



Delft University of Technology

Document Version

Final published version

Citation (APA)

Yarveisy, R., van Nunen, K. L. L., & Bouchaut, B. F. H. J. (2025). *Safy-by-Design: Een innovatieve aanpak voor omgevingsveiligheid*. Ministerie van Infrastructuur en Waterstaat.
<https://www.rijksoverheid.nl/documenten/rapporten/2025/06/30/safe-by-design-een-innovatieve-aanpak-voor-omgevingsveiligheid>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

In case the licence states "Dutch Copyright Act (Article 25fa)", this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.



Delft University of Technology

Document Version

Final published version

Citation (APA)

Yarveisy, R., van Nunen, K. L. L., & Bouchaut, B. F. H. J. (2025). *Safy-by-Design: Een innovatieve aanpak voor omgevingsveiligheid*. Ministerie van Infrastructuur en Waterstaat.
<https://www.rijksoverheid.nl/documenten/rapporten/2025/06/30/safe-by-design-een-innovatieve-aanpak-voor-omgevingsveiligheid>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

In case the licence states "Dutch Copyright Act (Article 25fa)", this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.



Safe-by-Design

Een innovatieve aanpak voor omgevingsveiligheid

Auteurs: Rioshar Yarveisy, Karolien van Nunen, Britte Bouchaut
Datum: Mei 2025

Safe-by-Design

Een innovatieve aanpak voor omgevingsveiligheid

Opdrachtgever en contactpersoon

Ministerie van Infrastructuur en Waterstaat (IenW)

Dhr. Victor van de Pas

victor.vande.pas@minienw.nl

Looptijd onderzoek

September 2024 - mei 2025

Datum rapport

Juni 2025

Auteurs

Dr. Rioshar Yarveisy

Dr. Karolien van Nunen - K.L.L.vanNunen@tudelft.nl

Dr.ir. Britte Bouchaut - B.F.H.J.Bouchaut@tudelft.nl

Veiligheidskunde

Techniek, Bestuur en Management

Technische Universiteit Delft

Jaffalaan 5

2628BX Delft

Samenvatting

Dit rapport richt zich op de implementatie van het Safe-by-Design (SbD)-principe binnen de context van omgevingsveiligheid in de chemische industrie. SbD is een opkomende methode voor risicomanagement dat veiligheid vanaf de ontwerpfase integreert in technologische en industriële systemen door ook naar onzekerheden te kijken. We spreken van onzekerheden in veiligheidsmanagement als de aard, de kans, de omvang of het effect van risico's niet volledig bekend of voorspelbaar is. Door het toepassen van SbD, en dus onzekerheden mee te nemen in ontwerpen en procesbeheer, pogen we onzekerheden terug te brengen naar een beheersbaar risico. Deze methode is bijzonder waardevol in een tijd waarin complexe systemen, zoals waterstof-infrastructuur, een cruciale rol spelen in de energietransitie.

Het rapport benadrukt dat traditionele methoden voor risicomanagement, zoals methoden die zich vooral op kwantificeerbare, 'harde cijfers' focussen, sterk afhankelijk zijn van beschikbare historische data. Echter, van nieuwe technologieën en industriële processen hebben we vaak niet dergelijke data voorhanden, en dus schieten deze methoden tekort bij het omgaan met onzekerheden en nieuwe risico's. Daarnaast richten huidige methoden voor veiligheidsmanagement in de chemische industrie zich voornamelijk op het verlagen van risico's, bijvoorbeeld door het toepassen van de inherente veiligheidsprincipes (ISPs), en zijn dus vooral toegespitst op de 'risicobehandeling'-fase in risicomanagement. In dit rapport kijken we breder naar de volledige risicomanagementcyclus, en worden mogelijke onzekerheden in elke fase van de cyclus bekeken. SbD biedt richtlijnen om veiligheid een integraal onderdeel van het gehele risicomanagementproces te maken.

Achtergrond en doel

Onzekerheden vormen een grote uitdaging in elk stadium van risicomanagement. Tijdens de contextbepaling kan het ontbreken van historische data leiden tot onvolledige risico-identificatie en verkeerde systeemgrenzen. In de analysefase kan de ernst van risico's worden onderschat, door modellen met lage betrouwbaarheid of door een gebrek aan deskundige kennis. Ook in de evaluatie- en behandelingsfase spelen onzekerheden een rol, vooral wanneer criteria voor risico-acceptatie vaag zijn of wanneer besluitvorming wordt beïnvloed door menselijke (vaak onbewuste) vooroordelen. Het rapport stelt dat deze tekortkomingen beter kunnen worden aangepakt door SbD-principes zoals het voorzorgsprincipe en systeemdenken te integreren in risicomanagement. Door te plannen voor *worst-case* scenario's en risico's met onzekerheden proactief te benaderen, kunnen organisaties niet alleen voldoen aan wettelijke eisen, maar deze ook overstijgen (*beyond compliance*) om veerkrachtige systemen te ontwikkelen.

Safe-by-Design als mentaliteit: van afvinken naar anticiperen

SbD vraagt om meer dan het volgen van stappenplannen of beslisbomen. In een technologische en maatschappelijke context die steeds complexer en onzekerder wordt volstaat het niet om veiligheid 'af te vinken'. SbD vergt een fundamentele mentaliteitsverandering: weg van compliance als einddoel, en richting veiligheid als een voortdurend proces van anticiperen, kritisch nadenken, afstemmen en iteratie.

Verschillende SbD-principes kunnen ingeschakeld worden om onzekerheden te adresseren in elke stap van de risicomanagement cyclus. Het voorzorgsprincipe helpt bij het omgaan met onzekerheden door uit te gaan van worst-case scenario's (waarbij de nadruk ligt op de *gevolgen* in plaats van op de (onzekere) kans) en extra veiligheidsmarges waar kennis nog beperkt is. Systeemdenken binnen SbD betekent verder kijken dan de grenzen van de eigen installatie en anticiperen op kettingreacties en wisselwerkingen binnen het grotere systeem. Ook neemt systeemdenken de complexiteit van moderne sociaal-technische systemen in beschouwing, met aandacht voor de interactie tussen technische factoren, mensen en de omgeving.

SbD houdt een integrale aanpak in waarbij bredere maatschappelijke en langetermijn risico's worden meegenomen. Het expliciet meenemen van deze risico's draagt bij aan een meer realistische inschatting van risico's in een context van onzekerheid en complexiteit. Dit vereist ook een levenscyclusbenadering waarin veiligheid verankerd is van ontwerp en constructie tot onderhoud en ontmanteling. Stakeholderparticipatie speelt hierin een centrale rol: door maatschappelijke zorgen en lokale kennis vanaf het begin te integreren, ontstaan zowel beter draagvlak als scherpere risicobeoordelingen. Ook samenwerking is essentieel om verschillende invalshoeken mee te nemen, en objectiviteit te vergroten door meerdere experts onafhankelijk een oordeel te laten vellen. Overheden kunnen deze samenwerking actief ondersteunen: enerzijds door het verspreiden van kennis over de beste beschikbare technologieën voor onder meer inspectie en monitoring, anderzijds door het stimuleren van kennisdeling binnen de sector.

Een iteratieve en dynamische aanpak is cruciaal binnen SbD, waarbij nieuwe informatie voortdurend wordt teruggekoppeld om zo risico's continu te actualiseren. Door actuele inspectiedata te vergelijken met ontwerpmodellen kunnen aannames worden getoetst en waar nodig worden bijgesteld, om zo onzekerheidsmarges te verkleinen.

Door SbD-principes in elke stap van de risicomanagementcyclus toe te passen worden onzekerheden teruggebracht tot beheersbare risico's. Dit leidt niet alleen tot minder incidenten, maar ook tot hogere betrouwbaarheid en beschikbaarheid van installaties en versterkt maatschappelijk vertrouwen. SbD verschuift de focus van 'veilig genoeg volgens de norm' naar 'veilig omdat het duurzaam en verantwoord is'.

Overheden spelen een cruciale rol in het toewerken naar de SbD-mentaliteit. Zij dienen beleidskaders te ontwikkelen die innovatie bevorderen, zorgen voor naleving van veiligheidsnormen, en aansporen tot anticiperen van nieuwe risico's met bijhorende onzekerheden.

Inhoudsopgave

Samenvatting	i
1 Inleiding	4
2 Omgaan met onzekerheden in risicomanagement	7
2.1 Contextbepaling	9
2.2 Risico-identificatie	11
2.3 Risicoanalyse	14
2.4 Risico-evaluatie	17
2.5 Risicobehandeling	19
2.6 Monitoring, evaluatie, communicatie en consultatie	22
3 Van ‘checklistdenken’ naar een Safe-by-Design mentaliteit	25
3.1 De valkuil van beslisbomen: waarom Safe-by-Design meer vraagt dan een keuzemenu	26
3.2 Casus: Waterstofpijpleidingen	27
4 Conclusie en aanbevelingen	32
Referenties	35

1 Inleiding

De grenzen van traditioneel risicomanagement bij opkomende risico's

De afgelopen jaren is binnen de chemische industrie een duidelijke verschuiving zichtbaar geworden van voorschrijvende veiligheidsregels naar meer prestatiegerichte richtlijnen. Hierbij ligt de verantwoordelijkheid om verder te gaan dan de minimale veiligheidsnormen bij de industrie zelf (lees: *beyond compliance*) (Wijnker & van der Velde, 2020). Deze verandering heeft geleid tot meer operationele efficiëntie en een groter concurrentievermogen binnen de chemische sector. Kwantitatieve risicobeoordelingen (*Quantitative Risk Assessments*, of QRA's) zijn daarbij de standaard geworden om een balans te vinden tussen veiligheid en winstgevendheid. Het vormt de basis voor prestatiegericht veiligheidsmanagement in sectoren waar risicovolle processen centraal staan. Bij deze vorm van risicobeoordeling wordt dus ingeschat hoe groot de kans is dat een risico zich voordoet en wat de mogelijke gevolgen zijn. Op basis van deze inschattingen kan worden vastgesteld of een risico acceptabel is, wat het 'kost', en kunnen passende maatregelen worden genomen in lijn met gangbare risicomanagementprincipes en methoden. Deze aanpak gaat ervan uit dat er voldoende kennis is over zowel de kans op optreden als de mogelijke impact (de zogeheten *known knowns*) (Aven & Renn, 2009).

Nieuwe technologieën of processen gaan echter vaak gepaard met nieuwe risico's, waar vaak weinig tot geen kennis of data beschikbaar voor is, wat zorgt voor (grote) onzekerheden. Sommige onzekerheden komen voort uit een gebrek aan kennis en ervaring over specifieke aspecten van een risico zoals onzekerheden over de kans (*probability*) of gevolg (*impact/effect*) (de zogeheten *known unknowns*), terwijl er in andere gevallen sprake kan zijn van volledige onwetendheid (*unknown unknowns*). Dit leidt tot de vraag of 'traditionele' risicomanagementmethoden, zoals QRA's, de veiligheid wel voldoende kunnen waarborgen in geval van nieuwe risico's die gepaard gaan met onzekerheden.

Daarnaast is het uitgangspunt van een QRA in de context van een incident vooral gericht op het aantal acute doden binnen een bepaald tijdsinterval en houdt het geen rekening met bredere maatschappelijke gevolgen¹ zoals te ontruimen gebieden of letsel met en zonder ziekenhuisopname. Ook bredere impacts zoals schade aan het milieu of de economie, verstoring van toeleveringsketens, welzijn van de bevolking en de organisatorische gevolgen van een incident worden niet meegenomen in de huidige QRA-methode. Dit kan ertoe leiden dat de werkelijke impact van een risico wordt onderschat. Een risico kan op papier acceptabel lijken, terwijl de maatschappelijke gevolgen in de praktijk alsnog ernstig kunnen zijn en de maatschappij juist kunnen ontwrichten. Het opnemen van dergelijke bredere gevolgen in risicobeoordelingen kan bijdragen aan een meer integrale en realistische inschatting van risico's, wat kan leiden tot beter onderbouwde besluitvorming en effectievere veiligheidsmaatregelen.

¹ De gevolgen voor mens, dier en milieu worden wel benoemd in ontwerpstandaarden maar zijn geen parameter in de QRA.

De meerwaarde van Safe-by-Design benaderingen bij risicomanagement van opkomende risico's

Opkomende risico's, die niet enkel gepaard gaan met onzekerheden bij de risicobeoordeling maar ook met onzekerheden binnen het volledige risicomanagement proces, vragen bijgevolg om een aanvulling op traditionele methoden waarbij expliciet rekening wordt gehouden met onzekerheid. Safe-by-Design (SbD) kan hierin een waardevolle rol spelen.

In theorie kunnen opkomende risico's met onzekerheden door toepassing van SbD worden beheerst vanuit het voorzorgsprincipe (*precautionary principle*). De SbD-benadering biedt een raamwerk waarin risico's met onzekerheden proactief worden meegenomen door middel van iteratief leren en vooruitkijkende strategieën. Zo komt er nadruk te liggen op voorzorgsmaatregelen, leren wat onzekerheden inhouden, en het nemen van passende maatregelen om veiligheid te waarborgen. Vanuit dit principe geredeneerd dient er ruimte gecreëerd te worden voor het vergaren van kennis en gegevens over de factoren die aan deze onzekerheden bijdragen. Hierop kunnen onzekerheden geanticipeerd en gemitigeerd worden, en kan onzekerheid teruggebracht worden naar een beheersbaar risico.

In dit onderzoek kijken we naar in hoeverre SbD-principes complementair kunnen worden ingezet op de huidige (kwantitatieve) risicomanagement strategieën. Het opnemen van bredere (maatschappelijke) gevolgen in risicobeoordelingen speelt hierbij een belangrijke rol, om zo bij te dragen aan een meer realistische inschatting van risico's in een context van onzekerheid en complexiteit.

Een Safe-by-Design aanpak die verder gaat dan inherente veiligheid

SbD is een methode voor risicomanagement die zijn oorsprong met name vindt binnen de chemische technologie onder het begrip 'Inherente Veiligheid', of *Inherent Safety*. Inherente veiligheid in de chemische industrie wordt veelal nagestreefd door het toepassen van Inherente Veiligheidsprincipes (ISP's) zoals *matiging* (d.w.z. het toepassen van lagere druk of temperaturen bij chemische reacties), *vereenvoudiging* van chemische processen om zo het risico op fouten te reduceren, *substitutie* van schadelijke of toxische grondstoffen of chemicaliën door minder gevaarlijke/toxische varianten, of *minimalisatie* van bestaande chemische processen zoals het gebruik van kleinere reactorvaten (Amyotte et al., 2007).

Een integrale SbD-aanpak gaat echter verder dan inherente veiligheid en de toepassing van ISP's. De huidige aanpak van inherente veiligheid en ISP's richt zich voornamelijk op het verlagen van risico's, en is dus vooral toegespitst op de 'risicobehandeling'-fase in risicomanagement. In dit rapport kijken we breder naar de volledige risicomanagementcyclus, en worden mogelijke onzekerheden in elke fase van risicomanagement bekeken om zo tot een integrale SbD-aanpak te komen.

Bovendien gaat de toepassing van ISP's uit van beschikbaarheid aan kennis en bestaande ervaringen. Nieuwe technologieën of processen gaan echter vaak gepaard met nieuwe risico's, waar vaak weinig tot geen kennis of data beschikbaar voor is, wat zorgt voor (grote) onzekerheden, en een hogere mate van onvoorspelbaarheid.

Onderzoeksvraag en casus

Samenvattend beantwoordt dit onderzoek de volgende onderzoeksvraag:

Hoe kan Safe-by-Design worden toegepast om risicomanagement te verbeteren door conventionele risicogebaseerde veiligheidsmanagementsystemen zoals QRA beter in staat te stellen om met opkomende onzekere risico's om te gaan, en zo de externe veiligheid in risicovolle sectoren te verbeteren, met name in de context van nieuwe processen en de energietransitie?

