

## (Petro)chemische clusters en veiligheid:

Een clusterspecifieke rangschikking van veiligheidsparameters

Versie 2 onderzoeksrapport

Augustus 2022



#### Opdrachtgever

Deze studie werd uitgevoerd in opdracht van het Ministerie van Infrastructuur en Waterstaat en maakt onderdeel uit van het bredere clusterbeleid binnen de (petro)chemische industrie (zie <u>Appendix</u>).

#### Uitvoerder

Deze studie werd uitgevoerd door de Safety & Security Science Group, TU Delft.

Drs. Karolien van Nunen Prof. dr. Genserik Reniers Prof. dr. Ming Yang Dr. Chao Chen Drs. Shuaigi Yuan

De ontwikkeling van de tool kwam tot stand met behulp van ondersteuning door het Digital Competence Centre, TU Delft.



#### Versie onderzoeksrapport

Versie 2 Augustus 2022

## (Petro)chemische clusters en veiligheid:

## Een clusterspecifieke rangschikking van veiligheidsparameters

## Inhoudstafel

	Samenvatting	4
1.	Aanleiding voor de studie	6
2.	Doel van de studie	8
3.	Gebruikers van de tool	11
4.	Inhoud van de tool	12
5.	Input voor de veiligheidsparameters & specifieke veiligheidsinitiatieven	13
6.	De tool: input – proces – output	13
7.	Uitleg van de veiligheidsparameters & specifieke veiligheidsinitiatieven	17
	7.1. Proactieve veiligheidsparameters en -initiatieven	18
	Uitwisselen van veiligheidsinformatie	18
	Beoordelen & beheersen van onderlinge risico's op clusterniveau	20
	Leren van elkaar	22
	Uniformiteit en standaardisatie van veiligheid	23
	De cluster van bedrijven als collectief	25
	7.2. Reactieve veiligheidsparameters en -initiatieven	27
	Gedeelde calamiteitenuitrusting en -faciliteiten	27
	Gezamenlijke noodorganisatie en crisiscommunicatie	29
8.	Een optimaal gebruik van de tool	31
	8.1. Factoren die bijdragen aan een optimaal gebruik	31
	8.2. Uitdagingen en aandachtspunten	32
9.	Referentielijst	33
	Appendix	35

### Samenvatting

Kenmerkend voor bedrijven die in een cluster gelegen zijn, zijn de onderlinge risico's waarbij de risico's van één bedrijf aanleiding kunnen geven tot nieuwe risico's bij een aangrenzend of een nabijgelegen bedrijf. Daarbij gaat het om de mogelijkheid op (a) domino-effecten, (b) keteneffecten, of (c) impact (letsel/schade) ten gevolge van een incident bij een buurbedrijf. Voor (petro)chemische bedrijven die geografisch nabij andere bedrijven liggen, is het bijgevolg noodzakelijk om (proces)veiligheid niet aan te pakken als een geïsoleerd bedrijf, maar in samenwerking met de nabijgelegen bedrijven, om zo ook de onderlinge risico's optimaal te beheersen. Samenwerking tussen bedrijven wordt dus gezien als dé sleutel tot het doelmatig aanpakken van onderlinge risico's.

Deze studie heeft als doel om deze samenwerking tussen geclusterde bedrijven te faciliteren, meer concreet te maken, en te optimaliseren. Om dit te bewerkstelligen is een praktische tool ontwikkeld. Een (sub)cluster van (petro)chemische bedrijven kan de tool gezamenlijk gebruiken om op een optimale en onderbouwde manier samenwerkingsinitiatieven op te zetten om de onderlinge risico's te beheersen, en om zo de (cluster)veiligheid te verhogen. Ten minste twee bedrijven die geografisch dicht bij elkaar gevestigd zijn, kunnen aan de slag gaan met de tool. Minstens één bedrijf heeft hierbij een BRZO-status. Verder is de tool bruikbaar voor zowel BRZO-bedrijven met en zonder een domino-effect aanwijzing, voor bedrijven die (net) onder de BRZO-drempel vallen, en voor niet-(petro)chemische bedrijven.

In de praktische tool (in de vorm van een online Excel-file) zijn verschillende algemene veiligheidsparameters opgenomen en daarbij horend meer specifieke veiligheidsinitiatieven. Hierbij gaat het om initiatieven die bedrijven *samen* kunnen opzetten om de onderlinge risico's te beheren en te beheersen. In de tool ligt de focus op zowel proactieve als reactieve veiligheidsparameters. Er zijn vijf proactieve veiligheidsparameters geformuleerd waarbij de focus ligt op het voorkomen van ongewenste gebeurtenissen:

- Het uitwisselen van veiligheidsinformatie
- Het beoordelen en beheersen van onderlinge risico's op clusterniveau
- Leren van elkaar
- Uniformiteit en standaardisatie van veiligheid
- De cluster van bedrijven als collectief

Er zijn twee reactieve veiligheidsparameters geformuleerd waarbij de focus ligt op het mitigeren van de gevolgen als er toch een ongewenste gebeurtenis plaatsvindt:

- Gedeelde calamiteitenuitrusting en -faciliteiten
- Gezamenlijke noodorganisatie en crisiscommunicatie

Deze veiligheidsparameters zijn in de tool uiteengezet in verschillende meer specifieke veiligheidsinitiatieven. De (sub)cluster van bedrijven die aan de slag gaat met de tool zal voor alle specifieke veiligheidsinitiatieven gezamenlijk de huidige prestatie (stap 1) en de

haalbaarheid scoren (stap 2). In stap 1 scoren de bedrijven de huidige prestatie, gaande van een optimale prestatie tot een suboptimale prestatie of de afwezigheid van samenwerking wat betreft het te scoren veiligheidsinitiatief. In stap 2 scoren de bedrijven de haalbaarheid van de veiligheidsinitiatieven. Aan de hand van meerdere criteria (zoals onder meer risicoreductie potentieel, kosten, concurrentiegevoeligheid, en invloed van het (moeder)bedrijf) wordt er door de bedrijven een inschatting gemaakt van de haalbaarheid van de veiligheidsinitiatieven.

Vervolgens worden op basis van een achterliggend algoritme de veiligheidsinitiatieven automatisch gerangschikt naargelang potentiële veiligheidswinst. Men krijgt dus als uitkomst veiligheidsparameters, prioriteitsstelling van waarbii de hooast veiligheidsparameters de meeste veiligheidswinst kunnen opleveren voor een bepaalde cluster. Door het toekennen van de huidige prestatie en de haalbaarheid houdt de rangschikking rekening met de reeds aanwezige (geïnstitutionaliseerde) veiligheidsparameters, en met de specifieke context van een bepaalde cluster.

De tool is uniek in die zin dat er gefocust wordt op *gezamenlijkheid*. De prioriteitsstelling van de veiligheidsparameters zal toelaten om op een onderbouwde en optimale manier te bepalen waarop men als (sub)cluster van bedrijven *samen* kan inzetten om tot veiligheidswinst te komen m.b.t. onderlinge risico's. De tool kan gezien worden als het *startpunt* om een hoger gezamenlijk veiligheidsniveau te bereiken, waarbij de uitkomst van de tool het vertrekpunt kan zijn om concrete veiligheidsinitiatieven (verder) vorm te geven.

De tool focust op het aanpakken van onderlinge risico's, waardoor de veiligheid van de gehele cluster geoptimaliseerd wordt. Hierbij zal ook de omgevingsveiligheid geoptimaliseerd worden, aangezien het gehele gebied waarin de geclusterde bedrijven functioneren veiliger wordt als de onderlinge risico's beter beheerst worden.

De praktische tool (in de vorm van een online Excel-file) is terug te vinden via volgende link:

https://clustersafety.github.io/Rangschikking\_veiligheidsparameters/

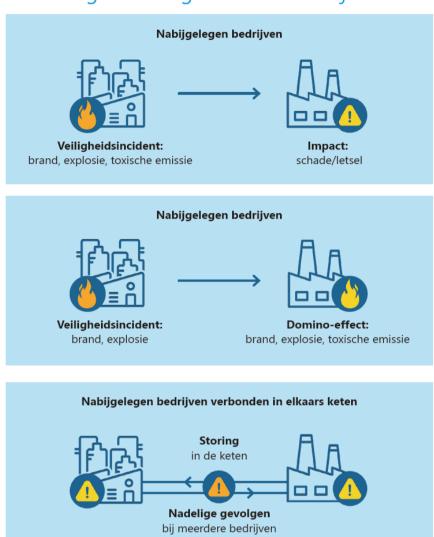
## 1. Aanleiding voor de studie

In 2018-2019 voerde Universiteit Antwerpen en TU Delft een verkennende studie uit om in kaart te brengen welke parameters een invloed hebben op de veiligheid van (petro)chemische clusters, en in welke mate deze parameters aanwezig zijn bij alleenstaande (petro)chemische bedrijven (van Nunen et al., 2019; 2020). De huidige studie bouwt verder op de veiligheidsparameters die in deze verkennende studie werden geïdentificeerd. In de huidige studie wordt de tweedeling geclusterde-alleenstaande bedrijven losgelaten, en wordt er enkel op veiligheidsparameters binnen *geclusterde* (petro)chemische bedrijven gefocust.

