barrières met een geopend balkje weergegeven. Het betreft onder andere de elektrische apparatuur van de installatie, die niet stofdicht is, er is dus een ontstekingsbron. Verder zijn stoflekken geconstateerd bij de poederverwerkende onderdelen van de installatie waardoor stof zich in de loop van de tijd kan ophopen tot kritische concentraties. Naast de geconstateerde stoflekken is stof bij de betreffende installatie een algemeen probleem wegens een gebrekkig schoonmaak regime. Daar de gehele installatie in de open lucht staat is ook aan de laatste conditie van het scenario voldaan.

De problemen met de elektrische apparatuur en de poederverwerkende onderdelen van de installatie in het voorbeeld zijn duidelijk ontwerpgerelateerd. Bij de drie genoemde condities speelt de inspectie en het onderhoud een duidelijke rol en voor het schoonmaakregime eveneens de procedure, de training en de beschikbaarheid en betrokkenheid van werknemers. In dit voorbeeld zijn de managementfactoren niet nader uitgewerkt, omdat de informatie te bedrijfsspecifiek zou worden.

De scenario audit, die als voorbeeld heeft gediend, is binnen een tijdsbestek van anderhalve dag afgerond. De eerste drie stappen hebben een halve dag gekost en de laatste twee stappen één dag. De constructie van de bow tie is, door de grafische aard van de presentatie, een eye opener voor de deelnemers van de locatie en de techniek is eenvoudig uit te leggen. Verschillende vestigingen hebben om de toepassing van deze techniek gevraagd, zodat op korte termijn veel ervaring wordt opgedaan. Een logische toekomstige ontwikkeling is de constructie van generieke scenario's voor verschillende type installaties, waardoor de aandacht in de eerste drie stappen



Figuur 5 Bow toe stofbrand/explosie, kwaliteit van barrièreses

gericht kan worden op locale afwijkingen van deze scenario's en de stappen sneller doorlopen kunnen worden.

Discussie en conclusie

Dit artikel is gestart met de vraag naar de tekortkomingen van bestaande procesveiligheidsaudits. De audittechnieken zijn in de bespreking beperkt tot de PSM audit, waar internationaal opererende bedrijven met Amerikaanse vestigingen aan moeten voldoen. De vraag is terecht. De audit technieken zijn tijdrovend en ondanks alle inspanningen blijven (bijna) incidenten en (bijna) rampen zich voordoen. De belangrijkste omissie van de bestaande audit technieken zijn de gebrekkige gevaarherkenning, gerelateerd aan storingen van het proces, en de losstaande beoordeling van de elementen van het audit programma. Incidenten en rampen hebben doorgaans meerdere oorzaken, die tegelijk of na elkaar tot verlies van beheersing kunnen leiden. Deze oorzaken liggen zowel op het domein van het ontwerp van de installaties, als in de organisatie en in het menselijk handelen. De resultaten van de 4 experts over een aantal rampen en incidenten hebben dit nogmaals bevestigd. Andere technieken, zoals taak-risico analyses, risico inventarisaties en evaluaties en analyses van ongevallen hebben op zichzelf waarde, maar zijn voor een adequate gevaarherkenning niet altijd effectief. Taak-risico analyses kunnen te sterk gericht zijn op taakgerichte gevaren van individuele werknemers en risico inventarisatie en evaluaties blijven vaak steken in een opsomming van mogelijke gevaren, zonder een relatie met processtoringen te leggen. Dit geldt ook voor ongevalsanalyses, die doorgaans alleen een ongevalsmaat als output kennen.
Om aan deze omissies tegemoet te komen is de scenario audit ontwikkeld en aan de hand van een voorbeeld nader uitgelegd. Deze audit techniek maakt gebruik van het bow tie model, een model dat reeds bekend is binnen het vakgebied, maar nog nauwelijks voor audit doeleinden is toegepast. Het voordeel van dit model is sterke aandacht voor de gevaarherkenning in de vorm van de directe fysische oorzaken van scenario's, de primaire barrières en de managementfactoren. Hierdoor is een integrale beoordeling van de oorzaken mogelijk. Het menselijk handelen is onderdeel van deze managementfactoren.

Voor een adequaat veiligheidsbeleid, dat door een veiligheidmanagementsysteem wordt gewaarborgd, is de kennis van alle mogelijke ongevals-, incident- en rampscenario's een eerste vereiste. Het veiligheidsbeleid is erop gericht te voorkomen dat scenario's zich kunnen ontwikkelen tot centrale gebeurtenissen en vervolgens tot schade. De scenario audit lijkt een veelbelovende techniek te zijn om dit inzicht te verkrijgen. Uit deze scenario's volgen de barrières die verhinderen dat scenario's zich kunnen ontwikkelen. De directe oorzaak van ongevallen, incidenten en rampen is per definitie één of meerdere falende primaire barrières, of de afwezigheid van barrière(s). Deze directe oorzaken hebben hun oorsprong in de organisatie en in de kwaliteit van het veiligheidsmanagement en kunnen worden teruggebracht tot de hierboven genoemde falende managementfactoren. Deze barrières, zowel de primaire barrières als de managementfactoren, zijn het centrum van een managementsysteem, daar het managen van barrières de sleutel is voor een adequate beheersing van de veiligheid.