In dit onderzoek wordt dus onderzocht in hoeverre SbD een aanvulling kan zijn op traditionele risicobenaderingen, met behulp van een casus over een hypothetische waterstof-pijpleiding in Nederland. Voor deze casus is ter illustratie een SbD-beslisboom ontwikkeld die een basis biedt voor het managen van veiligheid voor risico's met (hoge) onzekerheden. Deze beslisboom illustreert echter ook de tekortkomingen van een dergelijke aanpak. Hoewel de beslisboom SbD-richtlijnen volgt voor het vergaren van kwalitatieve data, en suggesties biedt voor het verantwoord omgaan met risico's met onzekerheden, laat deze casus ook zien dat SbD juist niet gepositioneerd moet worden als een 'vaste' set aan richtlijnen (lees: een checklist). Het terugbrengen van onzekerheden naar beheersbare risico's vraagt juist om een case-by-case benadering.

Er is gekozen voor een waterstof-pijpleiding vanwege het belang dat de waterstofinfrastructuur speelt in de Nederlandse energietransitie. Tegelijk brengen de ontwikkelingen rond nieuwe pijpleidingen nieuwe risico's met zich mee voor de omgevingsveiligheid. Dit komt onder meer door de eigenschappen van de getransporteerde stoffen (bijvoorbeeld ontvlambaarheid) en het gebruik van pijpleidingen met een grote diameter over lange afstanden. Daarbij gaat het om nieuwe risico's die sterk worden gekenmerkt door onzekerheden, door het ontbreken van historische gegevens, de ongekennde schaal van de volumes, en operationele parameters die aanzienlijk afwijken van wat de industrie gewend is. De casus illustreert hoe onzekerheden een rol spelen bij het omgaan met de risico's van pijpleidingen, hoe SbD-principes hierop kunnen inspelen en welke voorzorgsmaatregelen mogelijk (en nodig) zijn. Op basis van de resultaten worden conclusies getrokken en aanbevelingen gedaan over hoe SbD geïntegreerd kan worden in bestaande QRA's.

Deze studie is gebaseerd op deskresearch, bestaande uit peer-reviewed academische artikelen, grijze literatuur en andere online informatie verzameld in de periode september-november 2024.

Leeswijzer

Na deze introductie gaat hoofdstuk 2 verder in op de manier waarop onzekerheden van invloed kunnen zijn op de kwaliteit van risicomanagement, met extra aandacht voor situaties waarin SbD-principes deze aanpak kunnen versterken. Om de potentiële impact van deze onzekerheden te illustreren worden voorbeelden gegeven van industriële incidenten en rampen uit de chemische industrie en de olie- en gassector. De voorbeelden uit deze specifieke sectoren zijn relevant door het verband met de infrastructuur die een sleutelrol speelt in de energietransitie.

In hoofdstuk 3 wordt SbD aan de hand van een beslisboom toegepast op een deel van de risicomanagementcyclus, de 'contextbepaling', met behulp van een waterstof-pijpleiding casus. Hiermee wordt geïllustreerd hoe SbD-principes gebruikt kunnen worden om nieuwe risico's te identificeren, begrijpen en beheersen, maar ook hoe een 'vaste' set aan dergelijke principes juist begrenzend kan werken. Hoofdstuk 4 presenteert de conclusie van dit onderzoek, en geeft een aantal aanbevelingen voor het toewerken naar een SbD-mentaliteitsverandering.

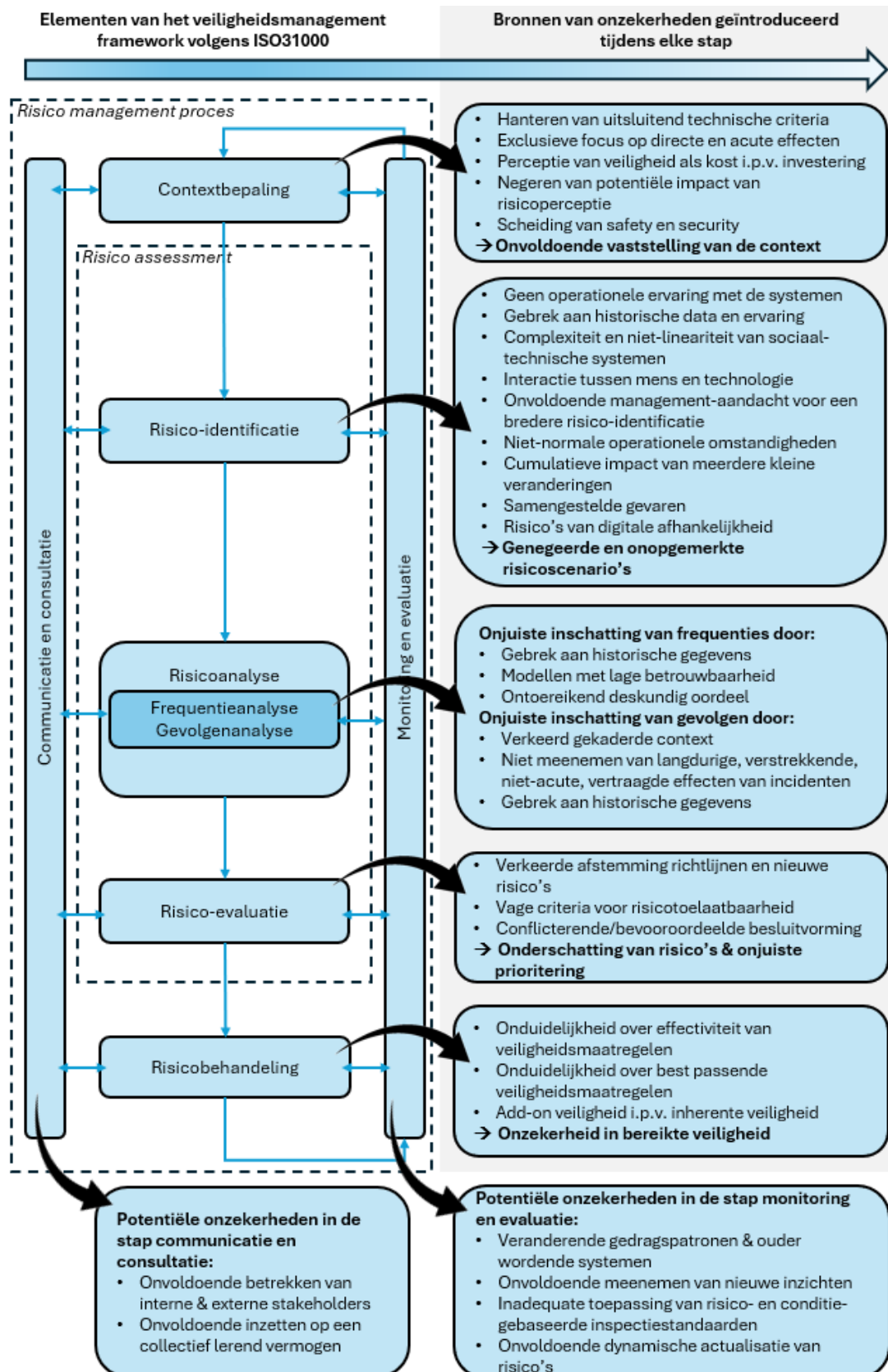
2 Omgaan met onzekerheden in risicomanagement

De energietransitie vraagt om een fundamentele herziening van hoe risico's in industriële systemen worden beheerst. De opkomst van nieuwe technologieën, veranderende processen en het toenemende belang van maatschappelijke betrokkenheid hebben geleid tot een complex risicolandschap dat niet langer adequaat kan worden beheerst met conventionele risicobeheersingsmethoden, zoals QRA.

Een op risico's gebaseerde beoordeling zoals QRA biedt een gestructureerde aanpak voor het identificeren, analyseren, evalueren en behandelen van risico's binnen een organisatie of systeem, en zorgt voor een systematische en efficiënte prioritering van veiligheid. Het risicomanagement proces dat in Figuur 1 is weergegeven is gebaseerd op de ISO 31000-norm (ISO, 2018), die over het algemeen wordt gebruikt voor risicomanagementpraktijken in de chemische industrie. Dit proces omvat zes kernfasen: 1) contextbepaling, 2) risico-identificatie, 3) risicoanalyse, 4) risico-evaluatie, 5) risicobehandeling en 6) monitoring, evaluatie, communicatie en consultatie. In elke fase kunnen onzekerheden optreden – zeker in het licht van nieuwe technologieën en infrastructuur voor de energietransitie. Deze onzekerheden maken het moeilijk om risico's volledig te doorgronden en effectief te beheersen met conventionele risicobeheersingsmethoden.

In dit hoofdstuk wordt uitgelegd hoe onzekerheden zich in elke van de zes stappen kunnen manifesteren, en hoe deze niet-aangepakte onzekerheden kunnen leiden tot ontoereikend risicomanagement. Per fase bespreken we de relevante uitdagingen en onzekerheden, en illustreren we hoe een SbD-benadering – met principes als inherente veiligheid, het voorzorgsprincipe en systeemdenken – kan helpen deze uitdagingen aan te pakken. Daarbij worden waar mogelijk relevante voorbeelden gegeven uit de industriële praktijk (zoals historische ongevallen) en worden aanbevelingen en richtlijnen gepresenteerd voor overheid, organisaties en technische experts om het risicomanagementproces te versterken.

Aangezien risicomanagement een continu en iteratief proces is, beïnvloeden de onzekerheden in elke stap ook de stappen ervoor en erna. De 'statische' presentatie van Figuur 1 is daarom een vereenvoudiging; het daadwerkelijke proces is dynamisch en onderling verbonden.



Figuur 1. Stappen in het veiligheidsmanagement framework en voorbeelden van onzekerheden die bij elke stap kunnen worden geïntroduceerd

2.1 Contextbepaling

De eerste stap in risicomanagement is het bepalen van de context, oftewel het vaststellen van de systeemgrenzen. Dit houdt in dat men duidelijk definieert *wie of wat* mogelijk schade kan ondervinden van potentiële incidenten en *hoe* die schade kan optreden. Met andere woorden: welke personen, omgevingen en waardevolle objecten vallen binnen het invloedsgebied van de activiteiten, en onder welke omstandigheden zouden zij geraakt kunnen worden? Een nauwkeurige contextbepaling is cruciaal voor het kunnen identificeren van realistische risicoscenario's. Immers, als de context verkeerd of te beperkt wordt gedefinieerd, ontstaat een onvolledig overzicht van risico's, kunnen belangrijke scenario's over het hoofd worden gezien, en ontstaat een vals gevoel van veiligheid.

In de praktijk blijkt dat onzekerheden bij de contextbepaling vaak leiden tot een te smalle blik. Traditionele veiligheidsbenaderingen in de industrie, zoals QRA, richten zich van oudsher vooral op directe technische gevaren binnen de installatie, terwijl bredere implicaties buiten de installatie minder aandacht krijgen. Historische rampen onderstrepen de gevolgen hiervan. De gaswolkontploffing in Bhopal (India) in 1984 (Broughton, 2005) toont bijvoorbeeld hoe een beperkte contextdefinitie de langetermijnpact op milieu en volksgezondheid onderschatte. Een ander voorbeeld is de instorting van een kolenmijn in Aberfan (VK) in 1966 (HM Stationary Office, 1966), waar men het bij het bepalen van de context naliet te beseffen dat een ogenschijnlijk lokale mijnbouwactiviteit een hele dorpsgemeenschap (inclusief een school) verderop in het dal in gevaar kon brengen. Dergelijke incidenten laten zien dat niet-acute, niet-onmiddellijke effecten en kwetsbaarheden zoals langdurige milieuschade of indirecte gevolgen voor omwonenden onopgemerkt kunnen blijven als de systeemgrenzen te nauw of beperkt getrokken worden.

Tevens maken deze voorbeelden duidelijk dat een exclusieve focus op *directe* en *acute* effecten achterhaald is in moderne risicobeheersing. Industriële ongevallen hebben vaak verstrekkende gevolgen die lang aanhouden. Bijvoorbeeld, naast de onmiddellijke dodelijke slachtoffers had de ramp in Bhopal decennialange milieugevolgen, en het vrijkomen van gevaarlijke chemicaliën na het Norfolk Southern-treinongeluk in 2023 (National Transportation Safety Board, 2023) in de VS laat zien hoe milieuschade en gezondheidszorgen langdurig kunnen doorwerken. Een te beperkte contextbepaling die voornamelijk op kortetermijnschade focust, miskent deze langdurige risico's.

Een ander belangrijk aspect van de contextbepaling is de wijze waarop veiligheid binnen organisaties wordt gezien. Als veiligheid primair wordt beschouwd als een kostenpost of verplichte bijkomstigheid, bestaat de neiging de context minimaal in te vullen – precies genoeg om aan de regels te voldoen (*compliance*), maar zonder bredere veiligheidsmarges in te bouwen (*beyond compliance*). Dit kan ertoe leiden dat organisaties bewust activiteiten blijven uitvoeren met risico's en onzekerheden die zij niet volledig beheersen, in de veronderstelling dat het 'goed zal gaan'. Korte-termijn financiële motieven gaan dan boven veiligheid op de lange termijn, met potentieel catastrofale gevolgen. Een voorbeeld hiervan is de Deepwater Horizon-ramp (Golf van Mexico, 2010). Het bedrijf BP nam grote risico's bij boren op extreme diepte waarvoor onvoldoende kennis en ervaring was. Hierbij vertrouwden ze op één technisch veiligheidssysteem (een blowout preventer) om een blowout te voorkomen. Toen dit systeem faalde, leidde het tot een olieramp die het bedrijf tegen 2018 naar schatting \$65 miljard kostte (US News, 2018), en leidde tot ongekende milieuschade en reputatieschade voor het bedrijf en de sector. De onderliggende oorzaak was een contextbepaling waarin financiële winst verkozen werd boven het integreren van veiligheid als primaire randvoorwaarde.

Daarnaast zijn in het afgelopen decennium diverse kwetsbaarheden in termen van *security* naar voren gekomen als een van de meest kritieke faalmechanismen van kritieke infrastructuur. Echter blijft beveiligingsbeheer (*security*) grotendeels gescheiden van veiligheidsbeheer (*safety*). Recente

gebeurtenissen (zoals de sabotage van de Nord Stream-gaspijpleiding in 2022 of de droneaanval op olieverwerkingsfaciliteiten in Abqaiq-Khuras in 2019) hebben aangetoond dat opzettelijke aanvallen, zowel fysiek als cyber, op kritieke infrastructuur verstreckende gevolgen kunnen hebben voor de maatschappij, toeleveringsketens en de gehele economie. Dit benadrukt de noodzaak om de klassieke focus te verleggen, en om ook security aspecten te integreren in veiligheidsbeheer.

Tot slot dient bij de contextbepaling niet alleen naar technische factoren gekeken te worden, maar ook naar maatschappelijke factoren zoals publieke risicoperceptie en politiek-bestuurlijke haalbaarheid. Grootschalige projecten in de context van de energietransitie kunnen bijvoorbeeld vastlopen door onvoldoende rekening te houden met de zorgen van omwonenden of het bredere publiek. Hoewel de publieke opinie niet direct van invloed is op de fysieke kans op een ongeval, bepaalt het wel de *maatschappelijke acceptatie* van risico's. In het kader van externe veiligheid en energietransitie, waar nieuwe infrastructuur (bijv. waterstof- of CO₂-pijpleidingen) door dichtbevolkte gebieden kunnen lopen, is het dus van belang de maatschappelijke context expliciet mee te nemen. Opvallende voorbeelden waarbij publieke tegenstand en politieke druk hebben geleid tot annuleringen van projecten waar al substantieel in was geïnvesteerd, zijn onder meer het DESERTEC-project voor hernieuwbare energie in woestijngebieden (Schmitt, 2018), de luchthaven Grand-Ouest in Frankrijk (Willsher, 2018) en de Keystone-pijpleiding (US) (Decherney & John, 2024). Mits vroegtijdig rekening was gehouden met maatschappelijke zorgen en bestuurlijke gevoeligheden, waren deze projecten wellicht niet geannuleerd.

Safe-by-Design in de contextbepalingfase

Een grondige en brede contextbepaling vormt de basis voor alle volgende stappen in risicomanagement. SbD benadrukt hierbij principes als *systeemdenken*, *stakeholderbetrokkenheid* en *maatschappelijke verantwoordelijkheid* om de relevante context zo volledig mogelijk te schetsen.