Bedrijven die in een cluster gelegen zijn hebben, net zoals bij alleenstaande bedrijven, veiligheidsrisico's waarbij de gevolgen van een veiligheidsincident beperkt blijven tot binnen de grenzen van het bedrijfsterrein. Bij geclusterde (petro)chemische bedrijven zijn bijkomend **onderlinge risico's** aanwezig waarbij de risico's van één bedrijf aanleiding kunnen geven tot nieuwe risico's bij een nabijgelegen bedrijf (zie Figuur 1):

- Een veiligheidsincident (brand, explosie, toxische emissie) in één bedrijf kan aanleiding geven tot een impact (materiële schade en/of menselijk letsel) bij een aangrenzend of nabijgelegen bedrijf.
- Ook is er de mogelijkheid tot domino-effecten, waarbij een ongevalsscenario (brand, explosie) in één bedrijf een ongevalsscenario (brand, explosie, toxische emissie) kan veroorzaken binnen een aangrenzend of nabijgelegen bedrijf. De gevolgen van een domino-ongeval (in termen van schade en letsel) zijn vaak groter dan een enkelvoudig ongevalsscenario door de opeenvolgende gebeurtenissen (Swuste et al., 2018; 2019).
- Ook kunnen nabijgelegen bedrijven gebruik maken van elkaars productstromen of nutsvoorzieningen (utilities) delen, en zo verbonden zijn in elkaars keten. Een (onverwachte) verandering of storing in deze keten heeft bijgevolg een potentieel nadelige impact op meerdere bedrijven.

Figuur 1
Onderlinge risico's geclusterde bedrijven



Aangezien er steeds meerdere bedrijven betrokken zijn bij deze onderlinge risico's is het doelmatig beheren en beheersen ervan enkel mogelijk door samen te werken. Voor (petro)chemische bedrijven die geografisch nabij andere bedrijven liggen, is het bijgevolg noodzakelijk om (proces)veiligheid niet aan te pakken als een geïsoleerd bedrijf, maar in samenwerking met de nabijgelegen bedrijven, om zo ook de onderlinge risico's optimaal te beheren en te beheersen.

#### 2. Doel van de studie

'Samenwerking' wordt gezien als dé sleutel tot het doelmatig beheren en beheersen van onderlinge risico's. Het gaat echter om een zeer ruim begrip dat kan gaan van het meedelen van informatie (éénrichtingsverkeer) tot een meer intensieve samenwerking zoals het gezamenlijk investeren in veiligheidsinitiatieven. **Deze studie heeft als doel om deze samenwerking tussen geclusterde bedrijven te faciliteren, meer concreet te maken, en te optimaliseren** (zie Figuur 2).

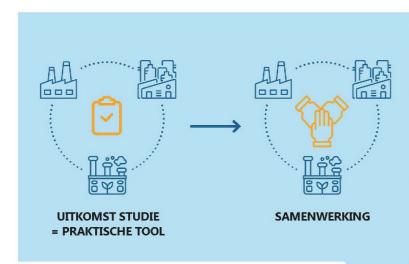
- Faciliteren: de tool faciliteert de samenwerking door het aanreiken van een gestandaardiseerde werkwijze die op een integrale manier veiligheidsparameters en specifieke veiligheidsinitiatieven includeert.
- *Concretiseren*: de uitkomst van de tool is een rangschikking van veiligheidsparameters en specifieke veiligheidsinitiatieven waarop ingezet kan worden om de meeste veiligheidswinst te bekomen voor een bepaalde cluster; het levert bijgevolg een concreet startpunt op om samenwerkingsverbanden op te zetten.
- Optimaliseren: de samenwerking wordt geoptimaliseerd omdat men zich gaat richten op die veiligheidsparameters waar voor een specifieke cluster het meeste verbeterpotentieel ligt wat betreft veiligheid.

De uitkomst van deze studie is een praktische tool waarmee bedrijven die zich in een (sub)cluster bevinden gezamenlijk aan de slag kunnen gaan. In deze tool zijn verschillende veiligheidsparameters opgenomen en daarbij horende meer specifieke veiligheidsinitiatieven (zie deel 4 inhoud van de tool). Geclusterde bedrijven kunnen gezamenlijk deze veiligheidsinitiatieven scoren (naargelang huidige prestatie (performance) en haalbaarheid voor de cluster in kwestie), waarna men op basis van een algoritme een prioriteitsstelling of rangschikking krijgt van veiligheidsparameters waarop ingezet kan worden om de meeste veiligheidswinst op te leveren voor de cluster waar de bedrijven deel van uitmaken. De prioriteitsstelling van de veiligheidsparameters zal dus toelaten om op een onderbouwde en optimale manier te bepalen waarop men als (sub)cluster van bedrijven prioritair kan inzetten om tot een veiligheidswinst te komen m.b.t. onderlinge risico's in een (petro)chemische cluster.

Het doel van deze studie is om geclusterde bedrijven een tool aan te reiken om op een optimale en onderbouwde manier samenwerkingsinitiatieven op te zetten om de onderlinge risico's te beheersen en de (cluster)veiligheid te verhogen. Door het gebruik van de tool door een cluster zal openheid, transparantie en dialoog (verder) op gang komen. In die zin zal het gezamenlijk invullen van de tool ook bijdragen tot (veiligheids)winst. Natuurlijk zal het louter gebruiken/invullen van deze tool er niet voor zorgen dat veiligheid geoptimaliseerd wordt, maar wel wat men met de uitkomst van deze tool doet. Het is als het ware het *startpunt* om een hoger gezamenlijk veiligheidsniveau (en onrechtstreeks bij uitbreiding een hoger individueel veiligheidsniveau) te bereiken. De tool zal bijgevolg een *middel* zijn om bij te dragen aan het hogere doel:

- Men gaat als bedrijf de **eigen veiligheid** optimaliseren: door het gebruik van de tool wordt er niet alleen een samenwerkende, maar ook een lerende gemeenschap gecreëerd. Men leert onder andere hoe andere bedrijven omgaan met gelijkaardige risico's of processen, bijvoorbeeld op het vlak van onderhoud van installaties.
- Optimaliseren **veiligheid van de gehele cluster**: de tool focust op het aanpakken van onderlinge risico's. Bedrijven zullen onderlinge risico's (beter) leren kennen, en belangrijke verbeterpunten identificeren.
- Optimaliseren omgevingsveiligheid: de mogelijke nadelige effecten van onderlinge risico's blijven natuurlijk niet beperkt tot de terreingrenzen van de clusterbedrijven. Onderlinge risico's impliceren ook mogelijke nadelige gevolgen voor de omgeving. Het aanpakken van onderlinge risico's impliceert bijgevolg veiligheidswinst voor de omgeving van het clustergebied. Zo wordt het gehele gebied waarin de geclusterde bedrijven functioneren veiliger als de onderlinge risico's beter beheerst worden.
- Optimaliseren veiligheidsperceptie: ook de perceptie die de omgeving heeft van de veiligheid van de cluster kan positief beïnvloed worden als geclusterde bedrijven de tool gebruiken. De tool zet immers aan tot een samenwerkende gemeenschap, waarbij men als cluster samen, als één geheel werkt aan het optimaliseren van veiligheid. Zo kan aan de omgeving (of andere relevante stakeholders) getoond worden dat veiligheid van de cluster als belangrijk wordt gezien. Aangezien de omgeving een cluster van bedrijven vaak ziet als één geheel, en niet als afzonderlijke bedrijven, kan men door samen te werken geloofwaardigheid en vertrouwen creëren.

Figuur 2
Doel van de studie



- Samenwerking faciliteren: de tool faciliteert de samenwerking door het aanreiken van een gestandaardiseerde werkwijze die op een integrale manier veiligheidsparameters includeert.
- Samenwerking concretiseren: de uitkomst van de tool is een rangschikking van veiligheidsparameters waarop ingezet kan worden om de meeste veiligheidswinst te bekomen voor een bepaalde cluster; het levert bijgevolg een concreet startpunt op om samenwerkingsverbanden op te zetten.
- Samenwerking optimaliseren: de samenwerking wordt geoptimaliseerd omdat men zich gaat richten op die veiligheidsparameters waar voor een specifieke cluster het meeste verbeterpotentieel ligt wat betreft veiligheid.