Literatuur

Ale B. (2003). Ons overkomt dat niet. Inaugurele rede. Technische Universiteit Delft

Bari R. (2000). Are risk measures suitably defined to manage risks that could lead to a large public impact? In Kondo S. & Furuta K. PSAM5: Probabilistic Safety Assessment & Management. Tokyo, Universal Academy Press. 2617-2622

Blom B. Swuste P. (2002). Hoe onvermijdelijk zijn ongevallen tijdens de productie van chocolade zoetwaren? Een vergelijking tussen een Nederlands en een Russisch bedrijf. Tijdschrift voor toegepaste Arbowetenschap 15 (4) 55-61

Carroll J. Rudolph J. Hatakenaka S. (2002). The difficult hand-over from incident investigation to implementation: a challenge for organisational learning. In: Wilpert B. Fahlbruch B. (eds) System Safety, challenges and pitfalls of interventions. New Technology and Work (NetWork), Bad Homburg. Pergamon, Oxford.

Center for Chemical Process Safety (1994), Guideline for Preventing Human Error in Process Safety

Collins R. (2004). Applying process safety management principles to manage indoor environmental quality. The Synergist October:40-41

EPA (2004). Risk Management Program Requirements Under Clean Air Act Section 112(r)(7); Amendments to the Submission Schedule and Data Requirements; Final Rule. 69FR18819

European Commission (2002). Report on the application in the Member States of Directive 82/501/EEC of 24 June 1982 on the major-accident hazards of certain industrial activities for the period 1997-1999 (2002/C 28/01)
Goossens L. (2003). What is a BARRIER? Safety Science Group, Delft University of Technology

Guldenmund F. Hale A. Goossens L. Betten J. Duijm N. (2005). The development of an audit technique to assess the quality of safety barrier management. Journal of Hazardous Materials (submitted)

Hale A. Baram M. Hovden J. (1998). Perspective on safety management and change. In: Hale A. Baram M. (eds). Safety management, the challenge of change. New Technology and Work (NetWork), Bad Homburg. Pergamon, Oxford

Hale A. Wilpert B Freitag M. (eds), (1997). After the event. From accident to organisational learning. New Technology

and Work (NetWork), Bad Homburg Pergamon, London

Hale A. (2002). Conditions of occurence of major and minor accidents. Tijdschrift voor toegepaste Arbowetenschap 15 (3) 34-41

Hale A. Guldenmund F. (2003). Barriers and delivery systems. Technische Universiteit Delft

Hale A. Goossens L. Ale B. Bellamy L. Post J. Oh J. Papazoglou I. (2004). Managing safety barriers and controls at the workplace. In: Spitzer, C. Schocker, U. Dang, V. (eds) Probabilistic Safety Assessment and Management. Berlin, Springer, 2004;608-613

Heinrich H. (1931). Industrial Accident Prevention. McGraw-Hill, New York

Hopkins A. (2000). Lessons from Longford. CCH Australia Limited

Kletz T. (1999). What went Wrong. Case histories of process plant disasters. Huston, Gulf (4th edition)

Kjellen U. (2000). Prevention of accidents through experience feedback. Taylor and Francis, London.

Koornneef F. (2000). Learning from small scale incidents. Proefschrift. Sectie Veiligheidskunde, Technische Universiteit Delft

Perrow C. (1999). Normal accidents. Living with high-risk technologies. 2e druk. Princeton University Press, Princeton.

Oh J. (2002). The EU Seveso II Directive: an example of a regulation that could act as an initiator to raise the major hazard safety awareness within society. In: Kirwan B. Hale A. Hopkins A. (eds). Changing regulations, controlling risks in society. New Technology and Work (NetWork), Bad Homburg. Pergamon, Oxford

OSHA Standard (1992). Process Safety Management of Highly Hazardous Chemicals. Standard 1910.119

Petrolekas P. Haritopoulos A. (2001). A risk management approach for Seveso II sites. Microrisk Internet Conference. ABS Group, Shell Gass, Greece

Rasmussen J. (1993). Learning from the past? How? Some research issues in industrial risk management. In: Wilpert B.

Qvale T. (eds) (1993). Reliability and safety in hazardous work systems. Approaches to analysis and design. New Technology and Work (NetWork), Bad Homburg Lawrence Erlbaum Associates Ltd, Publishers, Hove.

Reason J. (1997). Managing the risks of organisational accidents. Aldershot. Ashgate.

Rees J. (1994). Hostage of each other: the transformation of nucleair safety since Three Miles Island. Chicago, University of Chicago Press.

Salminen S. Saari J. Saarela K.L. & Räsänen T. (1992). Fatal and non-fatal occupational accidents: identical versus differential causation. Safety Science 15 (2) 109-118.
Saloniemi A. & Oksanen H. (1998). Accidents and fatal accidents: some paradoxes. Safety Science 29 (1) 59-66.

Swuste P. Guldenmund F. Hale A. (2002). Organisatiecultuur en veiligheid in een zware industrie, resultaten van onderzoek. Tijdschrift van toegepaste Arbowetenschap 15 (1) 7-14

U.S. Chemical Safety and Hazard Investigation Board (2002). Hazard Investigation, Improving reactive hazard management, Report No. 2001-01-H 2002.

Visser K. (1998). Developments in HSE management in oil and gas exploration and production. In: Hale A. Baram M. (eds). Safety management, the challenge of change. New Technology and Work (NetWork), Bad Homburg. Pergamon, Oxford

Weick K. Sutcliffe K. Obstfeld (1999). Organising for high reliability: process of collective mindfulness. Research in Organisational Behaviour 21, 81-123.

Zuijderduijn C. (1999). Risk Management by SHELL refinery, chemicals at Pernis, The Netherlands. European Conference on Risk management in the EU of 2000. The challenge of implementing Council Directive Seveso II. G. Papadakis (ed), Athens, 10-12 November. EU Report EN European Commission DG JRC MAHB, Ispra, Italy