Systeemdenken houdt in dat men verder kijkt dan de grenzen van de eigen installatie en anticipeert op kettingreacties en wisselwerkingen binnen het grotere systeem. Zo wordt veiligheid een integrale systeemwaarde in plaats van een losstaande eis.

Het betrekken van stakeholders, bijvoorbeeld omwonenden, lokale overheden en hulpdiensten, in een vroeg stadium zorgt ervoor dat hun zorgen en lokale kennis worden gehoord, waardoor over het hoofd geziene kwetsbaarheden aan het licht kunnen komen. Dit sluit aan bij bestaande kaderwerken: het Verdrag van Aarhus² geeft omwonenden en belanghebbenden bijvoorbeeld het recht op inspraak en informatie in milieukwesties, wat bij industriële projecten cruciaal is om publieke zorgen te adresseren. Overheden spelen hierin een faciliterende rol. Zij kunnen sociale verantwoordelijkheid en een ethische benadering bevorderen door binnen wet- en regelgeving participatie te stimuleren. Europese richtlijnen (zoals de Seveso III-richtlijn³, in Nederland geïmplementeerd via het BRZO⁴) vereisen al vroege publieke participatie bij besluiten over risicovolle infrastructuur, met speciale aandacht voor projecten voor de energietransitie. Een SbD-benadering moedigt aan dat deze participatiemogelijkheden ten volle worden benut en drempels ervoor worden verlaagd.

Daarnaast vereist SbD een *mentaliteitsverandering* binnen organisaties: veiligheid moet vanuit intrinsieke motivatie worden gezien als een investering en kernwaarde, niet als (financiële) last. Dit betekent dat het management veiligheid vanaf de ontwerpfase actief integreert in besluitvorming.

² <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=LEGISSUM%3AI28056>

³ <https://eur-lex.europa.eu/eli/dir/2012/18/oj/eng>

⁴ <https://seveso-plus.nl/aanpak/brzo-2015/inleiding-brzo-2015/>

Bestuurders en directies dienen proactief te sturen richting een mentaliteit waarbij niet alleen wordt voldaan aan minimale normen, maar waarbij men streeft naar het overtreffen van die normen (*beyond compliance*). Overheidsbeleid kan dit stimuleren door beleidskaders en vergunningen zo in te richten dat ze ruimte bieden – of zelfs aansporen – om verder te gaan dan de minimumvereisten. Tegelijk moet men waken dat regelgeving niet te beperkt of te strikt is: huidig veiligheidsbeleid richt zich vaak vooral op acute risico's en is veelal gebaseerd op ervaringen uit het verleden. SbD probeert deze kloof te dichten door besluitvormers te helpen een breder scala aan zorgen in acht te nemen, inclusief lange termijn milieu- en maatschappij-effecten, zelfs als die (nog) niet expliciet in de regelgeving staan.

Samengevat vergt de contextfase een integraal perspectief. Door veiligheidsgrenzen breed te trekken, ook buiten de poorten van het bedrijf en installaties, en door veiligheid vanaf het begin, proactief, als integraal onderdeel te beschouwen, legt men een solide basis voor adequaat en gepast veiligheidsmanagement. Hierbij is het betrekken van relevante stakeholders, zoals omwonenden, cruciaal om lokale kennis en bezorgdheden mee te nemen. Een goede contextbepaling onder SbD maakt duidelijk welke mensen en waarden beschermd moeten worden en creëert de randvoorwaarden om in de volgende stap alle relevante risico's te herkennen. Door dit overzicht kunnen ook interacties tussen processen en stakeholders in kaart worden gebracht, waardoor wisselwerkingen die risico's zouden kunnen creëren, kunnen worden ondervangen.

2.2 Risico-identificatie

In de fase van risico-identificatie worden de *bronnen van gevaar* (hazards) geïdentificeerd, als startpunt voor het opstellen van risicoscenario's. Het doel is om alle potentieel gevaarlijke situaties, stoffen, processen en gebeurtenissen te benoemen die binnen de gedefinieerde context schade kunnen veroorzaken. Het lijkt vanzelfsprekend om alle bronnen van gevaar op te sporen, maar in de praktijk kunnen onzekerheden in deze stap ertoe leiden dat sommige gevaren worden gemist. Vooral bij nieuwe systemen, procescondities of ongebruikelijke omgevingsomstandigheden is dit een uitdaging: men heeft nog niet de operationele ervaring met de systemen om de risico's te kunnen doorgronden. In de energietransitie, waar bijvoorbeeld nieuwe infrastructuren voor waterstof-, ammoniak- of CO₂-transport worden ontwikkeld, ontbreekt vaak historische data en ervaring. Bestaande gevarencatalogi en checklists (veelal gestoeld op de conventionele chemie- of oliesector) dekken dan niet alle unieke gevaren van deze nieuwe systemen (Amendola, Contini & Ziomas, 1992; Cameron et al., 2017; Casal & Holsen, 2016). Onzekerheden in de stap *risico-identificatie* kunnen ertoe leiden dat bronnen van gevaar over het hoofd worden gezien en kunnen daardoor leiden tot een vals gevoel van veiligheid.

De conventionele methoden voor de identificatie van potentiële bronnen van risico's, zoals HAZID (Hazard Identification), HAZOP (Hazard and Operability Study), FMEA (Failure Modes and Effects Analysis) en 'What-if'-analyse, brengen mogelijk niet alle risicoscenario's van opkomende risico's in kaart. Deze conventionele methoden voor risico-identificatie gaan uit van lineaire causale relaties tussen stappen in een systeemontwerp (dus een oorzaak-gevolg relatie tussen stap a en stap b in een proces). Moderne sociaal-technische systemen zijn echter weinig lineair, en veel complexer door onder meer de interactie tussen mens en technologie. Er vinden verschillende interacties plaats tussen bijvoorbeeld technische factoren, operators en de omgeving, en deze worden beïnvloed door factoren zoals het organisatiebeleid, economische factoren en wetgeving. Bijdragend aan de complexiteit is ook dat bepaalde factoren, zoals management en menselijk handelen, inherent onzekerheden met zich meedragen. De conventionele methoden zijn niet in staat om rekening te houden met deze veelheid aan factoren en onderlinge interacties, wat zorgt voor onzekerheden bij de risico-identificatie.

Bijkomende factoren die onzekerheden introduceren in de stap van risico-identificatie zijn: onvoldoende aandacht vanuit het management voor een bredere risico-identificatie, niet-normale operationele omstandigheden, de cumulatieve impact van vele kleine veranderingen, samengestelde gevaren, en het risico van digitale afhankelijkheid.

Onvoldoende aandacht vanuit het management voor een bredere risico-identificatie kan er voor zorgen dat risico's te eenzijdig of onvolledig worden benaderd. Dit raakt aan het eerder besproken punt over de manier waarop veiligheid binnen organisaties wordt gezien. Als het management veiligheid te veel ziet als kostenpost of verplichte bijkomstigheid, dan maakt veiligheid vaak geen fundamenteel onderdeel uit van een duurzame bedrijfsvoering. Dit kan leiden tot bijvoorbeeld een gebrekkig kwaliteitsmanagement van de materialen die gebruikt worden bij de constructie van een nieuwe fabriek of pijpleiding, waardoor de corrosiesnelheid wordt onderschat. Volgens een analyse van 100 grote incidenten in de onshore olie- en gassector (MARSH, 2018) en de analyse hiervan (Jarvis & Goddard, 2017), speelt (mis)management een belangrijk aspect in vrijwel alle incidenten. Het management kan een cruciale rol spelen in het stimuleren om buiten de conventionele methoden te kijken om risico's te identificeren. Zeer belangrijk is om ook de werknemers nauw te betrekken bij het identificeren van risico's, aangezien zij vaak als eersten signalen opvangen van potentiële gevaren in de praktijk en waardevolle inzichten hebben die niet altijd zichtbaar zijn in formele processen of rapportages.

De eerder genoemde interactie tussen mens en technologie brengt een breed scala aan potentiële risicoscenario's met zich mee. Dit geldt in het bijzonder tijdens 'niet-normale' of afwijkende bedrijfsomstandigheden, waarbij mens-technologie interactie onvoorspelbaar is en risico's introduceert in het systeem. Van de 100 grote incidenten geanalyseerd door Jarvis & Goddard (2017), vonden er 63 plaats tijdens niet-normale operaties. Onder niet-normale operaties vallen onderhoudswerkzaamheden, niet-routinematige of zeldzame activiteiten, ongeplande taken of operaties onder niet-standaard omstandigheden, zoals extreem weer.

Ook kan de cumulatieve impact van meerdere ogenschijnlijk kleine veranderingen gezamenlijk leiden tot een aanzienlijke verschuiving in het totale risicoprofiel van een systeem (Leveson, 2016). Verder kunnen samengestelde gevaren (meerdere gevaren die zich gelijktijdig voordoen) systemen op onverwachte manieren ontwrichten zoals bij de Fukushima Kernramp in 2011, waarbij een onverwachte aardbeving en tsunami gelijktijdig plaatsvonden (Tokyo Metropolis, 2012). Binnen de energie-infrastructuur, zoals bij pijpleidingen en vaten onder hoge druk, kunnen gelijktijdige degradatiemechanismen (zoals corrosie, scheurvorming en vermoeiing) leiden tot onverwachte integriteitsproblemen. Dit geldt vooral wanneer deze mechanismen onvoldoende begrepen worden in de context van nieuwe chemicaliën, zoals waterstofbroosheid (API, 2021).

Als laatste kan de integratie van digitale technologieën zoals AI, machine learning en computationele modellen ons begrip van de werkelijke toestand van een systeem vertekenen. Afhankelijkheid van systemen die moeilijk te interpreteren zijn, bijvoorbeeld door ondoorzichtige besluitvormingsprocessen van de modellen of een gebrek aan transparantie over hoe en in welke context de modellen zijn getraind, kan leiden tot onverwachte gevaren en niet-geïdentificeerde risico's (National Commission, 2011).

Een bijkomende valkuil is dat veiligheidsprofessionals in organisaties doorgaans opereren binnen de kaders van het geldende bedrijfsbeleid en de regelgeving. Hun primaire taak is vaak het voldoen aan wet- en regelgeving en aan vergunningseisen. Hierdoor ligt de focus op gevaren die expliciet genoemd worden in voorschriften of die bekend zijn uit de eigen industrie. Potentiële gevaren die buiten dit bekende kader vallen, bijvoorbeeld vanwege nieuwe of onvoorziene omstandigheden of combinaties

van factoren, kunnen onopgemerkt blijven. Het introduceren van nieuwe blikvelden is daarom van belang.

Safe-by-Design in de risico-identificatiefase

SbD-principes stimuleren het vergroten van die blikvelden. Zo benadrukt SbD de betrokkenheid van diverse stakeholders, met name ook al in de risico-identificatiefase. Door gericht te *luisteren naar zorgen van werknemers, omwonenden en andere belanghebbenden*, kunnen organisaties gevaren opvangen die anders moeilijk te identificeren zijn. Medewerkers op de werkvloer hebben bijvoorbeeld praktijkkennis en kunnen vroegtijdig wijzen op *near-misses* of onveilige situaties. Een open meldcultuur (ondersteund door het management) is hierbij essentieel, zodat werknemers zich vrij voelen om risico's te melden en actief mee te denken over verbeteringen. Dit kan onder andere inhouden dat het management regelmatig veiligheidsoverleg houdt met de medewerkers, en duidelijk communiceert dat veiligheid prioriteit heeft.

Een ander SbD-principe toepasbaar in deze fase is het *voorzorgsprincipe*. In plaats van te redeneren "als er geen bewijs van gevaar is, nemen we aan dat het veilig is", draait men dit om: in situaties van onzekerheid neemt men aan dat er *wel* een ernstig gevaar zou kunnen zijn en worden scenario's daarop afgestemd en verder onderzocht. Concreet betekent dit dat men niet enkel naar meest waarschijnlijke scenario's kijkt, maar ook naar extremere, zij het minder waarschijnlijke, scenario's (*worst-case scenarios*). Het hanteren van een Maximaal Geloofwaardig Ongevalsscenario (Maximum Credible Accident Analysis - MCAA) als analysekader kan daarbij helpen. Het is aan te bevelen dat bedrijven bij nieuwe systemen (waar weinig ervaringscijfers voorhanden zijn) een MCAA uitvoeren. In een MCAA ligt de nadruk op de *gevolgen* in plaats van op de (onzekere) kans, zodat men een robuust beeld krijgt van de potentiële schade als het misgaat. Dit voorzorgsinstrument zorgt ervoor dat zelfs bij gebrek aan betrouwbare faalkansdata de ernstigste denkbare gebeurtenissen toch kunnen worden geïdentificeerd en beoordeeld.

Hoewel deze aanpak door bedrijven als conservatiever kan worden opgevat en in eerste instantie misschien kostenverhogend lijkt, kan het juist rampen voorkomen die de organisatie op financieel en reputatievlak zwaar zouden kunnen schaden. Dergelijke lange termijnvisie sluit aan bij maatschappelijke verantwoordelijkheid, en dus een SbD-mentaliteit: investeren in preventie voorkomt dat men later wordt geconfronteerd met schade die niet meer beheersbaar is.

Naast worst-case scenario's dient men bij risico-identificatie onder SbD oog te hebben voor *samengestelde gevaren*, waarbij, met name in complexe systemen, meerdere gevaren zich gelijktijdig kunnen voordoen en een versterkend effect kunnen hebben op elkaar. Denk aan de combinatie van corrosie, materiaalvermoeding en trillingen, die gezamenlijk tot scheurvorming kunnen leiden. Een traditioneel risico-onderzoek zou deze factoren wellicht los van elkaar bekijken, maar SbD spoort experts aan om dit soort interacties expliciet te identificeren en mee te nemen. Zo krijgt men een realistischer beeld van de systeemintegriteit en worden zwakke schakels in kaart gebracht voordat ze falen. En juist door deze risico's al vroeg in kaart te brengen, kunnen deze meegenomen worden in de ontwerpfase en kan men passende maatregelen/condities creëren zodat deze risico's worden voorkomen.

Verder benadrukt SbD dat beveiligingsrisico's (*security*) direct meegenomen worden in de gevarenidentificatie. In een steeds meer digitale industriële omgeving zijn opzettelijke sabotage of

cyberaanvallen reële scenario's. Overheden bevelen aan om bijvoorbeeld methodieken als de NIS2⁵-richtlijn, of de ANSI/API Standard 780⁶ 'Security Risk Assessment' toe te passen bij het identificeren van hazards. Daarmee kunnen beveiligingsdreigingen (die in dichtbevolkte of gevoelige gebieden extra relevant zijn) naast de conventionele veiligheidsrisico's worden beoordeeld. Door *safety én security* te integreren, anticipeert men op kettingreacties waarbij een bewuste aanval tot een technisch ongeval kan leiden.

Ten slotte vraagt SbD in deze stap om een *iteratieve en dynamische benadering*. In plaats van een eenmalige HAZOP of checklist-achtige inventarisatie, worden gevaren continu geactualiseerd gedurende de levensduur van het systeem. Dit sluit aan bij het idee van dynamisch risicomanagement: nieuwe informatie, bijvoorbeeld van inspecties, near-misses of veranderende bedrijfsomstandigheden, wordt steeds teruggekoppeld. Moderne, dynamische 'hazard identification frameworks' ondersteunen dit door voortdurend informatie te updaten en zo opkomende gevaren als gevolg van onverwachte veranderingen vast te leggen. Concreet kunnen bedrijven periodiek (bijvoorbeeld jaarlijks) hun risico-inventarisatie herzien, of dit zelfs real-time doen met behulp van sensordata en digitale monitoring. Dergelijke iteratieve aanpak zorgt dat men niet statisch blijft hangen in een verouderd beeld van de risico's, maar *agile* inspeelt op nieuwe ontwikkelingen. Simpele middelen zoals toolbox meetings⁷ dragen hier ook aan bij: deze korte veiligheidsbesprekingen aan het begin van een shift of taak helpen om werknemers met uitvoerende taken alert te houden op actuele risico's, zeker bij niet-routine klussen. Ze versterken de betrokkenheid van werknemers en borgen dat cruciale veiligheidsinformatie actueel blijft.