## Hoger doel van de studie



#### 3. Gebruikers van de tool

De ontwikkeling van de tool is uniek in die zin dat er gefocust wordt op *gezamenlijkheid*. Welke initiatieven kan men *samen* opzetten om de onderlinge risico's doelmatig te beheren en te beheersen? Een voorwaarde om de tool te gebruiken is bijgevolg dat **ten minste twee bedrijven** zich engageren om aan de slag te gaan met de tool, waarvan er minstens één bedrijf een BRZO-status heeft.

Aangezien er gefocust wordt op de onderlinge risico's is een volgende voorwaarde dat de (sub)cluster van bedrijven die de tool gebruikt **geografisch dicht bij elkaar gevestigd zijn**.

Verder is het gebruik van de tool mogelijk voor:

- Bedrijven met of zonder een BRZO-status: BRZO-bedrijven, maar ook risicorelevante bedrijven (bedrijven die (net) onder de BRZO-drempel vallen) en niet-(petro)chemische bedrijven kunnen de tool samen gebruiken
- Bedrijven met en zonder domino-effect aanwijzing
- Bedrijven die verbonden zijn in elkaars keten en bedrijven die niet in elkaars keten functioneren
- Bedrijven die reeds een intensieve relatie onderhouden, bedrijven waartussen momenteel geen enkele vorm van samenwerking bestaat, en het hele spectrum daartussen
- Bedrijven die al dan niet zijn omgeven door hekwerk: bedrijven die gevestigd zijn op een afgebakend bedrijventerrein, maar ook bedrijven die niet omgeven zijn door een gemeenschappelijk hekwerk kunnen de tool gebruiken. Ook een combinatie is mogelijk, waarbij bedrijven die op een afgebakend terrein liggen de tool gebruiken samen met die bedrijven die buiten het hekwerk gevestigd zijn.

De personen die binnen de bedrijven aan de slag gaan met het invullen van de tool moeten accurate en volledige kennis hebben over de veiligheidsparameters binnen het eigen bedrijf (en makkelijk toegang hebben tot deze kennis), en deze personen moeten op een objectieve manier de veiligheidsparameters kunnen scoren. Vaak zullen dit de safety managers zijn, eventueel bijgestaan door operationele managers.

In eerste instantie is het een tool voor de bedrijven, maar optioneel kunnen ook **andere relevante stakeholders** betrokken worden als meewerkende partner. Dit kan nuttig zijn als er tussen de bedrijven zelf onduidelijkheid is over een bepaalde veiligheidsparameter, of als de mening verschilt tussen de bedrijven over de prestatiescore of haalbaarheidsscore.

- Stakeholders die deel uitmaken van de cluster, zoals overkoepelende clusterorganen, havenbedrijf, spoorwegbedrijf, ...
- Stakeholders die een rol spelen in het beheersen van de veiligheid van de bedrijven die de tool gebruiken: toezichthouder, provincie, gemeente, veiligheidsregio, omgevingsdienst, VNCI, VNPI, ...

#### 4. Inhoud van de tool

De tool is opgebouwd uit verschillende veiligheidsparameters en specifieke veiligheidsinitiatieven, die in de tool gescoord worden op prestatie en haalbaarheid.

Het reeds uitgevoerde verkennende onderzoek heeft duidelijk gemaakt dat er nog verschillende (op dit moment te weinig benutte) veiligheidsparameters zijn waarop men als (sub)cluster gezamenlijk kan inzetten (van Nunen et al., 2019; 2020). Zo worden veiligheidsinitiatieven binnen een cluster voornamelijk door individuele bedrijven genomen, zeker wat betreft proactieve veiligheidsparameters. Bestaande veiligheidsinitiatieven die binnen een (sub)cluster gezamenlijk worden genomen, focussen op dit moment voornamelijk op het mitigeren van ongewenste gebeurtenissen, zoals het inrichten van een gezamenlijke bedrijfsbrandweer of een gezamenlijk noodplan. In de tool ligt de focus op zowel **proactieve** als **reactieve veiligheidsparameters**. Zo zijn er proactieve veiligheidsparameters geïncludeerd waarbij de focus ligt op het voorkomen van ongewenste gebeurtenissen (linkerkant van de bow-tie), en er zijn reactieve veiligheidsparameters geïncludeerd die focussen op het mitigeren van ongewenste gebeurtenissen (rechterkant van de bow-tie).

De tool is uniek in die zin dat er gefocust wordt op *gezamenlijkheid*. Waarop kan men als (sub)cluster van bedrijven *samen* inzetten om tot een hoger niveau van veiligheid te komen? In de tool zijn bijgevolg enkel veiligheidsparameters geïncludeerd die focussen op deze **gezamenlijkheid**. Als cluster van bedrijven kan men bijvoorbeeld *gezamenlijk* risicoanalyses uitvoeren. Het gaat dus niet om veiligheidsmaatregelen die een enkel bedrijf kan nemen om de eigen (proces)veiligheid te beheersen, met mogelijks bijkomende positieve effecten op de veiligheid van aangrenzende of nabijgelegen bedrijven.

De meer algemene veiligheidsparameters kunnen opgesplitst worden in meer **specifieke veiligheidsinitiatieven**. Het gaat om initiatieven die bedrijven samen kunnen nemen om de onderlinge risico's te beheren en te beheersen. Zo kan bijvoorbeeld de algemene veiligheidsparameter 'De cluster van bedrijven als collectief' opgedeeld worden in de meer specifieke initiatieven 'Gemeenschappelijke veiligheidsvisie', 'Overkoepelende clustercoalitie', 'Gezamenlijk budget voor veiligheidsinitiatieven', 'Gezamenlijke communicatie naar/met de omwonenden', en 'Cultuur van aanspreekbaarheid'.

# 5. Input voor de veiligheidsparameters & specifieke veiligheidsinitiatieven

Voor het opstellen van de lijst van relevante veiligheidsparameters en specifieke veiligheidsinitiatieven wordt de volgende input gebruikt:

- Deze studie maakt gebruik van de data die werd verzameld in de eerder uitgevoerde verkennende studie naar veiligheidsparameters (van Nunen et al., 2019). Gedurende deze verkennende studie werd data verzameld op basis van 70 interviews met experten (bedrijven, veiligheidsregio's, omgevingsdiensten, provincies, havenbedrijven, VNCI, VNPI,...). Ook werd een vragenlijst afgenomen bij de inspectiediensten BRZO+. Deze onderzoeksdata is het vertrekpunt voor het opstellen van de lijst met veiligheidsparameters en specifieke veiligheidsinitiatieven.
- Aanvullend is een uitgebreide literatuurstudie uitgevoerd om de specifieke veiligheidsinitiatieven verder specificeren.
- Als vervolg op de voorliggende studie is het COSI<sup>1</sup>-project uitgevoerd. In de figuur in de Appendix is dit COSI-project te situeren onder spoor 1 (focus op bedrijven), ontwikkeling tool 2 'Aanpak'. Een onderdeel van dit COSI-project is het in kaart brengen van drijfveren en hindernissen voor samenwerking om onderlinge risico's te beheersen. Om dit in kaart te brengen zijn interviews afgenomen bij verschillende BRZO-bedrijven die deel uitmaken van een cluster. Op basis van de resultaten van deze interviews werden bijkomende veiligheidsinitiatieven en haalbaarheidscriteria geformuleerd.

## 6. De tool: input – proces – output

De veiligheidsparameters en specifieke veiligheidsinitiatieven zijn opgelijst in een Excelbestand. Elke specifiek veiligheidsinitiatief is in de tool voorzien van een omschrijving, zodat de tool eenduidig ingevuld kan worden. De (sub)cluster van bedrijven die aan de slag gaat met de tool zal voor alle specifieke veiligheidsinitiatieven de huidige prestatie (stap 1) en de haalbaarheid samen scoren (stap 2).

- Stap 1 Prestatiescore: ten eerste zullen de bedrijven gezamenlijk aan alle specifieke veiligheidsinitiatieven een score toekennen wat betreft de huidige prestatie. Aan de hand van een drop-down lijst kan men een prestatiescore van 0 tot 3 toekennen, waarbij 3 een optimale prestatie reflecteert, en 0 een suboptimale prestatie:
  - Score 0 = Samenwerking ontbreekt volledig op dit moment
  - Score 1 = Al enige samenwerking, maar kan nog grondig verbeterd worden
  - Score 2 = Al enige samenwerking, maar kan nog in eerder beperkte mate verbeterd worden
  - Score 3 = Optimale samenwerking (op strategisch niveau met focus op lange termijn)

<sup>&</sup>lt;sup>1</sup> COSI staat voor 'collaboration on safety in (petro)chemical clusters'.

In deze stap kan men ook de optie 'niet van toepassing' aanduiden. Als er bijvoorbeeld niet wordt gewerkt met contractoren zijn de hierbij horende veiligheidsinitiatieven niet van toepassing. Of als bedrijven bijvoorbeeld niet zijn verbonden in elkaars keten, kan men dit scoren als 'niet van toepassing' waardoor deze veiligheidsinitiatieven niet verder worden meegenomen in de analyse.

Stap 2 – **Haalbaarheidsscore**: de veiligheidsinitiatieven die in de eerste stap een score van 0, 1 of 2 kregen worden in een volgende stap door de bedrijven gezamenlijk gescoord wat betreft de haalbaarheid. Aan de hand van meerdere criteria wordt er een inschatting gemaakt van de haalbaarheid van een bepaald veiligheidsinitiatief (zie Tabel 1) (gebaseerd op Meyer et al., 2016). Deze haalbaarheidsscore zorgt ervoor dat de specifieke context van een bepaalde cluster mee in beschouwing wordt genomen bij het rangschikken van de veiligheidsinitiatieven. Het kan immers mogelijk zijn dat door bepaalde clusterkenmerken een bepaald veiligheidsinitiatief zeer moeilijk te implementeren is. Ook de haalbaarheidsscore kan in de Excel-tool op een eenvoudige manier worden toegekend. Aan de hand van een drop-down lijst scoort men de criteria met 'ja' of 'nee'. Ook kan men het gewicht van elk criteria aanpassen indien nodig. Standaard heeft elk criterium een normaal gewicht, maar men kan dit ook aanpassen naar een 'hoog gewicht' als in een bepaalde cluster een criterium zwaar doorweegt. Zo kan het bijvoorbeeld zijn dat een beleid van een (moeder)bedrijf zeer strikt is, en dat er zeer moeilijk kan worden afgeweken van dit beleid. Men kan dan het criterium 'Laat het beleid van de (moeder)bedrijven het toe om in te zetten op dit veiligheidsinitiatief?' scoren met 'ja', en hier bijgevolg een 'hoog gewicht' aan toekennen.

De cluster van bedrijven vult *samen* de tool in. De prestatiescore (stap 1) en de haalbaarheidsscore (stap 2) wordt dus door de bedrijven gezamenlijk toegekend. Optioneel kunnen bij het toekennen van deze scores ook andere relevante stakeholders betrokken worden.

#### Tabel 1. Te scoren criteria om een inschatting te maken van de haalbaarheid van een veiligheidsinitiatief

- 1. **Kosten**: Is het inzetten op dit veiligheidsinitiatief betaalbaar?
- 2. **Implementatie-tijd**: Kan dit veiligheidsinitiatief op een redelijke termijn geïmplementeerd worden?
- 3. **Kennis**: Is de nodige knowhow beschikbaar om in te zetten op dit veiligheidsinitiatief? (Mogelijks kan er innovatie of (technische) kennis nodig zijn om in te zetten op een veiligheidsinitiatief)
- 4. **Billijkheid**: Als er op dit veiligheidsinitiatief wordt ingezet, betalen dan diegenen ervoor die ook het risico creëren?
- 5. **Risicoreductie potentieel**: Zijn de investeringen voor dit veiligheidsinitiatief niet disproportioneel met de potentiële veiligheidswinst die dit initiatief kan opleveren? (Return-on-investment)
- 6. **Afstand van elkaar**: Laat de geografische afstand tussen de bedrijven toe om in te zetten op dit veiligheidsinitiatief? (Liggen de bedrijven bijvoorbeeld niet te ver van elkaar om te investeren in gezamenlijke schuilplaatsen)
- 7. **Invloed beleid (moeder)bedrijven**: Laat het beleid van de (moeder)bedrijven het toe om in te zetten op dit veiligheidsinitiatief?

- 8. **Concurrentiegevoeligheid**: Laat de concurrentiegevoeligheid van de informatie die gedeeld moet worden voor dit veiligheidsinitiatief het toe dat hierop wordt ingezet?
- 9. **Organisatorische context:** Laat de organisatorische context het toe om in te zetten op dit veiligheidsinitiatief? (Zijn er bijvoorbeeld organisatiestructuren of Service Level Agreements (SLA's) aanwezig die conflicteren met de opzet van het veiligheidsinitiatief)
- 10. **Wettelijke context**: Laat de wettelijke context het toe om in te zetten op dit veiligheidsinitiatief?
- 11. **Compatibiliteit**: Is dit veiligheidsinitiatief verenigbaar met andere (veiligheids)initiatieven die geïmplementeerd zijn binnen de cluster?
- 12. **Ondersteuning door relevante stakeholders**: Is het waarschijnlijk dat dit veiligheidsinitiatief zal worden gesteund door relevante stakeholders, zoals bijvoorbeeld autoriteiten, de omwonenden of sectorverenigingen? (Zo kan een veiligheidsinitiatief een speerpunt zijn van een sectorvereniging, of kan een veiligheidsinitiatief leiden tot een verbeterde veiligheidsbeleving van omwonenden)
- 13. **Vertrouwen**: Is er tussen de betrokken partijen sprake van voldoende vertrouwen om gezamenlijk in te zetten op dit veiligheidsinitiatief? Kan men zich ervan vergewissen dat bijvoorbeeld uitgewisselde informatie vertrouwelijk behandeld zal worden? Of kan men er op vertrouwen dat in geval van een incident de uitgewisselde informatie niet misbruikt zal worden (door bijvoorbeeld handhavers)?
- 14. **Erkenning van het verkleinen van het risico:** Wordt het inzetten op dit veiligheidsinitiatief erkend als een verkleining van het risico (door bijvoorbeeld de toezichthouder of de verzekeraar)? (Zo kan bijvoorbeeld het gezamenlijk investeren in een technische maatregel leiden tot een verkleining van de veiligheidscontour, een verandering in de vergunning, of een lagere verzekeringspremie)
- 15. **Bijkomende voordelen:** Levert het inzetten op dit veiligheidsinitiatief ook voordelen op nietveiligheidsgerelateerde vlakken? (Zo kan een veiligheidsinitiatief ook voordelen opleveren op operationeel vlak of ten aanzien van de bedrijfsvoering)
- 16. **Risicocreatie**: Kan er gegarandeerd worden dat door het inzetten op dit veiligheidsinitiatief er geen andere / nieuwe veiligheidsrisico's (of risico's op andere gebieden zoals milieu) geïntroduceerd worden binnen de bedrijven?
- 17. **Hefboomwerking**: Kan er gegarandeerd worden dat door het inzetten op dit veiligheidsinitiatief er geen andere / nieuwe veiligheidsrisico's geïntroduceerd worden bij andere stakeholders?
- 18. **Continuïteit**: Kan er een lange-termijn commitment worden aangegaan tussen de bedrijven om in te zetten op dit veiligheidsinitiatief?

Vervolgens worden op basis van een achterliggend algoritme de veiligheidsinitiatieven automatisch gerangschikt naargelang potentiële veiligheidswinst. Hiervoor is dus geen input meer nodig vanuit de bedrijven.

- Stap 3 **Geïntegreerde haalbaarheidsscore**: aan de hand van de haalbaarheidsindicatie 'ja/nee' en het gewicht (normaal/hoog) dat in stap 2 aan de verschillende criteria is toegekend, wordt er een geïntegreerde score berekend:
  - o Een haalbaarheidsindicatie 'ja' wordt omgezet in 1 en een 'nee' in -1
  - Een normaal gewicht wordt omgezet in 1/2 en een hoog gewicht in 2/2

Vervolgens wordt de score van de haalbaarheidsindicatie vermenigvuldigd met de score van het gewicht, waardoor de geïntegreerde score wordt bekomen.