Door een combinatie van stakeholderparticipatie, voorzorgsdenken, oog voor gevarensynergieën en continue actualisatie, vergroot een SbD-aanpak de kans dat in de risico-identificatiefase alle relevante gevaren daadwerkelijk worden onderkend, inclusief die gevaren waarvan men aanvankelijk niet wist dat ze bestonden. Dit vormt de opstap naar een meer volledige en betrouwbare risicoanalyse in de volgende stap.

2.3 Risicoanalyse

In de fase van risicoanalyse worden de geïdentificeerde risicoscenario's gekwantificeerd in termen van hun waarschijnlijkheid en potentiële gevolgen. Dit houdt doorgaans in dat men enerzijds een *frequentieanalyse* uitvoert (hoe vaak kan het scenario optreden?) en anderzijds een *gevolgenanalyse* (wat is de impact als het gebeurt?). Kwantitatieve risicoanalyses (QRA's) zijn hiervoor een gangbaar instrument: zij berekenen bijvoorbeeld kanscontouren of faalfrequenties en vergelijken die met gestelde criteria. Echter, zowel in de gevolgeschatting als in de frequentieberekening sluipen onzekerheden naar binnen, vooral bij nieuwe of complexe systemen. Onzekerheden in deze stap kunnen leiden tot een vertekende voorstelling of onderschatting van de ernst van risico's, en daarmee tot verkeerde prioritering van beheersmaatregelen.

Een eerste uitdaging is dat conventionele risicoanalyses zich richten op *acute en directe* gevolgen. Zoals eerder benoemd bij de contextbepaling, kan dit betekenen dat meer subtiele of langdurige effecten onderbelicht blijven. Bijvoorbeeld, een QRA voor een chemische fabriek berekent meestal het directe effect van een gaswolkexplosie in termen van acute slachtoffers en directe schades. Niet direct zichtbare gevolgen zoals mogelijke chronische gezondheidseffecten door milde blootstelling, langdurige evacuaties van omliggende woonwijken of verlies in ecosystemen, worden minder

⁵ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/>

⁶ <https://standards.globalspec.com/std/1603209/ansi-api-std-780>

⁷ <https://www.arbocentrum.nl/kennisbank/wat-zijn-de-regels-voor-een-toolbox-en-hoe-zien-deze-eruit/>

gemakkelijk in harde getallen gevangen en blijven daarom vaak buiten beschouwing. Hierdoor kan de ernst van een scenario in werkelijkheid groter zijn dan de cijfers suggereren.

Daarnaast geldt dat bij innovatieve systemen data vaak schaars is en modellen onzeker zijn, vooral voor zeldzame of ongekende (bijvoorbeeld 'black swans') gebeurtenissen, wat het moeilijk of zelfs onmogelijk maakt om toekomstige waarschijnlijkheden nauwkeurig te voorspellen (Lauridsen et al., 2002; Salvi & Debray, 2006). Experts die dergelijke analyses uitvoeren, verkeren in onbekend terrein: hun ervaring hebben ze opgedaan in andere contexten, waardoor ze niet geheel bekend zijn met de nieuwe situatie en de relevante risico's. Zo ontbreken voor waterstof- of ammoniaktransport over land nog de decennialange ervaring en de vergaarde data en statistieken die men voor aardgasleidingen wel heeft. De frequenties van bepaalde storingen of lekkages moeten dan worden geschat op basis van analogieën of theoretische modellen, wat inherente onnauwkeurigheid met zich meebrengt. Soms negeren risicoanalyses zelfs kleine onzekerheden of afwijkingen, bijvoorbeeld door afrondingen of het uitsluiten van scenario's met ogenschijnlijk minimale kans. Dit kan ertoe leiden dat bepaalde risico's in het geheel niet worden meegenomen. Een concreet voorbeeld: als men denkt dat de kans op een bepaald faalscenario 'verwaarloosbaar klein' is, wordt het misschien niet doorgerekend, terwijl juist dat scenario bij nieuwe technologie onbekende *failure modes* kan bevatten die de kans groter maken dan gedacht.

Safe-by-Design in de risicoanalysefase

De SbD-benadering probeert de risicoanalyse robuuster en inclusiever te maken, vooral door verbeteringen die voortvloeien uit de voorgaande stappen. Wanneer in de contextbepaling- en risico-identificatiefase al breder is gekeken (inclusief worst-case scenario's, langetermijnperspectief en stakeholderinput), dan vormt dat een betere basis voor de risicoanalysefase.

SbD versterkt het vermogen om onzekerheden in de risicoanalyse aan te pakken door conventionele methoden aan te vullen met extra dimensies. Men zou de definitie van wat de 'grenzen' van een risicoanalyse zijn, kunnen verbreden: niet alleen de directe locatie en directe effecten, maar ook de langetermijneffecten op het omliggende milieu en de bredere gemeenschappen tellen mee. Dergelijke integrale benadering dwingt om ook diffuse of toekomstige gevolgen mee te wegen, zoals bodem- of waterverontreiniging op de langere termijn, psychosociale effecten op gemeenschappen, cumulatieve milieu-impact van combinaties van verontreinigingen, en mogelijke impact op toekomstige generaties.

Ook wordt voorgesteld om naast kwantitatieve uitkomsten ook *kwalitatieve* en *waarden-gedreven* elementen in de analyse te betrekken. Overheden kunnen bijvoorbeeld eisen dat bij grootschalige industriële projecten de langetermijnpact uitdrukkelijk in kaart wordt gebracht, zowel in kwantitatieve cijfers als kwalitatief beschreven effecten. Dit betekent bijvoorbeeld dat men bij een potentieel ongeval niet alleen de directe schade (€) berekent, maar ook schat wat de kosten van biodiversiteitsverlies, maatschappelijke ontwrichting (bijvoorbeeld evacuatie) of reputatieschade voor het bedrijf zouden zijn. Methoden hiervoor zijn beschikbaar: er zijn ISO-normen zoals ISO 31010⁸ (Risk Assessment) en managementstandaarden als ISO 14001⁹ (milieumanagement) die organisaties kunnen helpen deze aspecten systematisch mee te nemen. Dergelijke raamwerken bevorderen bovendien dat resultaten van risicoanalyses niet op zichzelf staan, maar worden geïntegreerd in het bredere veiligheidsbeheersysteem en worden vertaald naar concrete acties.

⁸ <https://www.iso.org/standard/72140.html>

⁹ <https://www.iso.org/standard/60857.html>

Ook binnen organisaties zelf valt winst te behalen door bij risicoanalyses verder te kijken dan alleen technische uitkomsten en acute gevolgen. SbD moedigt bedrijven aan om *duurzaamheid en milieuveiligheid* expliciet in de projectdoelstellingen te verankeren en mee te nemen in risicoanalyses. Bijvoorbeeld door bij elke geïdentificeerde hazard te vragen: wat betekent dit voor onze duurzaamheidsdoelen, voor het milieu, voor de maatschappij? Een praktisch instrument hiervoor is het integreren van risicoanalyses over de hele levenscyclus in vergunningsvereisten (bijvoorbeeld via milieueffectrapportages). Door een *levenscyclusbenadering* te hanteren – dus te analyseren hoe risico's zich kunnen ontwikkelen tijdens ontwerp, operatie, onderhoud en zelfs ontmanteling – krijgt men inzicht in langetermijnsrisico's en kan men proactief maatregelen treffen die ook in latere fases veiligheid garanderen. Dit helpt bedrijven bovendien om te voldoen aan toekomstige wetgeving (zoals de EU-taxonomie¹⁰ voor duurzame financiering, die vereist dat bedrijven hun milieurisico's beheersen).

Wat de frequentieanalyse betreft stimuleert SbD het gebruik van de *best beschikbare kennis en technieken*. Voor nieuwe risico's, waar men beperkte data heeft, wordt aangeraden om niet alleen op kwalitatieve 'expert judgement' te vertrouwen, maar ook actief op zoek te gaan naar aanvullende kwantitatieve methoden. In Nederland schrijven richtlijnen (zoals het Besluit Externe Veiligheid Inrichtingen¹¹ – BEVI – en Transportroutes¹² – BEVT) al kwantitatieve risico-eisen voor. Toch vallen veel organisaties in de dagelijkse praktijk vooral terug op generieke veiligheidsindexen en expert-oordelen. Overheden kunnen hier ingrijpen door bij vergunningen het gebruik van probabilistische analyses en geavanceerde inspectieprogramma's te stimuleren. Dergelijke inspectieprogramma's, bijvoorbeeld risicogebaseerd onderhoud, leveren actuele data over de conditie van systemen, wat de frequentieanalyse voedt met *real-time* informatie en zo onzekerheden verkleint. Binnen organisaties vergt dit investeringen in continue beoordeling van de *geschiktheid voor gebruik* (fitness for service) van assets. Dit kan door het toepassen van moderne inspectietechnieken, zoals digitale monitoring en IoT-sensoren. Maar ook door het samenwerken in de branche om kennis over faalkansen te delen. Ook het reeds integreren van technologieën in de ontwerpfase die latere inspectie vergemakkelijken, verhoogt de betrouwbaarheid op de lange termijn. Zulke maatregelen geven veiligheidsmanagers beter inzicht in de actuele faalkansen van systemen en stellen hen in staat tijdig in te grijpen – cruciaal in een dynamische risicoanalyse-aanpak.

Omdat geen enkele modelberekening 100% zekerheid geeft, benadrukt SbD tot slot het *bewust blijven van onzekerheden* tijdens de risicoanalyse. Professionals dienen alert te zijn op afwijkingen tussen hoe een systeem is ontworpen/geanalyseerd en hoe het zich in werkelijkheid gedraagt. Door dynamische inspectieprogramma's op te zetten, en continu actuele inspectiegegevens te vergelijken met ontwerpmodellen, kunnen aannames in de risicoanalyse worden getoetst en waar nodig bijgesteld. Geavanceerde technieken als digitale tweelingen (digital twins), Bayesiaanse modellen en feedback loops in risicomodellen ondersteunen dit proces: zij integreren nieuwe informatie iteratief zodat de onzekerheidsmarges kleiner worden. Een praktisch effect is dat mitigerende of preventieve maatregelen beter kunnen worden geprioriteerd – men ziet immers sneller welke berekende risicocijfers afwijken van de realiteit en waar extra beheersing nodig is. De risicoanalyse evolueert daarmee van een statische oefening tot een *dynamisch en responsief* onderdeel van risicomanagement, continu gevoed door monitoringresultaten uit de laatste fase.

Om de effectiviteit van dynamische risicoanalyse verder te vergroten, is het essentieel om inspectietechnieken te verfijnen. Een cruciale eerste stap hierbij is het uitvoeren van een nulmeting: een referentie-inspectie die als basis dient voor het detecteren van latere afwijkingen. Door

¹⁰ https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/eu-taxonomy-sustainable-activities_en

¹¹ <https://wetten.overheid.nl/BWBR0016767/2016-01-01>

¹² <https://wetten.overheid.nl/BWBR0034233/2015-04-01>

gestructureerd te vergelijken met deze nulmeting kunnen subtiele veranderingen tijdig worden geïdentificeerd, en kan er beoordeeld worden of een systeem zich binnen aanvaardbare risicogrenzen bevindt of dat bijsturing noodzakelijk is. Pas wanneer over een langere periode sprake is van stabiliteit – waarbij het systeem herhaaldelijk geen afwijkingen ten opzichte van de nulmeting vertoont – kan overwogen worden de inspectie-intervallen te verlengen.

Door op deze wijze in de risicoanalyse niet alleen 'harde' data maar ook voorzorg, lange termijn visie en adaptief leren centraal te stellen, krijgen besluitvormers een vollediger en betrouwbaarder beeld van de risico's. Dit is essentieel om in de volgende stap, de risico-evaluatie, goed onderbouwde beslissingen te nemen over welke risico's acceptabel zijn en welke niet.

2.4 Risico-evaluatie

Tijdens de fase van risico-evaluatie worden de resultaten van de risicoanalyse afgewogen tegen criteria om te beslissen of risico's *aanvaardbaar* zijn, of dat er verdere maatregelen nodig zijn. Dit is bij uitstek een fase waarin waardeoordelen en beleidskeuzes een rol spelen: wat voor de één acceptabel is, is dat voor de ander misschien niet. Onzekerheden kunnen de kwaliteit van deze beslissingen sterk beïnvloeden. Vooral wanneer men te maken heeft met nieuwe risico's die niet goed in bestaande richtlijnen passen, of wanneer de criteria voor risicotoelaatbaarheid vaag zijn, wordt risico-evaluatie lastig. Ook spelen cognitieve *biases* mee; besluitvormers (of experts die adviseren) kunnen onbewust een voorkeur hebben voor een bepaalde uitkomst op basis van hun achtergrond, ervaring of belangen. Zo kan een bedrijf, omdat er bedrijfsmatige of financiële overwegingen meespelen, een risico als 'laag genoeg' bestempelen als de wettelijke norm niet overschreden wordt, terwijl omwonenden of andere stakeholders datzelfde risico mogelijk onaanvaardbaar vinden gezien de onzekerheden.

Safe-by-Design in de risico-evaluatiefase

Een SbD-aanpak probeert de risico-evaluatie te *verbreden* en te *verscherpen* en te ontdoen van ongegronde aannames. Centraal hierin staat opnieuw het *voorzorgsprincipe*: wanneer er enige aanleiding is tot twijfel bij het inschatten van nieuwe risico's (effect of kans) door nieuwe omstandigheden, ga dan uit van worst-case scenarios. Door expliciet te veronderstellen dat het mis *kán* gaan en te kijken naar de meest ernstige gevolgen, voorkomt men dat een risico onderschat enkel omdat de kans gering lijkt. Deze benadering dwingt besluitvormers veiligheid voorop te stellen, met name als gegevens onzeker zijn. Organisaties worden zo aangespoord om hogere veiligheidsniveaus na te streven dan strikt juridisch vereist is, juist omdat minimale eisen ontoereikend kunnen blijken voor nieuwe complexe systemen. Bij nieuwe infrastructuur gelieerd aan de energietransitie zijn bijvoorbeeld de *failure modes* nog onzeker; een conservatieve evaluatie zou kunnen inhouden dat men extra veiligheidsmarges inbouwt en voorlopig uitgaat van strengere criteria tot er meer zekerheid (ervaring met en data over het gebruik) is.

Overheden kunnen dit stimuleren via vergunningverlening. In vergunningseisen kan expliciet worden opgenomen dat bij processen of systemen met beperkte ervaring strengere, conservatievere risico-evaluaties moeten worden toegepast die passen bij de mate van onzekerheid. Conventionele risicostudies houden immers vaak amper rekening met onzekerheidsmarges, wat maakt dat de ernst van risico's in nieuwe systemen kan worden onderschat. Bijvoorbeeld in de context van waterstof- of CO₂-leidingen voor de energietransitie: dergelijke leidingen opereren mogelijk bij hogere druk en temperatuur en lopen via trajecten die kunnen afwijken van bestaande aardgasleidingen. Van bedrijven zou geëist mogen worden dat ze in hun risico-evaluatie aantonen deze verschillen te hebben meegenomen. Dit leidt er bijvoorbeeld toe dat ze aanvullende risicobeheersmaatregelen treffen voor

scenario's die in oude richtlijnen niet voorkwamen. Denk aan het opnemen van extra veiligheidsmarges in berekeningen, het instellen van dynamische en strengere monitoringseisen, of het invoeren van adaptieve maatregelen die risicobeheersing bijsturen naarmate men leert. In feite kan zo via het vergunningstelsel het voorzorgsprincipe, en dus de SbD-mentaliteit, al ingebed worden binnen organisaties: bij nieuwe onzekerheden meer doen dan enkel wat strikt nodig is.

Een SbD-mentaliteit gaat er bovendien van uit dat bij twijfelgevallen altijd wordt gekozen voor de optie die het voorzorgsprincipe het meest respecteert, ook als dit leidt tot extra inspanning of kosten. *Voorzorg bij risicoprioritering* betekent dat een veiligheidsafdeling de ruimte en steun krijgt om "nee" te zeggen tegen operaties waarvan de risico's niet goed bekend zijn. Hoewel dit op korte termijn tot extra kosten of gemiste kansen kan leiden, zijn de potentiële lange termijnbaten (het voorkomen van een ramp met alle bijhorende kosten, behoud van reputatie, en een veerkrachtigere organisatie) vele malen groter. Het management moet dus niet louter op compliance sturen (voldoen we aan de norm = klaar), maar juist teams aansporen om *ambitieuze veiligheidsdoelen* te stellen dan de wet minimaal vereist. Door intern dit 'beyond compliance'-principe te omarmen en successen op dat gebied te erkennen, ontstaat een houding waarbij men proactief extra maatregelen treft. Dit straalt bovendien positief af op het publieke vertrouwen: een organisatie die vrijwillig strengere veiligheidsnormen hanteert, toont leiderschap in maatschappelijk verantwoord ondernemen en veiligheidszorg.

Op methodologisch niveau kan SbD de risico-evaluatie verbeteren door *waarde-gedreven besluitvorming* te integreren. In plaats van alleen cijfers te vergelijken met drempelwaarden, kan er ook gekeken worden naar moeilijk kwantificeerbare waarden. Multicriteria-analyse of beslistkundige raamwerken kunnen helpen om aspecten als milieuschade, sociale gevolgen of ethische bezwaren een expliciete plek te geven in de risico-evaluatie. Zo kan een matrix opgesteld worden waarin naast het verwachte aantal (acute) slachtoffers ook bijvoorbeeld de impact op de reputatie van het bedrijf of het verlies aan ecosystemen wordt beoordeeld. Het gebruik van *kosten-batenanalyses* wordt eveneens aangemoedigd, zij het met een lange-termijnhorizon. Bij traditionele kosten-batenanalyses worden langlopende effecten vaak weggelaten; SbD raadt aan om ook die effecten (bijvoorbeeld milieurisico's die zich wellicht pas na jaren manifesteren) mee te nemen. Tegelijkertijd ligt hier een belangrijke rol voor de overheid: niet alleen als toezichthouder, maar ook als kadersteller. De overheid kan, in overleg met experts en belanghebbenden, minimale SbD-vereisten formuleren die langetermijnrisico's expliciet meenemen. Tegelijk moet worden gewaakt voor het terugvallen in de oude, normatieve systematiek waarin naleving belangrijker wordt dan inhoudelijke reflectie. Om te voorkomen dat bedrijven SbD slechts gebruiken als label zonder substantiële verandering (wat gezien kan worden als een vorm van *safetywashing*¹³), is transparantie essentieel. Het openbaar maken, of aanleveren van gebruikte risicomatrices en ontwerpafwegingen maakt vergelijkbaarheid tussen bedrijven mogelijk en voorkomt dat subjectieve keuzes leiden tot schijnveiligheid.

Een ander technisch aandachtspunt is het opnieuw iken van risicocriteria voor nieuwe systemen. Vaak hanteert men standaard criteria voor individueel risico (kans per jaar op dodelijk slachtoffer) of groepsrisico (Vrouwenvelder et al., 2001), of ALARP-principes (*As Low As Reasonably Practicable*). Bij projecten waar met nieuwe, onbekende technieken of infrastructuur wordt gewerkt, zouden deze criteria bijgesteld moeten worden om de onzekerheden die hierbij komen kijken te weerspiegelen. In lijn met SbD zouden er bijvoorbeeld extra *veiligheidsmarges* ingebouwd kunnen worden in toelaatbaarheidsgrenzen wanneer er onzekerheid is over data. Dit komt neer op het hanteren van

¹³ Safetywashing is de praktijk van het promoten en profileren van veiligheidspraktijken zonder volledige openheid over negatieve informatie, met als doel het imago van een organisatie te verbeteren. Safetywashing is vergelijkbaar met greenwashing, waarbij een organisatie het imago probeert te verbeteren door een positief beeld te schetsen van hun milieuvriendelijke waarden en inzet voor duurzaamheid. Net als bij greenwashing wordt bij safetywashing de publieke beeldvorming beïnvloed zonder dat er sprake hoeft te zijn van daadwerkelijke verbeteringen op het gebied van veiligheid (Ninan & van Nunen, 2025).

conservatievere grenswaarden. Ook kan men besluiten niet alleen naar waarschijnlijkheden te kijken maar ook naar het *ernstniveau* van gevolgen: dat wil zeggen, een scenario met potentieel ernstige impact als reëel risico beschouwen, zelfs wanneer de waarschijnlijkheid onzeker is of gering lijkt. Dit is feitelijk een toepassing van het voorzorgsprincipe: liever uitgaan van ernst dan van kans bij nieuwe onzekere risico's. Verder dienen organisaties en experts zich bewust te zijn van mogelijke vooringenomenheid bij kwalitatieve oordelen. Om te voorkomen dat persoonlijke inschattingen te veel gewicht krijgen kunnen gestructureerde methoden zoals de Delphi-methode of collegiale toetsing gebruikt worden voor risico-evaluatie. Door meerdere experts onafhankelijk een oordeel te laten vormen en die samen te brengen, of door gebruik te maken van ondersteunende beslissingssoftware, wordt de objectiviteit vergroot. Het betrekken van diverse disciplines (technisch, milieu, sociaal) minimaliseert de kans dat blinde vlekken blijven bestaan.

Al deze maatregelen hebben als doel om in de risico-evaluatiefase het besluit over 'aanvaardbaar of niet' zo onderbouwd en conservatief mogelijk te maken, gegeven de onzekerheden. Op die manier worden scenario's met potentieel grote gevolgen niet te snel afgedaan als acceptabel. Wat als onaanvaardbaar wordt aangemerkt, stroomt door naar de volgende fase: de risicobehandeling, waar daadwerkelijk ingegrepen gaat worden om het risico te reduceren.

2.5 Risicobehandeling

Risicobehandeling is de fase waarin voor de onaanvaardbaar bevonden risico's maatregelen worden geïmplementeerd. Dit kan variëren van het elimineren van de bron van gevaar (zoals een proces stoppen of een stof substitueren), het reduceren van de kans of het beperken van de gevolgen, tot het voorbereiden van responsmaatregelen om de impact te mitigeren mocht er toch iets misgaan. In wezen vertaalt risicobehandeling het papierwerk van analyses en evaluaties naar *concrete, tastbare acties*. Juist daarom is dit een cruciale stap: gedegen analyses leiden niet altijd tot veiligheid, *tenzij* de juiste acties worden ondernomen. Onzekerheden spelen ook hier een rol. Als er onzekerheid is over de effectiviteit van een maatregel, of over welke maatregel het best past bij een onzeker risico, dan beïnvloedt dat direct het veiligheidsniveau dat uiteindelijk bereikt wordt. Bovendien komen in deze fase vaak praktische overwegingen om de hoek kijken (kosten, inpasbaarheid, levertijd van voorzieningen,...), wat kan resulteren in een beperkte implementatie ten opzichte van de oorspronkelijke intentie.

Traditioneel gezien hebben veel organisaties de neiging risicobehandeling op te vatten als een compliance-taak: voldoen aan hetgeen dat de wet voorschrijft, vaak door middel van technische veiligheidsmaatregelen. Veiligheid wordt dan een kwestie van vinkjes zetten; "hebben we een sprinklersysteem, een noodplan, explosiebeveiliging? Dan voldoen we aan de regels." In dergelijke benadering blijft veiligheid een bijzaak, een soort add-on op het ontwerp, in plaats van een integraal ontwerpprincipe. Dit leidt er vaak toe dat men voornamelijk inzet op *actieve* of procedurele maatregelen (bijvoorbeeld extra sensoren, noodstoppen, gedetailleerde procedures) om risico's te beheersen, terwijl fundamentele oplossingen misschien nooit zijn overwogen. Dit kent twee wezenlijke implicaties. Ten eerste behandelt men symptomen in plaats van oorzaken: het gevaar zelf blijft bestaan, men probeert alleen de gevolgen te beperken. Ten tweede zijn actieve maatregelen storingsgevoelig en afhankelijk van menselijk handelen. Het inzetten op actieve maatregelen gaat vaak schuilt achter een mentaliteit waarin veiligheid wordt afgevinkt in plaats van intrinsiek nagestreefd. Kostenafwegingen en kortetermijndoelen domineren, waardoor structurele risicovermijding onderbelicht blijft. SbD vraagt juist om een diepere vorm van 'in control zijn', waarbij veiligheid in ontwerpkeuzes en bedrijfsvoering centraal staan.

Safe-by-Design in de risicobehandelingfase

De SbD-filosofie pleit voor een meer integrale aanpak dan enkel *compliance*: maak veiligheid onderdeel van het *ontwerp* en de *bedrijfsvoering* zelf. Inherente veiligheid is daarbij een leidend principe, wat inhoudt dat men gevaren aan de bron wegneemt of minimaliseert, in plaats van te vertrouwen op toevoegingen achteraf. Overheden kunnen dit ondersteunen door bijvoorbeeld bij vergunningen of subsidies eisen te stellen aan het toepassen van inherent veilige ontwerpprincipes in nieuwe installaties.

Vier klassieke strategieën voor inherente veiligheid zijn: elimineren of *substitueren* van gevaarlijke stoffen door minder gevaarlijke alternatieven; *minimaliseren* van hoeveelheden van gevaarlijke stoffen of energie (intensiteit verlagen); *matigen* van procesomstandigheden (lagere drukken, temperaturen) en het *beperken van effecten* door bijvoorbeeld fysieke barrières of afstand (isoleer bronnen zodat een incident niet overal impact heeft). Wanneer (combinaties van) deze vier worden toegepast, kan men vaak al een aanzienlijke risicoreductie bereiken. Echter, SbD erkent dat niet alle risico's volledig inherent weg te ontwerpen zijn. Sommige rest-risico's blijven en daarvoor zijn andere maatregelen nodig. Men kiest daarom idealiter voor een *gelaagde aanpak*: eerst zoveel mogelijk inherent veilig maken, en rest-risico's opvangen met preventieve en vervolgens mitigerende maatregelen. Deze filosofie ligt in lijn met de Seveso III/BRZO-verplichtingen: voorkom ongevallen zoveel mogelijk, maar zorg ook voor mitigatie als er toch iets gebeurt. Daarnaast dient men deze filosofie ook door te voeren in andere, organisatorische zaken. Denk aan een noodproceduredocument van 50 pagina's versus 5 pagina's – personeel zal eerder de kortere versie correct opvolgen. In lijn met SbD wordt daarom aangeraden veiligheidsprocedures beknopt en gebruiksvriendelijk te houden.

Ter ondersteuning van inherente veiligheid introduceert SbD een *hiërarchie van ontwerpstrategieën* die professionals kunnen volgen. Let wel, deze hiërarchie dient niet te worden gezien als een 'checklist' (zie ook Hoofdstuk 3), maar juist als een leidraad. Door deze lijst te volgen, wordt risicobehandeling niet iets wat achteraf wordt gedaan, maar wordt het een integraal onderdeel van het systeemontwerp en -beheer waardoor een hoger *inherent* veiligheidsniveau wordt bereikt. Hierdoor daalt de kans op zware ongevallen drastisch.

SbD-hiërarchie van ontwerpstrategieën

1. *Elimineer* gevaren waar mogelijk.
2. *Vervang* gevaarlijke elementen door minder gevaarlijke (substitutie).
3. *Reduceer* de hoeveelheid of energie-inhoud (minimalisatie/intensivering).
4. *Matig* de omstandigheden (druk, temperatuur, reactieve stoffen) tot veiligere niveaus.
5. *Isoleer* of *beperk de effecten* door ontwerpen zo te maken dat als er iets misgaat, de impactzone klein blijft (bijvoorbeeld door compartimentering).
6. *Vereenvoudig* systemen zodat er minder fout kan gaan.
7. Ontwerp met *fouttolerantie* en *domino-effecten* in het achterhoofd; een enkelvoudige storing mag niet tot ketenreactie leiden.
8. Gebruik waar mogelijk *passieve* in plaats van actieve veiligheidsmaatregelen en zorg dat actieve systemen *fail-safe* zijn.
9. Zorg voor *gebruiksvriendelijke besturing* en interface, zodat operatoren in stressvolle situaties niet verdwalen in complexiteit.
10. Houd rekening met de *volledige levenscyclus* – ontwerp ook met het oog op veilige constructie, onderhoud en uiteindelijke ontmanteling.
11. Zorg er voor dat veiligheid een *iteratief proces* is: monitoring van veiligheidsmaatregelen, evaluatie, communicatie en herziening maken deel uit van een dynamische risicobeheersstrategie.
12. Maak stakeholder consultatie een breed, open, en iteratief (niet-eindig) proces.

Een belangrijk aspect van risicobehandeling onder SbD is bovendien de voorbereiding op noodsituaties, *rekening houdend met het ergste scenario*. Men erkent dat ondanks alle preventie, een restrisico¹⁴ blijft bestaan. Daarom moeten organisaties en overheden gezamenlijk zorgen dat, mocht een ongeval plaatsvinden, de gevolgen beheersbaar zijn. Dit kan door bijvoorbeeld hulpdiensten te betrekken in de vormgeving en besluitvorming over veiligheidsmaatregelen. Brandweer en rampenbestrijders weten uit de praktijk welke scenario's beheersbaar zijn en welke niet (*tacit knowledge*), en kunnen adviseren over voorzieningen die nodig zijn om adequaat te kunnen ingrijpen. Dergelijke samenwerking leidt tot realistische noodplannen die aansluiten bij de capaciteit van lokale hulpdiensten. Organisaties op hun beurt doen er goed aan nauwe relaties op te bouwen met brandweer en GHOR (Geneeskundige Hulpverleningsorganisatie in de Regio)¹⁵. Door deze partijen inzicht te geven in de risico's en worst-case scenario's van de installatie, kunnen hulpdiensten beter trainen en voorbereiden op een eventuele calamiteit. Hierdoor zullen (grote) incidenten effectiever bestreden worden, en blijven maatschappelijke risico's bedwongen.

Naast technische en fysieke maatregelen wijst SbD ook op het belang van *menselijke en organisatorische maatregelen*. Training is daarvan een pijler. Overheden kunnen strengere trainingseisen opleggen voor hoog-risico industrieën, en organisaties zelf worden aangemoedigd om te investeren in geavanceerde veiligheidsopleidingen voor hun personeel. Goed getraind personeel is beter voorbereid op abnormale of onverwachte situaties en zal minder snel fouten maken onder stress. Regelmatige *drills*, scenariotrainning (inclusief worst-case simulaties) en contractor training zorgen dat iedereen die op het terrein werkt weet wat te doen en wat van hen verwacht wordt in nood.

¹⁴ Restrisico's zijn risico's die overblijven na het uitvoeren van een risico-inventarisatie en -evaluatie. Het zijn risico's die niet met de geïmplementeerde maatregelen kunnen worden weggenomen of gemitigeerd.

¹⁵ <https://www.rijksoverheid.nl/onderwerpen/veiligheidsregios-en-crisisbeheersing/geneeskundige-hulpverleningsorganisatie-in-de-regio-ghor>

Ook onderhoud maakt onderdeel uit van risicobehandeling: een zorgvuldig ontworpen veiligheidssysteem verliest zijn waarde als het niet operationeel is tijdens een kritieke situatie. Daarom promoot SbD het invoeren van *risicogebaseerd en conditie-gebaseerd onderhoud* als norm. Overheid en sector kunnen samen richtlijnen opstellen die ervoor zorgen dat kritieke apparatuur proactief wordt onderhouden op basis van werkelijke slijtage en risico-inschatting, in plaats van louter reactief. Organisaties dienen hiervoor middelen vrij te maken en dergelijke onderhoudsprogramma's structureel in te bedden. Zo blijven veiligheidskritieke systemen (zoals drukventielen, explosiebeveiligingen) betrouwbaar en beschikbaar.