- Stap 4 **Finale ranking**: als laatste stap worden alle veiligheidsinitiatieven gerangschikt, eerst op basis van de prestatiescore, vervolgens op basis van de geïntegreerde haalbaarheidsscore:
  - o Ten eerste worden alle veiligheidsinitiatieven in 5 categorieën verdeeld
    - 1. De veiligheidsinitiatieven die in stap 1 de score van 0 kregen (suboptimale prestatie) staan helemaal bovenaan de lijst en worden onderverdeeld in categorie l
    - 2. De veiligheidsinitiatieven die in stap 1 de score van 1 kregen worden onderverdeeld in categorie II
    - 3. De veiligheidsinitiatieven die in stap 1 de score van 2 kregen worden onderverdeeld in categorie III
    - 4. De veiligheidsinitiatieven die in stap 1 de score van 3 kregen (optimale prestatie) worden onderverdeeld in categorie IV. Dit zijn initiatieven die niet verder worden gerangschikt. Bedrijven moeten er wel voor zorgen dat de optimale prestatie van deze veiligheidsinitiatieven behouden blijft.
    - 5. De veiligheidsinitiatieven die in stap 1 de score 'niet van toepassing' kregen staan helemaal onderaan in de lijst en krijgen het label 'niet van toepassing' (categorie V)
  - Ten tweede worden binnen categorie 1 tot 3 de veiligheidsparameters gerangschikt naargelang de geïntegreerde haalbaarheidsscore, waarbij de veiligheidsinitiatieven met de hoogste score – dit wil zeggen met de hoogste haalbaarheid – hoger gerangschikt worden.

Men krijgt dus als uitkomst een prioriteitsstelling van veiligheidsparameters, waarbij de hoogst gerankte veiligheidsparameters de meeste veiligheidswinst kunnen opleveren voor een bepaalde cluster.

De uitkomst van de tool is geen strikte kwantificering. Er zal dus niet nagegaan worden wat een cluster van bedrijven zal besparen of hoeveel incidenten er voorkomen kunnen worden als er wordt ingezet op een bepaalde veiligheidsparameter. Wel zal het een rangschikking zijn die rekening houdt met de reeds aanwezige (geïnstitutionaliseerde) veiligheidsparameters in een cluster en met de context van de specifieke cluster.

De praktische tool (in de vorm van een online Excel-file) is terug te vinden via volgende link:

https://clustersafety.github.io/Rangschikking veiligheidsparameters/

# 7. Uitleg van de veiligheidsparameters & specifieke veiligheidsinitiatieven

In wat volgt worden de veiligheidsparameters en specifieke veiligheidsinitiatieven die zijn geïncludeerd in de tool opgesomd, en wordt de relevantie van deze parameters om onderlinge risico's op een gezamenlijke manier te beheren en te beheersen gekaderd.

Deel 1 omvat de **proactieve** veiligheidsparameters en -initiatieven, waarbij de focus ligt op het voorkomen van ongewenste gebeurtenissen (Tabel 2). Deel 2 omvat de **reactieve** veiligheidsparameters en -initiatieven, waarbij de focus ligt op het mitigeren van de gevolgen als er toch een ongewenste gebeurtenis plaatsvindt (Tabel 3).

#### Tabel 2. Overzicht proactieve veiligheidsparameters & specifieke veiligheidsinitiatieven

#### Uitwisselen van veiligheidsinformatie

- Uitwisselen van veiligheidsinformatie over ongevalsscenario's
- Uitwisselen van contactgegevens
- Uitwisselen van informatie over niet-reguliere werkzaamheden
- Communiceren over incidenten
- Uitwisselen van informatie over veiligheidsinspecties van toezichthouders

#### Beoordelen & beheersen van onderlinge risico's op clusterniveau

- Gezamenlijke risicoanalyses met focus op onderlinge risico's
- Beheersen van onderlinge risico's op clusterniveau

#### Leren van elkaar

- Leren van gedeelde veiligheidsrisico's
- Leren van elkaars veiligheidsmanagement (operationeel)
- Leren van elkaars veiligheidsbeleid (strategisch)
- Gezamenlijk leren uit incidenten
- Peer-to-peer veiligheidsaudits

#### Uniformiteit en standaardisatie van veiligheid

- Standaardisatie van werkprocedures
- Standaardniveau van veiligheidskennis en -vaardigheden
- Uniforme veiligheidsregels en -normen
- Uniforme veiligheidsregels voor contractoren

#### De cluster van bedrijven als collectief

- Gemeenschappelijke veiligheidsvisie
- Overkoepelende clustercoalitie
- Gezamenlijk budget voor veiligheidsinitiatieven
- Gezamenlijke communicatie naar/met de omwonenden
- Cultuur van aanspreekbaarheid

#### Tabel 3. Overzicht reactieve veiligheidsparameters & specifieke veiligheidsinitiatieven

#### Gedeelde calamiteitenuitrusting en -faciliteiten

- Gezamenlijke bedrijfsbrandweer
- Samen investeren in of delen van technische uitrusting & faciliteiten om calamiteiten te bestrijden
- Early-warning systeem bij calamiteiten
- Uniforme evacuatiealarmen

#### Gezamenlijke noodorganisatie en crisiscommunicatie

- Gezamenlijk noodplan
- Clusterbreed bedrijfshulpverleningsteam (BHV-team)
- Gezamenlijke evacuatie- en rampenbestrijdingsoefeningen
- Communicatie tussen de clusterbedrijven in geval van calamiteiten
- Communicatie naar omwonenden in geval van calamiteiten

#### 7.1. Proactieve veiligheidsparameters en -initiatieven

Er zijn vijf proactieve parameters geformuleerd: het uitwisselen van veiligheidsinformatie, het beoordelen en beheersen van onderlinge risico's op clusterniveau, leren van elkaar, uniformiteit en standaardisatie van veiligheid, en de cluster van bedrijven als collectief. Bij deze veiligheidsparameters en de bijhorende veiligheidsinitiatieven ligt de focus op het voorkomen van ongewenste gebeurtenissen (linkerkant van de bow-tie).

#### Proactieve parameter: Uitwisselen van veiligheidsinformatie

#### Initiatief. Uitwisselen van veiligheidsinformatie over ongevalsscenario's

Als er een domino-effect aanwijzing is tussen bedrijven volgens de BRZO-wetgeving, dan is het uitwisselen van informatie over ongevalsscenario's die naburige bedrijven kunnen beïnvloeden wettelijk verplicht. Onderzoek toont echter aan dat, in geval van deze wettelijke verplichting, de informatie-uitwisseling vaak oppervlakkig plaatsvindt (van Nunen et al., 2019; 2020). Als er een wettelijke domino-effect aanwijzing is, zal dit bijgevolg (in het beste geval) bepalen of er reeds een vorm van informatie-uitwisseling aanwezig is, maar dit is geen garantie voor een *kwaliteitsvolle* informatie-uitwisseling.

Bovendien is het uitwisselen van informatie over mogelijke ongevalsscenario's niet enkel relevant in geval van een domino-effect aanwijzing. Ook voor BRZO-bedrijven zonder domino-effect aanwijzing, voor risicorelevante bedrijven (bedrijven die net onder de BRZO-drempel vallen), en zelfs voor niet-BRZO-bedrijven is deze informatie-uitwisseling nuttig, en in het kader van optimale veiligheid, nodig. Wat zijn de algemene activiteiten en de relevante aanwezige risico's van het buurbedrijf? Weet men met welke gevaarlijke stoffen een buurbedrijf werkt en wat de hoofdeigenschappen hiervan zijn (bijvoorbeeld als het vrijkomt is het geur- en kleurloos, bijtend,...)?

Het uitwisselen van informatie over ongevalsscenario's kan leiden tot een beter begrip van:

- Mogelijke ongevalsscenario's die in één bedrijf ontstaan, maar ook een impact (schade/letsel) kunnen hebben op naburige bedrijven. Denk hierbij bijvoorbeeld aan een toxische emissie waarvan de wolk een naburig bedrijf kan impacteren
- Mogelijke ongevalsscenario's die in één bedrijf ontstaan en leiden tot een secundair ongevalsscenario in een ander bedrijf (domino-effecten en keteneffecten)

Binnen een cluster van bedrijven is het dus nodig om goed op de hoogte te zijn van elkaars mogelijke ongevalsscenario's (zowel safety als security gerelateerde scenario's). Deze ongevalsscenario's moeten ook op periodieke basis geëvalueerd worden, of wanneer er zich belangrijke wijzigingen voordoen binnen het bedrijf, bijvoorbeeld bij een wijziging in het proces.

Als volgende stap is het cruciaal dat er ook echt iets wordt gedaan met deze informatieuitwisseling. Als naburige bedrijven goed geïnformeerd zijn over mogelijke ongevalsscenario's die een invloed kunnen hebben op andere bedrijven binnen de cluster, dan kan het duidelijk worden of men (extra) veiligheidsmaatregelen moet nemen.

#### Initiatief. Uitwisselen van contactgegevens

Binnen een cluster is het nodig om op regelmatige basis contactgegevens uit te wisselen van personen die men kan contacteren in geval van vragen m.b.t. veiligheid of bij calamiteiten. Een up-to-date contactenlijst is ten eerste handig in geval van (niet dringende) veiligheidsvragen, en is ten tweede noodzakelijk in geval van calamiteiten: wie moet men contacteren in geval van een calamiteit, en op welke manier zijn deze personen te bereiken? Het regelmatig updaten van deze informatie zorgt er bovendien voor dat men bij een eventuele wissel wat betreft contactpersonen kan kennismaken met elkaar.