2.6 Monitoring, evaluatie, communicatie en consultatie

Risicomanagement eindigt niet na het nemen van maatregelen; het is een *continu* en *iteratief* proces. Monitoring en evaluatie vormen de terugkoppeling waarmee men bewaakt of de genomen risicobeheersmaatregelen inderdaad het beoogde effect bereiken. Bovendien is het de fase waarin nieuwe gevaren of veranderingen in bestaande risico's opgespoord moeten worden. Deze stap is cyclisch van aard: resultaten uit monitoring vloeien weer terug naar eventuele bijstellingen in context, identificatie, etc. Communicatie en consultatie lopen als een dwarse activiteit door dit geheel heen, omdat op elk moment stakeholders geïnformeerd en betrokken moeten worden. In Figuur 1 wordt deze continue en iteratieve aard van risicomanagement benadrukt. Monitoring, beoordeling, communicatie en consultatie zijn geïntegreerde activiteiten die ervoor zorgen dat veiligheidsmaatregelen gedurende de *gehele levenscyclus* van een systeem effectief blijven. Naarmate systemen ouder worden, gebruikspatronen veranderen of nieuwe inzichten ontstaan, moeten risico's opnieuw beoordeeld en beheerst worden.

Safe-by-Design in de fase van monitoring, evaluatie, communicatie en consultatie

Monitoring gaat verder dan het enkel aflezen van bestaande data. Effectieve monitoring omvat rigoureuze inspectieprogramma's en het gebruik van geavanceerde technologieën om een realistisch en gedetailleerd beeld te krijgen van de conditie van installaties. In de onshore oliesector is duidelijk geworden wat er kan gebeuren bij gebrekkige monitoring: van 100 onderzochte grote ongevallen bleken er 17 direct verband te houden met falende apparatuur als gevolg van inadequate inspecties (API, 2021). De explosie in de BP Texas City raffinaderij (2005) en de Piper Alpha ramp op het Noordzee-platform (1988) zijn voorbeelden waar achteraf geconcludeerd werd dat cruciale waarschuwingssignalen en ontwerptekortkomingen in de procesbewaking niet tijdig waren opgemerkt. Dergelijke incidenten onderstrepen dat men door continue en nauwgezette monitoring veel ongevallen kan voorkomen. Daarom adviseren moderne richtlijnen het toepassen van *risico- en conditie-gebaseerde inspectiestandaarden*. Zo zijn er internationale normen zoals EN 16991¹⁶ (risicogebaseerd inspectiekader) en API RP 580¹⁷/581¹⁸ (Recommended Practice for Risk-Based Inspection) die bedrijven helpen te bepalen waar en wanneer te inspecteren op basis van risico-inzichten. Door hun assets te monitoren op indicatoren van slijtage, corrosie, trillingen, etc., kunnen bedrijven kwetsbaarheden vroegtijdig detecteren en onderhoud gericht prioriteren.

Tegenwoordig biedt digitalisering nieuwe mogelijkheden: digital twins, real-time sensornetwerken en het Internet of Things (IoT) maken het mogelijk om continu de 'gezondheid' van systemen te bewaken. Een SbD-georiënteerde organisatie investeert in dergelijke IoT-gestuurde risicobewakingskaders. Daarmee kunnen risico's dynamisch worden geactualiseerd en kunnen afwijkingen of trends die op

¹⁶ <https://www.nen.nl/nen-en-16991-2018-en-246232>

¹⁷ <https://www.api.org/products-and-services/individual-certification-programs/certifications/api580>

¹⁸ <https://inspectioneering.com/tag/api-rp+581>

opkomende gevaren duiden, direct worden gesignaleerd. Dit vergroot het aanpassingsvermogen van de organisatie aan veranderende omstandigheden, omdat men sneller inzicht heeft in nieuwe risico's en direct maatregelen kan treffen. Een praktisch voorbeeld is het plaatsen van slimme corrosiesensoren op pijpleidingen die realtime data geven; zodra corrosie sneller gaat dan verwacht, kan men direct ingrijpen (bijvoorbeeld de leidingdruk verlagen of het corrumperende medium aanpassen) in plaats van te wachten op de volgende geplande inspectie. Het werken met nulmetingen – een referentie-inspectie die als basis dient voor het detecteren van latere afwijkingen – kan dit proces ondersteunen (zoals toegelicht in deel 2.3).

Overheden kunnen het monitoren ook ondersteunen door het *verspreiden van kennis over de beste beschikbare technologieën* voor inspectie en monitoring, zoals voorbeelden van succesvolle toepassingen van bijvoorbeeld drones voor fakkeltoren-inspectie, of AI voor patroonherkenning in procesdata om afwijkingen vroegtijdig te identificeren. Dit verlaagt voor individuele bedrijven de drempel om zulke technologie te adopteren, vooral voor kleinere spelers die minder eigen expertise hebben.

Naast fysieke monitoring is ook het *monitoren van veiligheidsperformance* essentieel. Procesveiligheidsindicatoren, zoals die gedefinieerd in API RP 754 (API, 2021) voor de petrochemie, stellen organisaties in staat om bijna-incidenten, storingen van veiligheidslagen en operationele afwijkingen systematisch bij te houden. Door deze indicatoren te volgen, kunnen trends worden ontdekt die op verslechtering duiden. Vroegtijdige identificatie van dergelijke tekortkomingen maakt corrigerende acties mogelijk nog vóórdat zich een ongeval voordoet. Bijvoorbeeld, een toenemend aantal kleine lekkages (Tier 3-incidenten) kan een voorbode zijn van een grote lekkage, en zou aanleiding moeten geven tot diepgaand onderzoek en herstelmaatregelen.

Evaluatie in deze laatste fase betekent dat de organisatie periodiek het hele risicoprofiel opnieuw bekijkt. Zijn er nieuwe activiteiten begonnen? Zijn er veranderingen in de omgeving (zoals nieuwbouw rond de inrichting, klimaatverandering die extremere weersomstandigheden brengt) waardoor eerdere inschattingen bijgesteld moeten worden? Door geregeld risicoscenario's te herzien en nieuwe gevaren te identificeren, krijgt men een steeds completer inzicht in de risico's voor de omgeving, werknemers en de organisatie. Dergelijke herzieningen, bijvoorbeeld jaarlijkse veiligheidsreviews of vijfjaarlijkse uitgebreide HAZOP-updates, zijn cruciaal om het risicomanagement in lijn te houden met de actuele situatie. In Nederland schrijft de regelgeving al minimaal vijfjaarlijkse actualisatie van QRA's voor, maar SbD zou zelfs pleiten voor *continu* verbeteren: als best practice kan een site bijvoorbeeld een living QRA hanteren die jaarlijks bijgesteld wordt met de laatste inzichten, zeker in dynamische sectoren als de energietransitie. Ook leent Management of Change (MoC) zich uitermate goed voor periodieke evaluatie. MoC biedt een structureel proces om geplande (en soms ongeplande) veranderingen tijdig te signaleren, te beoordelen en te beheersen voordat ze worden doorgevoerd. Denk aan wijzigingen in processen, installaties, materialen, technologie of organisatie – factoren die het risicoprofiel aanzienlijk kunnen beïnvloeden. MoC kan hier dus een sleutelrol vervullen: zodra een verandering plaatsvindt of wordt overwogen, activeert het proces automatisch een risicobeoordeling. Daarmee vormt het een belangrijk vangnet dat kan voorkomen dat kleine of interne aanpassingen onopgemerkt leiden tot nieuwe kwetsbaarheden.

Communicatie en consultatie zijn essentieel om het risicomanagement kenbaar te maken aan alle stakeholders, zowel intern als extern, en om er draagvlak voor te creëren. In de ontwerp- en besluitvormingsfase helpt goede communicatie om stakeholders (intern en extern) mee te nemen en verwachtingen te managen. Dit voorkomt verrassingen of verzet achteraf. In de operationele fase wordt communicatie een doorlopend feedbackmechanisme.

Interne communicatie zorgt ervoor dat iedereen met een veiligheidskritische rol steeds op de hoogte is van de actuele veiligheidstoestand. Dit stelt hen in staat proactief tekortkomingen aan te pakken, bijvoorbeeld door extra trainingen te plannen, aanpassingen van procedures door te voeren, of te investeren in betere technologie, voordat problemen escaleren.

Externe communicatie met regelgevende instanties betreft de toezichthouder bij het proces en bevordert transparantie en vertrouwen. Door tijdig incidenten te melden en open over risico's te rapporteren, voldoet een organisatie niet alleen aan de wettelijke plichten, maar bouwt men ook goodwill op. Tegelijk is communicatie met het brede publiek en andere bedrijven, zoals het delen van best practices en lessen geleerd uit incidenten, waardevol. Wanneer bedrijven onderling (zoals via brancheverenigingen) open zijn over near-misses en oplossingen, dan kan dat de hele sector veiliger maken. Overheden kunnen dit faciliteren door platforms te creëren voor dergelijke kennisdeling, binnen vertrouwelijke kaders. Het uitwisselen van operationele en incidentdata tussen publieke en private partijen zorgt voor het ontstaan van een collectief lerend vermogen, en voorkomt dat er zich 'eenzame eilandjes' van kennis vormen.

Voor communicatie richting publiek geldt dat *transparantie* (openheid) van groot belang is om vertrouwen te winnen. Men moet consistent en eerlijk communiceren over zowel risico's als getroffen maatregelen. Het Verdrag van Aarhus en de Europese wetgeving (Seveso III) verplichten al publieke communicatie over veiligheidsinformatie. Een SbD-aanpak zou er daarnaast op toezien dat zorgen van omwonenden actief worden opgehaald en beantwoord. Bijvoorbeeld via regelmatige bewonersavonden, het publiceren van toegankelijk geschreven veiligheidsrapportages, of het instellen van een omgevingsadviesraad. Dit sluit aan bij het subsidiariteitsbeginsel¹⁹ waarbij beslissingen zo dicht mogelijk bij de getroffen gemeenschappen worden genomen.

Samenvattend kan op organisatieniveau de communicatie verbeterd worden door in te zetten op drie niveaus: *intra-organisatorisch*, *inter-organisatorisch* en *regelgevend*. Intra-organisatorisch betekent zorgen voor transparante, begrijpelijke communicatie over veiligheid die alle lagen van de organisatie bereikt – van de directiekamer tot de werkvloer. Dit kan onder meer via toolbox meetings en het actief betrekken van medewerkers via overleg. Inter-organisatorisch houdt in dat veiligheidsinformatie met andere organisaties gedeeld wordt (bijvoorbeeld bedrijven op hetzelfde industrieterrein of binnen de keten) om ook buiten de poort risico's te verlagen en van elkaar te leren. Communicatie met de regelgevende instanties houdt in dat belangrijke veiligheidsinformatie proactief wordt gedeeld met autoriteiten, zodat zij beter geïnformeerd toezicht kunnen houden.

De zesde fase van risicomanagement verzekert dat 'veiligheid op papier' wordt omgezet in 'veiligheid in de praktijk', en dat veiligheid gewaarborgd blijft in een veranderende wereld. Safe-by-Design fungeert hier als verbindend principe doordat het *leren van ervaringen* en *continue verbetering* centraal stelt. SbD ziet een systeem niet als iets statisch dat veilig blijft na het ontwerp, maar als iets dat voortdurend aandacht en bijstelling behoeft naarmate nieuwe kennis beschikbaar komt. Die dynamiek is precies waar monitoring, evaluatie, communicatie en consultatie voor staan. Door data te verzamelen, door te leren, te delen, en stakeholders te blijven betrekken, ontwikkelt zich een lerende organisatie die risico's met hoge onzekerheid steeds beter beheerst. Zo ontstaat een veiligheidsbeheersysteem dat niet alleen reageert op incidenten, maar proactief anticipeert op veranderingen; een must in de context van de energietransitie en andere innovatieve ontwikkelingen. Uiteindelijk leidt dit tot een structurele borging van externe veiligheid: *niet alleen voldoen aan de norm van vandaag, maar klaar zijn voor de uitdagingen van morgen.*

¹⁹ <https://www.europarl.europa.eu/factsheets/nl/sheet/7/het-subsidiariteitsbeginsel>

3 Van 'checklistdenken' naar een Safe-by-Design mentaliteit

In de praktijk van industriële veiligheid bestaat een duidelijke voorkeur voor gestructureerde methoden zoals checklists, matrixen en beslisbomen. Deze tools zijn overzichtelijk, gestandaardiseerd, en sluiten aan bij bestaande managementstructuren. Zeker in sectoren met complexe technologieën en processen en met strikte regelgeving bieden zulke middelen houvast. Ze suggereren controle en geven richting aan besluitvorming: als alle vakjes zijn afgevinkt, dan lijkt het systeem veilig. Toch schuilt in deze benadering een fundamenteel risico. Wanneer veiligheid wordt gereduceerd tot het volgen van stappenplannen of het naleven van normen, kan dit leiden tot een vals gevoel van controle. Deze benadering stimuleert vooral naleving (*compliance*), waarbij wettelijke eisen worden 'afgevinkt', in plaats van het proactief beheersen van risico's en omgaan met onzekerheden.

In de context van opkomende risico's vraagt veiligheid méér dan het naleven van wettelijke vereisten en het voorkomen van juridische aansprakelijkheid. Een proactieve mindset waarin veiligheid vanaf de ontwerpfase wordt meegenomen, en waarbij onzekerheden proactief teruggebracht worden naar beheersbare risico's, zou de mentaliteit moeten zijn. Binnen deze mentaliteit gaat het niet om de vraag of een bedrijf achteraf 'veilig genoeg' was om claims te vermijden, maar is de drijfveer het creëren van een robuust systeem dat bestand is tegen onverwachte verstoringen. SbD kan hiervoor een kader bieden, waarbij het geen methode is die als losse checklist kan worden afgevinkt, maar als denkwijze die veiligheid structureel verankert in ontwerp, besluitvorming en organisatiecultuur.

Juist bij nieuwe technologieën en systemen, zoals pijpleidingen voor waterstof of ammoniak, staan bedrijven voor risico's met (hoge) onzekerheden die zich niet eenvoudig laten kwantificeren. Denk aan het gedrag van materialen bij hoge druk, de wisselwerking met omgevingsfactoren, of de onbekende impact van storingen op dichtbevolkte gebieden. Traditionele risicobenaderingen, gebaseerd op historische data en kwantitatieve berekeningen zoals QRA, bieden hierbij te weinig zekerheid. Wat veilig lijkt op basis van aannames of modellen, kan ontoereikend blijken wanneer onzekerheden zich anders manifesteren dan verwacht. SbD richt zich daarom specifiek op het omgaan met dergelijke onzekerheden. Door onder meer het verkennen van worst-case scenario's, het betrekken van stakeholders om hun zorgen en lokale kennis mee te nemen, en het verfijnen van inspectietechnieken kunnen bedrijven incidenten structureel voorkomen.

Het toepassen van SbD biedt verschillende tastbare voordelen. Wanneer veiligheid als integraal onderdeel van ontwerp en beheer wordt beschouwd, neemt de betrouwbaarheid en beschikbaarheid van installaties toe. Ongeplande stilstanden door lekkages of faalmechanismen worden voorkomen, en de kans op kostbare incidenten daalt. Bovendien draagt een proactieve veiligheidsaanpak bij aan het vertrouwen van burgers, bestuurders en andere stakeholders. Imagoschade, maatschappelijke weerstand en langdurige vergunningstrajecten kunnen worden beperkt als een bedrijf aantoon niet alleen wettelijk correct te handelen, maar óók maatschappelijk verantwoord.

Daarbij speelt ook de betrokkenheid van burgers een belangrijke rol. Maatschappelijke zorgen over bijvoorbeeld geur, geluid, gezondheid of rampenrisico's zijn niet altijd technisch meetbaar, maar kunnen wijzen op blinde vlekken in het ontwerp. Juist deze signalen kunnen helpen om bestaande aannames in vraag te stellen. SbD nodigt uit tot het betrekken van omwonenden, experts en andere belanghebbenden: niet als verplichting, maar als verrijking van het ontwerpproces. Een waterstofleiding

die technisch veilig is, maar maatschappelijk onacceptabel wordt geacht, is in de praktijk niet duurzaam realiseerbaar en loopt het risico op vertraging, verzet of zelfs annulering. Alleen door brede participatie ontstaat een ontwerp dat zowel robuust als maatschappelijk gedragen is.