#### Initiatief. Uitwisselen van informatie over niet-reguliere werkzaamheden

Binnen een cluster van bedrijven is het nodig om elkaar tijdig op de hoogte te brengen van geplande niet-reguliere werkzaamheden die mogelijks een impact kunnen hebben op de buurbedrijven (bijvoorbeeld onderhoud aan installaties), of waarbij er mogelijks overlast wordt veroorzaakt (bijvoorbeeld geluidsoverlast bij fakkelen). Men kan dan als buurbedrijf (veiligheids)maatregelen nemen indien nodig. Bovendien zorgt kennis over het plaatsvinden van niet-reguliere werkzaamheden bij een buurbedrijf voor een zekere staat van alertheid in het eigen bedrijf.

Dergelijke informatie-uitwisseling kan men op regelmatige basis inplannen, bijvoorbeeld maandelijks, maar ook moet de mogelijkheid bestaan om deze informatie op een snelle en eenvoudige manier ad hoc uit te wisselen.

#### Initiatief. Communiceren over incidenten

Er kan een clusterbreed rapportagesysteem voor (safety & security) incidenten opgezet worden, zodat de bedrijven op een laagdrempelige en uniforme manier informatie over incidenten met elkaar kunnen delen. Het gaat hierbij voornamelijk over (bijna-)ongevallen met (potentiële) arbeidsongeschiktheid tot gevolg, of voor procesgerelateerde incidenten.

Als informatie over incidenten binnen de bedrijven op regelmatige basis worden uitgewisseld (zelfs zonder dat de nabijgelegen bedrijven nadelige effecten van deze incidenten ondervonden), dan kan men hieruit lessen trekken voor het eigen bedrijf, en zorgt het binnen de cluster voor een cultuur van openheid (Nivolianitou et al., 2006).

#### Initiatief. Uitwisselen van informatie over veiligheidsinspecties van toezichthouders

Binnen een cluster van bedrijven kan het nuttig zijn om de resultaten van veiligheidsinspecties van toezichthouders met elkaar te delen (bijvoorbeeld inspectieresultaten BRZO+). Zo kan men als bedrijf zelf lessen trekken over bijvoorbeeld de vastgestelde overtredingen bij het buurbedrijf. Ook kan men elkaar binnen de cluster bijstaan met het zoeken naar verbeteringen.

Het delen van deze informatie, zeker als er een overtreding wordt vastgesteld, fungeert bovendien als een vorm van *peer-supervision*, waarbij de cluster als collectief de nodige acties mee kan opvolgen, en kan afdwingen indien nodig. Het delen van deze informatie kan bijdragen aan een cultuur van openheid.

#### Proactieve parameter: Beoordelen & beheersen van onderlinge risico's op clusterniveau

#### Initiatief. Gezamenlijke risicoanalyses met focus op onderlinge risico's

Een eerder geformuleerde veiligheidsparameter gaat over het uitwisselen van informatie over mogelijke ongevalsscenario's. Een stap verder is om gezamenlijk risicoanalyses uit te voeren om de onderlinge risico's en ongevalsscenario's samen in kaart te brengen. Risicoanalyses worden vaak enkel uitgevoerd door de individuele bedrijven, maar als aanvulling (dus niet als vervanging) kan een risicoanalyse die wordt uitgevoerd door meerdere bedrijven een meerwaarde opleveren (Reniers et al., 2008; Casciano et al., 2019).

Als men met meerdere bedrijven een risicoanalyse uitvoert kan dit leiden tot nieuwe inzichten, en kan het een vollediger en accurater overzicht opleveren van mogelijke (onderlinge) risico's en ongevalsscenario's. Vaak kijken bedrijven immers enkel naar de eigen risico's, zonder de risico's van buurbedrijven hierin mee te nemen. Het gezamenlijk uitvoeren van risicoanalyses kan er zo voor zorgen dat niet enkel mogelijke ongevalsscenario's van een individueel bedrijf in kaart worden gebracht, maar ook de ongevalsscenario's die kunnen ontstaan door de aanwezigheid van het buurbedrijf.

De mogelijkheid op impact (letsel/schade), domino-effecten, en keteneffecten zijn kenmerkend voor bedrijven die in een cluster gelegen zijn. In een gezamenlijke risicoanalyse kunnen deze onderlinge risico's de focus zijn. Zo kan er gezamenlijk in kaart gebracht worden

wat de mogelijke domino-effecten en keteneffecten zijn binnen de cluster, en in welke mate de bedrijven impact (letsel/schade) kunnen ondervinden ten gevolge van een incident bij een buurbedrijf. Bedrijven kunnen zich telkens opstellen als zowel veroorzaker van een ongevalsscenario, en als getroffene van een ongevalsscenario.

Onder meer een QRA, HAZOP of FMEA kan uitgevoerd worden op clusterniveau om de mogelijke onderlinge risico's te identificeren en te kwantificeren, en een zicht te krijgen op de mogelijke ongevalsscenario's in termen van waarschijnlijkheid en ernst. Cruciaal in een gezamenlijke risicoanalyse is dat de *interactie* tussen de bedrijven wordt meegenomen.

Een gezamenlijke risicoanalyse levert een kwantitatief en kwalitatief inzicht in de veiligheid binnen de cluster. Belangrijk is om deze risicoanalyse op regelmatige basis te evalueren, of te herbekijken in geval van een verandering, bijvoorbeeld veranderingen in het proces of gebruikte chemische stoffen.

Deze gezamenlijke risicoanalyses zijn zeker niet enkel nuttig voor BRZO-bedrijven of bedrijven met een wettelijke domino-effect aanwijzing. Ook risicorelevante bedrijven (bedrijven die net onder de BRZO-drempel vallen) of niet-BRZO-bedrijven kunnen deelnemen aan deze gezamenlijke risicoanalyse. Zeker wat betreft het in kaart brengen welke impact (letsel/schade) men kan ondervinden ten gevolge van een incident bij een buurbedrijf, kan een gezamenlijke risicoanalyse een meerwaarde opleveren voor alle bedrijven binnen een cluster.

Het meest optimaal is dat een gezamenlijke risicoanalyse echt *samen* door en met verschillende bedrijven wordt uitgevoerd. In de praktijk is dit echter niet altijd even evident. Een mogelijk alternatief is het uitvoeren van een risicoanalyse waarbij andere bedrijven uit de cluster aanwezig zijn als *observator*. Zo leert men ook de risico's van het bedrijf kennen, alsook de interpretaties en uitgangspunten in de uitgevoerde risicoanalyse.

Niet enkel risicoanalyses (die focussen op safety gerelateerde ongevalsscenario's), maar ook dreigingsanalyses, die focussen op het in kaart brengen van security gerelateerde ongevalsscenario's kunnen door de cluster gezamenlijk worden uitgevoerd.

#### Initiatief. Beheersen van onderlinge risico's op clusterniveau

Op basis van de aanwezige onderlinge risico's binnen een cluster is het nodig om veiligheidsmaatregelen (technisch, organisatorisch & menselijk) te nemen om deze risico's te beheersen. Als cluster kan men samen nadenken over mogelijkheden, of kan men gezamenlijk veiligheidsmaatregelen opzetten of hier in investeren om de onderlinge risico's te beheersen op een clusterniveau (Alileche et al., 2015).

Er kunnen preventieve acties genomen worden om onderlinge risico's te beheersen. Worden bijvoorbeeld werknemers opgeleid / bewust gemaakt over de aanwezige onderlinge risico's? M.a.w. weten werknemers dat handelingen mogelijks een impact kunnen hebben die verder reikt dan enkel het eigen bedrijf?

Ook kunnen er mitigerende acties genomen worden om onderlinge risico's te beheersen. De onderlinge risico's kunnen opgenomen worden in het (gezamenlijke) noodplan. En men kan andere relevante stakeholders, zoals bijvoorbeeld de reguliere brandweer, op de hoogte brengen van de mogelijke onderlinge risico's tussen de verschillende bedrijven.