3.1 De valkuil van beslisbomen: waarom Safe-by-Design meer vraagt dan een keuzemenu

Zoals eerder aangehaald geven bedrijven doorgaans de voorkeur aan gestructureerde en afgebakende methoden voor risicomanagement, zoals QRA. Vanuit die denkwijze ligt het voor de hand om ook SbD te benaderen als een gesystematiseerd instrument, zoals in de vorm van een stappenplan of beslisboom die richting biedt bij het managen van risico's onder onzekerheid. Echter, juist deze structurering vormt een potentiële valkuil.

Een beslisboom is ontworpen om complexiteit te ordenen: via een reeks ja/nee-keuzes wordt de gebruiker geleid naar een logische uitkomst of handeling. Dat lijkt aantrekkelijk in risicomanagementprocessen die gebaat zijn bij structuur. Echter, zoals hoofdstuk 2 al illustreert, draait SbD juist om het actief en iteratief omgaan met onzekerheden, in plaats van deze te herleiden tot een vereenvoudigd, binair keuzemenu. Het gebruik van beslisbomen in het kader van nieuwe risico's vormt een risico op schijnzekerheid: de indruk dat wanneer een bepaalde tak in de boom wordt gevolgd, het systeem veilig is ontworpen.

Een SbD aanpak vergt meer dan het doorlopen van een beslisboom. Het vraagt om een herhaaldelijke, kritische reflectie op aannames, systeemgrenzen en nieuwe inzichten. In een context met onzekerheden betekent dit dat het ontwerp continu moet worden bijgesteld op basis van voortschrijdend inzicht, stakeholderinput en veranderende omstandigheden. Beslisbomen stimuleren dergelijke iteraties nauwelijks. Ze impliceren lineariteit van systemen, terwijl een SbD-proces juist cyclisch en adaptief moet zijn. Zo is bijvoorbeeld bij waterstofpijpleidingen een statische, lineaire beslisstructuur onvoldoende door de onzekerheden op het gebied van materiaalgedrag (zoals waterstofbrosheid), omgevingsimpact en maatschappelijke acceptatie.

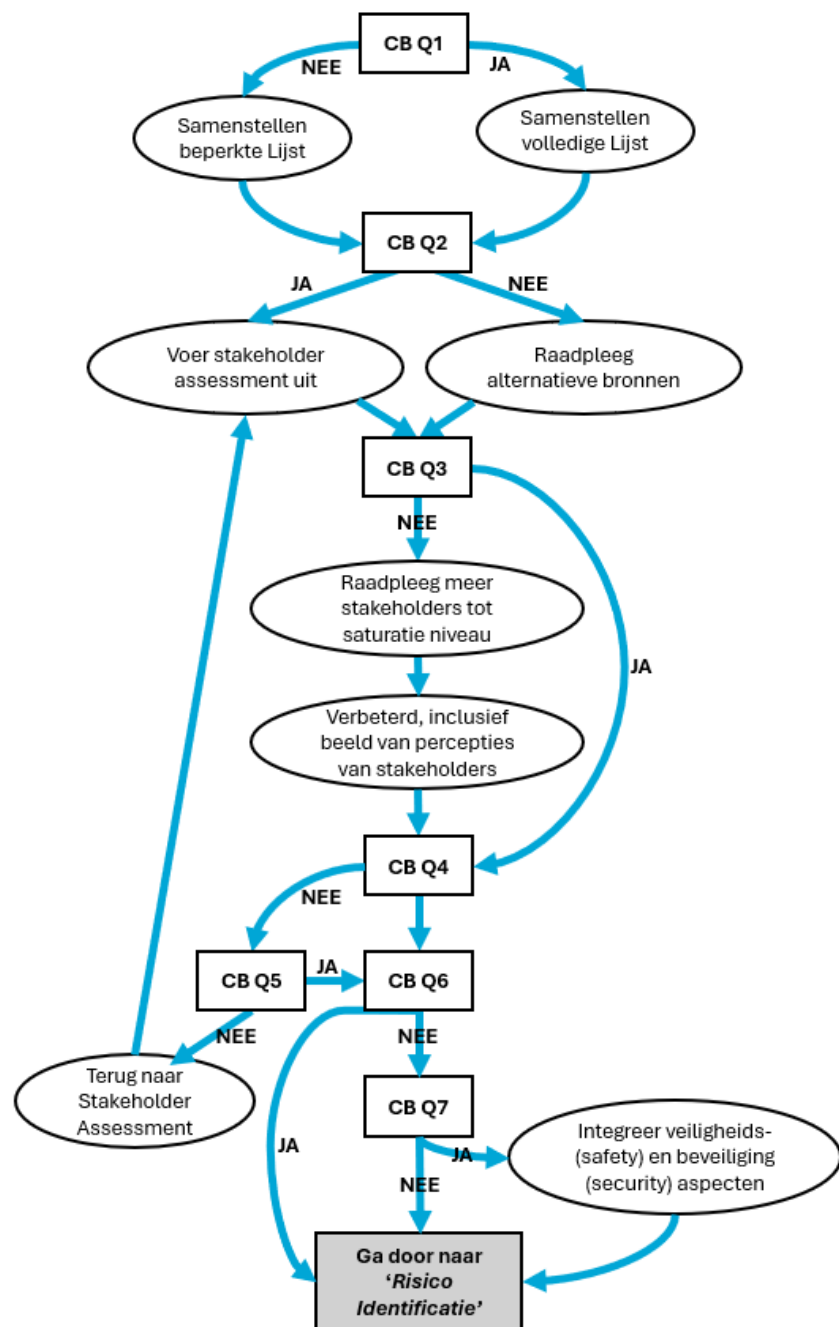
In plaats van het reduceren van SbD tot een beslisstructuur, zou het een proces moeten zijn gericht op continue reflectie en deliberatie. Dit betekent dat ontwerpteam samen met stakeholders onzekerheden opsporen, scenario's doorrekenen en kritisch blijven op aannames. Ook dient een ontwerp ruimte te laten voor aanpassing naarmate de context of kennis verandert. Hiervoor zijn geen vooraf gedefinieerde keuzes nodig, maar open gespreksvormen, zoals stakeholderdialogen en iteratieve scenarioplanning. Deze vormen van co-creatie helpen niet alleen om veiligheidsvraagstukken beter te begrijpen, maar dragen ook bij aan maatschappelijke legitimiteit, een dimensie die vaak ontbreekt in beslisbomen.

Beslisbomen delen een probleem op in vooraf gedefinieerde keuzes. Opkomende risico's laten zich echter moeilijk op voorhand in vaste uitkomsten vastleggen, juist door de onzekerheden en complexiteit van systemen. Door de verschillende interacties die plaatsvinden tussen technologie, mens en de omgeving ontstaan dynamieken die moeilijk voorspelbaar zijn, en zich dus moeilijk laten vastleggen in vooraf gedefinieerde keuzes zoals die in beslisbomen worden voorgesteld.

3.2 Casus: Waterstofpijpleidingen

SbD moet niet gepositioneerd worden als een ‘vaste’ set aan richtlijnen (lees: een checklist). Het terugbrengen van onzekerheden naar beheersbare risico's vraagt juist om een case-by-case benadering die gericht is op continue reflectie en deliberatie. Dat wordt in dit deel geïllustreerd met behulp van een casus over een hypothetische waterstof-pijpleiding in Nederland.

De hypothetische casus. Een nieuw waterstofnetwerk wordt aangelegd om Nederland van duurzame energie te voorzien. De route van deze pijpleiding loopt van een productiehub in de haven van Rotterdam naar een industriecluster in Zuid-Nederland. De waterstof wordt onder hoge druk (meer dan 100 bar) getransporteerd over tientallen kilometers, door stedelijk en landelijk gebied. Het project is technisch complex, politiek gevoelig en maatschappelijk zichtbaar. Bij aanvang van het project wordt een uitgebreide risicoanalyse uitgevoerd, met behulp van gangbare methoden zoals de QRA. De projectontwikkelaar stelt daarnaast beslisbomen op die gebaseerd zijn op SbD-principes met als doel om gestructureerd na te denken over veiligheid in elke fase van het risicomanagementproces. Figuur 2 biedt een illustratie van een beslisboom die is ontworpen voor de fase van contextbepaling, gebaseerd op de richtlijnen gepresenteerd in Sectie 2.1 van dit rapport. De beslisboom en begeleidende vragen benadrukken de identificatie en het betrekken van stakeholders, het identificeren van kwetsbaarheden en bronnen van gevaar, en de integratie van beveiligingsaspecten (security) in de veiligheidsaanpak.



Figuur 2. Beslisboom voor contextbepaling (CB)

Stakeholder identificatie en betrokkenheid

Q1: Is het haalbaar om een uitgebreide, inclusieve lijst op te stellen van alle betrokken partijen? (Individueel, groepen of organisaties die mogelijk worden beïnvloed door de implementatie of uitkomsten van het project, bijv. regelgevende instanties, gemeenschappen, naburige bedrijven).

- **Nee** → Stel een beperkte lijst samen, zo goed als mogelijk → Ga door naar Q2.
- **Ja** → Stel een volledige, inclusieve lijst van betrokken partijen samen → Ga door naar Q2.

Q2: Is het haalbaar om de zorgen en meningen van betrokken partijen op een gestructureerde manier vast te leggen, en deze ook zo te beoordelen via een stakeholder assessment?

- **Nee** → Vertrouw op andere bronnen, bijv. social media, nieuwsbronnen of historische gegevens van vergelijkbare projecten om zorgen te identificeren → Ga door naar Q3.
- **Ja** → Voer een beoordeling uit d.m.v. stakeholder assessment → Ga door naar Q3.

Maatschappelijke acceptatie

Q3: Denkt u dat u maatschappelijke acceptatie heeft bereikt? (Hiermee verwijzen we naar de algehele goedkeuring en acceptatie van betrokkenen, groepen en het publiek, gebaseerd op vertrouwen, ethisch gedrag en waargenomen effecten).

- **Nee** → Betrek meer stakeholders tot geen nieuwe bevindingen → Verbeterde, inclusieve perceptie van stakeholders → Ga door naar Q4.
- **Ja** → Ga door naar Q4.

Kwetsbaarheden en bronnen van gevaar

Q4: Zijn bij Q3 zorgen en kwetsbaarheden geïdentificeerd en actie genomen om (negatieve) gevolgen te verbeteren? (Langetermijneffecten die verder gaan dan enkel naleving van regelgeving zoals zorgen over het milieu, de economie of algemeen welzijn).

- **Nee** → Ga door naar Q5.
- **Ja** → Ga door naar Q6.

Q5: Heeft uw aanpak de identificatie van (aanvullende) kwetsbaarheden vergroot?

- **Nee** → Herzien het assessment omtrent geuite zorgen → Ga terug naar 'Voer stakeholder assessment uit'.
- **Ja** → Ga door naar Q6.

Safety en security integratie

Q6: Heeft u gekeken naar beveiligingsdreigingen (cyber en fysiek), en deze geïntegreerd in uw veiligheidsaanpak?

- **Nee** → Ga door naar Q7.
- **Ja** → **Eindpunt:** Ga door naar de stap 'Risico Identificatie'.

Q7: Is er een mogelijkheid dat opzettelijke aanvallen (cyber of fysiek) resulteren in ongewenste gebeurtenissen die het publiek, het milieu of gerelateerde industrieën treffen (acuut of langere termijn)?

- **Nee** → **Eindpunt:** Ga door naar 'Risico Identificatie'.
- **Ja** → Integreer ook security aspecten → **Eindpunt:** Ga door naar 'Risico Identificatie'.

Elke stap in het proces is verbonden aan ja/nee-vragen en bijbehorende maatregelen. De projectgroep doorloopt de beslisboom, vinkt de relevante beslissingen af, en komt tot de conclusie dat het ontwerp in ieder geval voor de fase 'contextbepaling', 'SbD-proof' is. Toch blijkt tijdens de uitvoering dat het project zich in een complexer socio-technisch systeem bevindt dan verwacht. Wat leert deze casus over de grenzen van besluitvorming op basis van vooraf gedefinieerde keuzepadten in de context van SbD?

De nood aan een dynamische en inclusieve benadering van stakeholders

De beslisboom voor contextbepaling begint bij de vraag of het haalbaar is om een inclusieve lijst van stakeholders op te stellen. Wanneer dat niet lukt, wordt een beperkte lijst geaccepteerd. Hoewel dit een pragmatische benadering lijkt, verhuult deze aanpak een fundamenteel probleem: het proces maakt geen ruimte voor reflectie op wie er *wel* en *niet* wordt meegenomen, en waarom. In plaats van te erkennen dat stakeholderidentificatie altijd een politiek en normatief proces is, wordt het gereduceerd tot een logistieke handeling. Dat kan leiden tot blinde vlekken.

Daarnaast zijn stakeholders geen neutrale, vanzelfsprekende categorieën. Ze worden gedefinieerd door het perspectief van de besluitvormers. Wie invloed kan uitoefenen, wordt sneller als stakeholder erkend dan wie geen directe stem heeft, ondanks mogelijk wezenlijke belangen. Denk aan natuurbelangen zonder directe menselijke vertegenwoordiging, of aan jongeren en toekomstige generaties. Waterstofinfrastructuur heeft een mogelijke impact op de lange termijn, wat onderstreept dat ook belangen van generaties zonder formele vertegenwoordiging in de besluitvorming structureel betrokken moeten worden.

In plaats van een 'zo goed mogelijke' lijst op te stellen, zou een SbD-aanpak moeten starten met een kritische reflectie: Wie beslist wie wel of niet een stakeholder is? Wie missen we in ons beeld van de omgeving? Wie wordt niet gehoord? Welke stemmen worden systematisch onderdrukt of over het hoofd gezien? Hiervoor zijn participatieve methoden nodig, zoals open consultaties, sociale netwerk analyses of zelfs verkennende veldonderzoeken waarin lokale kennis wordt verzameld buiten de formele overlegstructuren om. Daarbij zou in plaats van te streven naar volledigheid als doel op zich, het proces gericht moeten zijn op het maximaliseren van diversiteit aan perspectieven en het voortdurend aanpassen van het stakeholdersbeeld naarmate nieuwe informatie beschikbaar komt. Een dynamische, inclusieve benadering erkent dat context niet iets is wat vooraf vastgesteld wordt, maar een sociaal proces dat mee verandert met het project zelf.

De nood aan het benaderen van maatschappelijke acceptatie als continu en divers proces

Vraag Q3 in de beslisboom luidt: "Denkt u dat u maatschappelijke acceptatie heeft bereikt?" Deze formulering suggereert dat maatschappelijke acceptatie een statische toestand is, een soort eindpunt dat men bereikt en dan kan afvinken. In werkelijkheid is acceptatie juist een voortdurend proces van vertrouwen opbouwen, betrekken, luisteren en aanpassen. Vertrouwen van de samenleving is niet vanzelfsprekend of blijvend; het is kwetsbaar en onderhevig aan veranderingen in perceptie, incidenten elders, of veranderingen in beleid en bestuur. Zo staat waterstof bekend als groene energie, maar na incidenten kan publieke opinie snel kantelen.

Deze benadering kan er ook voor zorgen dat afwezigheid van protest verkeerd wordt geïnterpreteerd als brede instemming. Zo kan het zijn dat er tijdens de planningsfase van een waterstofpijpleiding door een landelijke regio weinig publieke weerstand is. Later kan blijken dat bewoners zich niet konden uitspreken, omdat ze het project te technisch vonden en zich er daardoor simpelweg weinig bij voor konden stellen.

In een SbD-aanpak wordt maatschappelijke acceptatie niet gezien als een momentopname, maar als een relatie die continu aandacht vraagt. Die relatie kan versterkt worden door langdurige betrokkenheid van stakeholders, open communicatie en het daadwerkelijk integreren van hun zorgen in het ontwerp en besluitvorming. In plaats van éénmalige raadplegingen, zou een iteratief model moeten worden gevolgd waarin dialoog centraal staat.

Bovendien kan acceptatie fundamenteel verschillen tussen stakeholders. Zo kan een gemeente geen bezwaren hebben tegen een waterstof-tracé door het grondgebied, terwijl bewoners zorgen hebben over bijvoorbeeld veiligheid, gezondheid of onduidelijkheid over noodprocedures. De beslisboom biedt geen ruimte om met deze verschillen om te gaan of deze als waardevolle signalen van onderliggende spanningen te zien. Een SbD-benadering neemt deze mogelijke verschillen mee.

De nood aan ruimte voor fundamentele herzieningen en kritische reflectie op methodes

De beslisboom bevat enkele terugkoppelmechanismen, zoals in Q5 waar de vraag gesteld wordt of de aanpak de identificatie van kwetsbaarheden vergroot. Wanneer het antwoord nee is, volgt een instructie om de stakeholder assessment te herzien. Dit lijkt op het eerste zicht een vorm van iteratie, maar in werkelijkheid blijft het proces beperkt tot een gesloten kring van vooraf gedefinieerde vragen en stappen. Er is weinig ruimte voor fundamentele herziening van de gehanteerde aannames, of voor het ter discussie stellen van de structuur zelf. Iteratie wordt hier gereduceerd tot herhaling binnen een vast format, niet tot daadwerkelijke heroverweging.

Bovendien beperkt de beslisboom zich tot technische terugkoppeling: zijn er al dan niet bijkomende kwetsbaarheden geïdentificeerd? Waar geen ruimte voor is, is een kritische reflectie op de gekozen methoden om de kwetsbaarheden te identificeren. Zijn de gekozen methoden gevoelig genoeg om sociale of psychologische kwetsbaarheden op te sporen? Zo kan in een wijk waar een waterstof-pijpleiding ondergronds komt te liggen, na verloop van tijd sprake zijn van verhoogde stress en ongerustheid onder bewoners, ondanks technische en theoretische geruststellingen.

Een SbD-benadering moet ruimte bieden voor dergelijke continue reflectie en herijking, waarbij niet alleen bestaande kwetsbaarheden worden beoordeeld, maar ook de geschiktheid van de gebruikte methoden ter discussie kan worden gesteld.

De nood aan een gelijktijdige integratie van safety en security

Het gebruik van beslisbomen zorgt ervoor dat aspecten een 'vaste' positie in een proces hebben. In deze beslisboom komen security aspecten als laatste aan bod (Q6 en Q7), nadat zorgen van stakeholders zijn behandeld en kwetsbaarheden zijn geïdentificeerd. Safety en security zijn echter onlosmakelijk met elkaar verbonden, en dienen continue aandacht te krijgen. Een waterstof lek

door een defect ventiel of door sabotage kunnen dezelfde gevolgen hebben, maar vragen om verschillende preventiestrategieën. Als security pas aan het einde van het beslisproces wordt meegenomen, kan de ruimte ontbreken om ontwerpkeuzes aan te passen aan potentiële dreigingen. Een SbD-benadering pleit voor het *gelijktijdig* integreren van safety en security vanaf het begin. Daarbij gaat het niet alleen om technische beveiliging (firewalls, camera's, toegangscontrole, etc.), maar ook om organisatorische weerbaarheid zoals: Hoe snel kunnen systemen worden afgesloten? Hoe zijn bevoegdheden verdeeld?

4 Conclusie en aanbevelingen

Safe-by-Design als mentaliteit

De analyse van de casus, evenals de bredere reflectie op het gebruik van beslisbomen binnen de context van SbD, maken duidelijk dat het reduceren van SbD tot een stappenplan of beslisstructuur fundamenteel tekort doet aan waar het principe voor staat. In een technologische en maatschappelijke context die steeds complexer, onzekerder en veranderlijker wordt – precies de context waarin de energietransitie zich afspeelt – volstaat het niet meer om veiligheid ‘af te vinken’. Het vergt een fundamentele mentaliteitsverandering: weg van compliance als einddoel, en richting veiligheid als een voortdurend proces van anticiperen, kritisch nadenken, afstemmen en iteratie.

De toepassing van lineaire methodes zoals beslisbomen reduceren onzekerheid tot overzichtelijke keuzemomenten, terwijl SbD juist vraagt om het erkennen en exploreren van onzekerheid. Beslisbomen zijn niet geschikt om maatschappelijke dynamieken mee te nemen, en schieten tekort in het adresseren van systemische interacties. Een SbD-aanpak moet dus verder gaan dan een beslisboom, en begint voor de contextbepaling met bijvoorbeeld een open risicodialog en iteratieve ontwerpcycli waarin aannames telkens opnieuw worden getoetst, en waarin ruimte is voor aanpassingen. In zo'n aanpak worden systeemgrenzen niet vooraf vastgelegd in een schema, maar ontstaan ze gaandeweg door interactie met stakeholders, en op basis van voortschrijdend inzicht.

Onzekerheden adresseren in elke stap van de risicomanagementcyclus door middel van Safe-by-Design principes

Huidige methoden voor veiligheidsmanagement in de chemische industrie richten zich voornamelijk op het verlagen van risico's, bijvoorbeeld door het toepassen van de inherente veiligheidsprincipes (ISPs), en zijn dus vooral toegespitst op de 'risicobehandeling'-fase in risicomanagement. Het is echter nodig om in elke stap van de risicomanagementcyclus mogelijke onzekerheden te adresseren. Verschillende SbD-principes kunnen hiervoor ingeschakeld worden.

Een SbD-aanpak vraagt om het **meenemen van bredere maatschappelijke en langetermijn risico's**, in plaats van louter te kijken naar directe en acute risico's. Dit omvat onder meer milieu-impact, economische impact, welzijn van de bevolking, en mogelijke impact op toekomstige generaties. Het expliciet meenemen van deze risico's draagt bij aan een meer realistische inschatting van risico's in een context van onzekerheid en complexiteit.

De toepassing van SbD vereist een **levenscyclusbenadering**, waarbij veiligheid wordt benaderd vanuit de volledige levenscyclus van een systeem, van ontwerp en constructie tot onderhoud en ontmanteling. Hierdoor krijgt men inzicht in langetermijn risico's en kan men proactief maatregelen treffen die ook in latere fases veiligheid garanderen. Deze aanpak draagt bij aan de directe veiligheid, en aan de duurzaamheid op lange termijn.

SbD stelt **stakeholderparticipatie** vanaf het begin centraal. Het betrekken van stakeholders, zoals omwonenden en lokale overheden, zorgt ervoor dat hun maatschappelijke zorgen en lokale kennis worden gehoord. Dit draagt bij aan draagvlak en maatschappelijke acceptatie. Bovendien leidt het ook tot betere risicobeheersing, aangezien stakeholderparticipatie voor essentiële input kan zorgen om blinde vlekken en nieuwe onzekerheden te detecteren. Overheden spelen hierin een faciliterende rol door participatie te stimuleren en drempels ervoor te verlagen.

Een belangrijk SbD-principe is het **voorzorgsprincipe**. In plaats van te redeneren “als er geen bewijs van gevaar is, nemen we aan dat het veilig is”, gaat men uit van: in situaties van onzekerheid neemt men aan dat er *wel* een ernstig gevaar zou kunnen zijn en worden scenario's daarop afgestemd en verder onderzocht. Dit betekent dat men niet enkel kijkt naar meest waarschijnlijke scenario's, maar ook naar extremere, zij het minder waarschijnlijke, scenario's. Bij nieuwe systemen (waar weinig ervaringscijfers voorhanden zijn) moeten deze worst-case scenario's worden meegenomen, waarbij de nadruk ligt op de *gevolgen* in plaats van op de (onzekere) kans. Ook bij het inschatten van risico's kan het voorzorgsprincipe worden gehanteerd door extra veiligheidsmarges in te bouwen in toelaatbaarheidsgrenzen wanneer er onzekerheid is over data. Het voorzorgsprincipe spoort bedrijven aan om uit te gaan van strengere, meer conservatieve criteria, tot er meer zekerheid (ervaring met en data over het gebruik) is. Daarbij worden er hogere veiligheidsniveaus nagestreefd dan strikt juridisch vereist is. Overheidsbeleid kan dit stimuleren door beleidskaders en vergunningen zo in te richten dat ze ruimte bieden – of zelfs aansporen – om verder te gaan dan de minimumvereisten bij nieuwe risico's gekenmerkt door onzekerheden.

SbD stelt **systeemdenken** voorop, waarbij men verder kijkt dan de grenzen van de eigen installatie en anticipeert op kettingreacties en wisselwerkingen binnen het grotere systeem. Zo spoort SbD experts aan om interacties expliciet te identificeren en mee te nemen, zoals samengestelde gevaren, waarbij, met name in complexe systemen, meerdere gevaren zich gelijktijdig kunnen voordoen en een versterkend effect kunnen hebben op elkaar. Ook neemt systeemdenken de complexiteit van moderne sociaal-technische systemen in beschouwing, met aandacht voor de interactie tussen technische factoren, mensen en de omgeving.

Binnen een SbD-benadering is **samenwerking** essentieel. Het betrekken van diverse disciplines (technisch, milieu, sociaal) minimaliseert de kans dat blinde vlekken blijven bestaan. Ook kan samenwerking de objectiviteit vergroten door meerdere experts onafhankelijk een oordeel te laten vormen. Zo kan voorkomen worden dat persoonlijke inschattingen te veel gewicht krijgen. Overheden kunnen deze samenwerking actief ondersteunen: enerzijds door het verspreiden van kennis over de beste beschikbare technologieën voor onder meer inspectie en monitoring, anderzijds door het stimuleren van kennisdeling binnen de sector. Dit kan bijvoorbeeld via platforms voor het uitwisselen van best practices en lessons learned.

Tot slot vraagt SbD een **iteratieve en dynamische benadering**. Risico's zijn voortdurend in beweging waardoor veiligheidsbeheer een iteratief en dynamisch proces moet zijn. Nieuwe informatie, bijvoorbeeld van inspecties, near-misses of veranderende bedrijfsomstandigheden, wordt steeds teruggekoppeld, om zo risico's continu te actualiseren.

Inspectieprogramma's hebben een centrale rol binnen deze iteratieve en dynamische benadering. Door actuele inspectiegegevens te vergelijken met ontwerpmodellen kunnen

aannames worden getoetst en waar nodig bijgesteld. Dit zorgt voor een verkleining van de onzekerheidsmarges. Bij inspectietechnieken is een nulmeting essentieel, die als referentie dient om afwijkingen systematisch op te sporen. Pas bij aantoonbare stabiliteit, i.e., gedurende een langere periode geen afwijkingen ten opzichte van de nulmeting (wat wijst op meer zekerheid), kunnen er langere inspectie-intervallen worden toegestaan.

In de context van innovatie kan er dus niet vanzelfsprekend worden aangenomen dat risico's beheerst zijn; onzekerheid is een inherent onderdeel van het proces. Besluitvormers zouden daarom een specifiek **plan** moeten opstellen om SbD-principes in te bedden in elke stap van de risicomanagementcyclus. Dit betekent onder meer het proactief vastleggen van striktere onderhoudsregimes en gerichte inspecties om afwijkingen vroegtijdig te detecteren en onzekerheden te reduceren. Een dergelijk plan moet worden opgesteld door personen met de juiste technische, operationele en veiligheidskundige expertise.

Het toepassen van deze SbD-principes in elke stap van de risicomanagementcyclus kan ervoor zorgen dat onzekerheden worden terug gebracht naar beheersbare risico's. Dit biedt verschillende tastbare voordelen. Wanneer veiligheid als integraal onderdeel van ontwerp en beheer wordt beschouwd, neemt de betrouwbaarheid en beschikbaarheid van installaties toe. Ongeplande stilstanden door lekkages of faalmechanismen worden voorkomen, en de kans op kostbare incidenten daalt. Bovendien draagt een proactieve SbD-aanpak bij aan het vertrouwen van burgers, bestuurders en andere stakeholders. Imagoschade, maatschappelijke weerstand en langdurige vergunningstrajecten kunnen worden beperkt als een bedrijf aantoon niet alleen wettelijk correct te handelen, maar óók maatschappelijk verantwoord. SbD maakt daarmee de stap van 'veilig genoeg volgens de norm' naar 'veilig omdat het duurzaam en verantwoord is'.

Referenties

- Amendola, A., S. Contini, & Ziomas, I. (1992). Uncertainties in chemical risk assessment: results of a European benchmark exercise. *Journal of Hazardous Materials*, 29(3): 347-363.
- Amyotte, P. R., Goraya, A. U., Hendershot, D. C., & Khan, F. I. (2007). Incorporation of inherent safety principles in process safety management. *Process safety progress*, 26(4): 333-346.
- API (2021). API RP 754: Process Safety Performance Indicators for the Refining and Petrochemical Industries. American Petroleum Institute.
- Aven, T. & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of risk research*, 12(1): 1-11.
- BP (2007). Investigation Report Report No. 2005-04-I-TX Refinery Explosion And Fire. Texas City.
- Broughton, E. (2005). The Bhopal disaster and its aftermath: a review. *Environmental Health*, 4: 1-6.
- Cameron, I., Mannan, S., Németh, E., Park, S., Pasman, H., Rogers, W., & Seligmann, B. (2017). Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better?. *Process Safety and Environmental Protection*, 110: 53-70.
- Casal, A., & H. Olsen (2016). Operational risks in QRAs. *Chemical Engineering Transactions*, 48: 589-594.
- Decherney, S.A.R. & John, P. (2024). Keystone pipeline. Encyclopedia Britannica.
- HM Stationery Office (1966). Tribunal Appointed to Inquire into the Disaster at Aberfan on October 21st, H.E. Edmund-Davies, and B. Edmund-Davies, *Report of the Tribunal Appointed to Inquire into the Disaster at Aberfan October 21st, 1966*.
- ISO (2018). Risk Management (ISO Standard No. 31000).
- Jarvis, R. & Goddard, A. (2017). An analysis of common causes of major losses in the onshore oil, gas & petrochemical industries. *Loss prevention bulletin*, 255.
- Lauridsen, K., Kozine, I., Markert, F., Amendola, A., Christou, M., & Fiori, M. (2002). Assessment of uncertainties in risk analysis of chemical establishments. The ASSURANCE project. Final summary report.
- Leveson, N.G. (2016). Engineering a safer world: Systems thinking applied to safety. The MIT Press.
- MARSH (2018). The 100 largest losses 1978–2017 – Large property damage losses in the hydrocarbon industry. *Marsh Report*.
- National Commission (2011). BP Deepwater Horizon Oil Spill Offshore Dril, Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling: Report to the President, January 2011.
- National Transportation Safety Board (2023). Norfolk Southern Railway Derailment and Hazardous Materials Release. *Railroad Investigation Report RIR 24-05*. East Palestine, Ohio. Available via <https://www.nts.gov/investigations/AccidentReports/Reports/RIR2405%20CORRECTED.pdf>.
- Ninen, J. & van Nunen, K. (2025). Safetywashing in de bouwsector: Imago versus werkelijkheid. *Veiligheidsnieuws*, 227: 64-66.

- Salvi, O. & Debray, B. (2006). A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive. *Journal of hazardous materials*, 130(3): 187-199.
- Schmitt, T.M. (2018). (Why) did Desertec fail? An interim analysis of a large-scale renewable energy infrastructure project from a Social Studies of Technology perspective. *Local Environment*, 23(7): 747-776.
- Tokyo Metropolis (2012). National Diet of Japan, The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission: Executive Summary: National Diet of Japan.
- US New (2018). BP Takes \$1.7 Billion Charge on Deepwater Horizon; Costs Now Top \$65B. 2018 20-11-2024; Available from: <https://www.usnews.com/news/national-news/articles/2018-01-16/bp-takes-17-billion-charge-on-deepwater-horizon-costs-now-top-65b>.
- Vrouwenvelder, A., Lovegrove, R., Holicky, M., Tanner, P. & Cansius, G. (2001). Risk assessment and risk communication in civil engineering. CIB REPORT.
- Wijnker, J. & van der Velde, S. (2020). *Verkenning vernieuwde toezicht*. Stuurgroep Duurzame Veiligheid 2030. Available from: <https://www.rijksoverheid.nl/documenten/rapporten/2020/10/15/verkenning-vernieuwend-toezicht>.
- Willsher, K. (2018). France abandons plan for €580m airport and orders squatters off site, in The Guardian. Available from: <https://www.theguardian.com/world/2018/jan/17/france-abandons-plan-for-580m-airport-in-west-of-country>.