#### Proactieve parameter: Leren van elkaar

#### Initiatief. Leren van gedeelde veiligheidsrisico's

Verschillende bedrijven binnen eenzelfde cluster hebben vaak veiligheidsrisico's met overeenkomsten in de oorzaak van het risico. Dit zijn de zogenaamde gedeelde risico's (OVV, 2018). Een voorbeeld zijn de specifieke risico's van onderdelen die in veel (petro)chemische fabrieken voorkomen, zoals afsluiters of warmtewisselaars (OVV, 2018). Ook cybersecurity is hiervan een voorbeeld. Het kan een meerwaarde opleveren als deze bedrijven *good practices* delen en van elkaar leren hoe ze met deze gedeelde risico's omgaan binnen de bedrijven, en waar ze zelf nog aanpassingen of aanvullingen kunnen doorvoeren om deze risico's op een optimale manier te beheersen. Men kan bijvoorbeeld een training aanpassen op basis van nieuwe inzichten.

#### Initiatief. Leren van elkaars veiligheidsmanagement (operationeel)

Binnen een cluster kan het nuttig zijn om op regelmatige basis samen te zitten met elkaar om good practices te delen en te leren hoe andere bedrijven hun veiligheidsmanagement (operationele veiligheid) aanpakken. Hoe pakken bijvoorbeeld andere bedrijven grote onderhoudstops aan? Hoe gaan bedrijven om met cybersecurity? Hoe gaan andere bedrijven om met een aanpassing in de wet- en regelgeving? Of hoe pakken bedrijven bepaalde veiligheidsgerelateerde opleidingen en trainingen aan?

#### Initiatief. Leren van elkaars veiligheidsbeleid (strategisch)

Niet enkel wat betreft operationele veiligheid, maar ook op het vlak van strategische veiligheid kan men in een cluster *good practices* delen en leren van elkaar. Zo kunnen (top)managers van verschillende bedrijven op regelmatige basis overleggen over de aanpak van het veiligheidsbeleid. Wat kan men met andere woorden beleidsmatig op strategisch niveau van elkaar leren over veiligheid? Indien nodig kan men aanpassingen doorvoeren in het veiligheidsmanagementsysteem op basis van nieuwe inzichten.

#### Initiatief. Gezamenlijk leren uit incidenten

Incidenten (zowel safety als security gerelateerd) die binnen de cluster hebben plaatsgevonden met een (potentieel) ernstige impact, kunnen op clusterniveau geanalyseerd worden. Dit niet als vervanging, maar wel als aanvulling op het incidentenonderzoek gevoerd door het bedrijf waar het incident plaatsvond.

Als noemenswaardige incidenten gezamenlijk worden geanalyseerd, kunnen ook andere bedrijven hun inzichten delen over mogelijke oorzaken en lessen die men hieruit kan trekken.

Deze gezamenlijke analyse kan leiden tot nieuwe inzichten, en een tunnelvisie kan zo voorkomen worden.

Bovendien kan men door gezamenlijk te leren uit incidenten bij buurbedrijven ook zelf maatregelen nemen in het eigen bedrijf om gelijkaardige incidentscenario's te voorkomen. Zo worden er niet enkel maatregelen geformuleerd op bedrijfsniveau, maar ook op clusterniveau.

Als gezamenlijk incidentenonderzoek moeilijk in de praktijk te realiseren is, kan men ook als individueel bedrijf het incident onderzoeken, en vervolgens het rapport delen en laten reviewen door de andere bedrijven uit de cluster.

#### Initiatief. Peer-to-peer veiligheidsaudits

Binnen een cluster kunnen er gezamenlijk veiligheidsaudits worden uitgevoerd door een team dat bestaat uit leden van verschillende bedrijven uit de cluster. Zo kan men leren van de aanpak van andere bedrijven, en voorkomt men een tunnelvisie.

Belangrijk bij deze peer-to-peer veiligheidsaudits is dat met uitgaat van een *risicogerichte* aanpak in plaats van een *regelgerichte* aanpak, waarbij de cluster van bedrijven met elkaar in gesprek gaat en kennis deelt om de veiligheid op een hoger niveau te brengen. De meeste veiligheidsinspecties door toezichthouders richten zich immers op *compliance*, waarbij de focus ligt op het zoeken naar overtredingen. Deze regelgerichte aanpak werkt eerder reactief gedrag bij de bedrijven in de hand. Risicogerichte peer-to-peer veiligheidsaudits kunnen hier een waardevolle aanvulling zijn.

#### Proactieve parameter: Uniformiteit en standaardisatie van veiligheid

Uniformiteit en standaardisatie wat betreft veiligheid kan er binnen een cluster voor zorgen dat veiligheid overzichtelijker, meer transparant en meer voorspelbaar wordt, dat er een bepaald kwaliteitsniveau wordt behaald, en dat er een duidelijk verwachtingspatroon gecreëerd wordt.

#### Initiatief. Standaardisatie van werkprocedures

In een werkproces of -procedure wordt gespecificeerd hoe een bepaalde taak of activiteit wordt uitgevoerd, en welke veiligheidsmaatregelen hierbij genomen moeten worden. Als men werkprocedures van gelijkaardige processen in verschillende bedrijven uniform maakt, verhoogt dit onder meer de voorspelbaarheid van normale werkzaamheden (Antonsen et al., 2012). Zeker als bedrijven verbonden zijn in elkaars keten kan standaardisatie van werkprocedures veiligheidswinst opleveren.

#### Initiatief. Standaardniveau van veiligheidskennis en -vaardigheden

Binnen een cluster kan men bepaalde kwaliteitseisen vastleggen wat betreft veiligheidskennis en -vaardigheden van de eigen werknemers. Zo kan men alle werknemers bijvoorbeeld een basispakket veiligheidsopleidingen en -trainingen laten volgen, en kan men enkel werken met

gecertificeerde opleidingsinstellingen. Dergelijke standaardisatie zorgt ervoor dat eenzelfde niveau wordt behaald binnen de verschillende bedrijven die deel uitmaken van de cluster.

#### Initiatief. Uniforme veiligheidsregels en -normen

Verschillende arbeidsveiligheidsregels op de verschillende bedrijfsterreinen kunnen voor werknemers voor onduidelijkheid en complexiteit zorgen. Uniforme veiligheidsregels kunnen hier een oplossing bieden. Zo kan men bijvoorbeeld dezelfde maximumsnelheid hanteren op alle bedrijfsterreinen die binnen een bepaald geografisch gebied liggen.

Ook wat betreft procesveiligheid kunnen er binnen een cluster afspraken gemaakt worden, bijvoorbeeld over de kwaliteit van risicoanalyses. Hierbij gaat het om een 'code van goede praktijk' waarbij er niet zozeer uniformiteit nodig is wat betreft de risicoanalysemethode, maar wel wat betreft de kwaliteit van de analyse: hoe grondig voert men de analyse uit, en wat neemt men hierbij in rekening? Is men bijvoorbeeld verbonden in de keten, dan is het een meerwaarde om mogelijke veranderingen in de processen van het verbonden ketenbedrijf mee te nemen in de eigen risicoanalyse. Of men kan in een HAZOP ook onderlinge risico's opnemen (relevante scenario's van buurbedrijven).

Deze uniformiteit draagt bij aan het verzekeren van een bepaald kwaliteitsniveau van veiligheid, waarbij bepaalde veiligheidsnormen door alle leden van de cluster gevolgd moeten worden. Bovendien kunnen verschillende veiligheidsregels op de verschillende bedrijfsterreinen voor onduidelijkheid en complexiteit zorgen.

#### Initiatief. Uniforme veiligheidsregels voor contractoren

Het kan zijn dat contractoren andere veiligheidsregels opgelegd krijgen bij verschillende bedrijven die deel uitmaken van dezelfde cluster. Een uniforme aanpak binnen de cluster wat betreft veiligheidsregels voor contractoren kan verschillende voordelen opleveren. Zo kan uniformiteit ervoor zorgen dat veiligheid overzichtelijker wordt. Een groot aantal verschillende veiligheidsregels kan enerzijds zorgen voor onduidelijkheid, en anderzijds voor onverschilligheid. Als contractoren op elke locatie verschillende veiligheidsvoorschriften krijgen, bestaat de kans dat men deze niet meer grondig leest.

Bovendien kan uniformiteit een duidelijk verwachtingspatroon creëren voor alle betrokken partijen. Als bepaalde veiligheidsregels voor contractoren gelden binnen de hele cluster, kan men ook de gevolgen van een overtreding doortrekken binnen de hele cluster. Het overtreden van een veiligheidsregel of een 'life saving rule', zoals bijvoorbeeld wanneer een contractor aan de slag is zonder werkvergunning, kan als gevolg hebben dat deze contractor niet meer wordt toegelaten binnen het bedrijf waar de overtreding werd begaan. Men zou dit kunnen doortrekken naar de gehele cluster, waar bij uitbreiding de betreffende contractor ook niet meer wordt toegelaten bij de andere bedrijven van de cluster. De cluster kan m.a.w. inzetten op een gemeenschappelijk beleid over hoe er met contractoren wordt omgegaan als er veiligheidsregels overtreden worden. Dergelijke uniformiteit zorgt ook voor een daling in complexiteit wat betreft controle op het naleven van gemaakte afspraken.

Contractoren die aan de slag gaan bij een bedrijf dat deel uitmaakt van een cluster kunnen bovendien ook best een introductie krijgen voordat ze aan de slag gaan, waarbij het bedrijf gekaderd wordt als deel uitmakend van een cluster (om bijvoorbeeld de mogelijkheid op domino-effecten of keteneffecten te benadrukken).

#### Proactieve parameter: De cluster van bedrijven als collectief

#### Initiatief. Gemeenschappelijke veiligheidsvisie

Als cluster kan men een gemeenschappelijke veiligheidsvisie opstellen waarbij duidelijke doelen worden geformuleerd (met een focus op de lange termijn). Deze gemeenschappelijke veiligheidsvisie kan de cluster vervolgens vertalen in een (gemeenschappelijk) veiligheidsbeleid om deze doelen te bereiken.

Het aangaan en vastleggen van dergelijk engagement zorgt voor een duidelijk kader waarbinnen men kan handelen om clusterveiligheid te optimaliseren, niet alleen op het moment dat een incident dat vereist, maar ook als 'goede buur'.

#### Initiatief. Overkoepelende clustercoalitie

Het oprichten van een overkoepelende clustercoalitie kan ervoor zorgen dat een sterkere samenhang en goede samenwerking tussen de verschillende bedrijven wordt gecreëerd of wordt onderhouden. Het zorgt ook voor het gelijktrekken van veiligheid, waarbij elk bedrijf aan bepaalde veiligheidseisen moet voldoen. Alle veiligheidsinitiatieven die worden opgezet op het niveau van de cluster kunnen gecoördineerd en gemanaged worden door deze overkoepelende clustercoalitie.

Om veiligheid binnen een cluster op een hoger niveau te brengen kan men aan een overkoepelende clustercoalitie bepaalde mandaten toekennen. Hierbij kan het bijvoorbeeld gaan om het opleggen van bepaalde veiligheidsregels die door alle bedrijven gevolgd moeten worden, of om de mogelijkheid om in bijzondere omstandigheden vergaderingen te beleggen en beslissingen te nemen (bijvoorbeeld het verplicht laten stilleggen van processen en werkzaamheden in geval van veiligheidsproblemen). Het gaat dus om een top-down structuur waarbij de clustercoalitie een bepaalde bevoegdheid heeft over de bedrijven.

Belangrijk is dat dergelijk clustermandaat niet enkel een reeks van veiligheidsregels oplegt aan de leden van de cluster, maar dat de clustercoalitie ook het vermogen heeft om het groter geheel te zien, en de toekomst van de veiligheid van de cluster beter te sturen. Een langetermijnvisie op vlak van veiligheid wordt zo ontwikkeld voor de cluster in zijn geheel.

Essentieel bij een overkoepelende clustercoalitie is dat de verschillende bedrijven die deel uitmaken van de cluster hierin een stem moeten krijgen, bijvoorbeeld door het afvaardigen van elk bedrijf in de coalitie (of als er heel veel kleine bedrijven zijn een afgevaardigde aanduiden die het geheel van deze kleinere bedrijven vertegenwoordigt). Zo worden kennis en expertise uit de verschillende bedrijven gebundeld wat de slaagkans van veiligheidsinitiatieven op clusterniveau ten goede kan komen. Het afvaardigen van elk bedrijf

in de coalitie zorgt bovendien voor een soort van controlemechanisme (*checks and balances*) dat ervoor zorgt dat de clustermacht niet in de handen van één bedrijf wordt geconcentreerd.

Bij het oprichten van een overkoepelende clustercoalitie moeten er duidelijke afspraken worden gemaakt en moeten de rollen en verantwoordelijkheden vastgelegd worden om de veiligheid op clusterniveau te beheren en te beheersen. Individuele bedrijven moeten goed op de hoogte zijn van de rechten en de plichten (wat als bijvoorbeeld een bedrijf de opgelegde regels door de clustercoalitie niet volgt). Dit kan opgenomen worden in een Service Level Agreement (SLA). Transparantie en een goede communicatie is essentieel om de synergie van een overkoepelende clustercoalitie te behouden.

#### Initiatief. Gezamenlijk budget voor veiligheidsinitiatieven

Een cluster van bedrijven kan ervoor kiezen om voor bepaalde veiligheidsinitiatieven op clusterniveau de financiële middelen te bundelen. Dit kan zorgen voor een beter en bewuster gebruik van financiële middelen. Zo kan men als cluster van bedrijven meer hoogwaardige investeringen doen dan wanneer een enkel bedrijf hierin moet investeren (Porter, 1998).

Enkele voorbeelden van (proactieve / preventieve) veiligheidsinitiatieven waarin men samen kan investeren:

- Gezamenlijke onderhoudsdienst
- Gezamenlijke veiligheidsopleiding en -training (programma's en/of faciliteiten) (al dan niet voor contractoren)
- Gezamenlijk outsourcen van activiteiten, bijvoorbeeld terreinbeveiliging
- Gezamenlijk een firewall neerzetten om cybersecurity te optimaliseren

#### Initiatief. Gezamenlijke communicatie naar/met de omwonenden

Als cluster is het nodig om bij communicatie naar (éénrichtingsverkeer) en met (tweerichtingsverkeer) de omwonenden als één geheel naar buiten te treden. Omwonenden zien een cluster immers vaak als één geheel, en niet als verschillende afzonderlijke bedrijven.

Zo is het aan te raden om als cluster onder normale operationele omstandigheden op regelmatige basis te communiceren naar en met de omwonenden. Men kan bijvoorbeeld informeren over de veiligheidsinitiatieven die men gezamenlijk neemt als cluster, en men kan in gesprek gaan met de omwonenden om eventuele (veiligheids)bezorgdheden te bespreken en te bekijken op welke manier hier men hier als cluster aan tegemoet kan komen. De (veiligheids)perceptie van omwonenden over de cluster zal zo op een positieve manier beïnvloed worden.

#### Initiatief. Cultuur van aanspreekbaarheid

Als cluster kan men ernaar streven om een 'cultuur van aanspreekbaarheid' te creëren waarbij men elkaar kan aanspreken op een niet- dwingende, niet-veroordelende, en positiefconstructieve manier, bijvoorbeeld als er iets minder goed gaat binnen een clusterbedrijf. Als bedrijf kan men leren en verbeteren naar aanleiding van dit aanspreken, en het zorgt binnen de cluster voor een cultuur van openheid.

#### 7.2. Reactieve veiligheidsparameters en -initiatieven

Er zijn twee reactieve parameters geformuleerd. Bij deze parameters ligt de focus op het mitigeren van de gevolgen als er toch een ongewenste gebeurtenis plaatsvindt (rechterkant van de bow-tie). Ten eerste gaat het om gezamenlijke technische initiatieven (calamiteitenuitrusting en -faciliteiten), en ten tweede gaat het om gezamenlijke organisatorische initiatieven (noodorganisatie en crisiscommunicatie).

#### Reactieve parameter: Gedeelde calamiteitenuitrusting en -faciliteiten

#### Initiatief. Gezamenlijke bedrijfsbrandweer

Als verschillende nabijgelegen bedrijven een aanwijzing bedrijfsbrandweer hebben, kan het voor de cluster van bedrijven veiligheidswinst opleveren als men dit gezamenlijk organiseert. Een gezamenlijke bedrijfsbrandweer kan een kostenbesparing opleveren, en door het bundelen van kennis en middelen kan de bedrijfsbrandweer ook professioneler georganiseerd worden, waardoor de kwaliteit van de hulpverlening stijgt (Rosmuller et al., 2019).

Het inzetten op een gezamenlijke bedrijfsbrandweer is niet enkel aan te raden als alle bedrijven van de cluster een aanwijzing bedrijfsbrandweer hebben. Ook wanneer er geen aanwijzing is kan het voor een bedrijf (en bijgevolg voor de cluster in zijn geheel) veiligheidswinst opleveren<sup>2</sup>. Zo is de aanrijtijd van een bedrijfsbrandweer korter waardoor er sneller ingegrepen kan worden. Ook is een bedrijfsbrandweer opgeleid om industriële calamiteiten te bestrijden, en zijn ze beter bekend met de aanwezige gevaarlijke stoffen. Als bedrijven zonder aanwijzing zich aansluiten bij een bedrijfsbrandweer kunnen afspraken gemaakt worden om de bijdragen/investeringen af te stemmen op de aanwezige risico's.

Als er een gezamenlijke bedrijfsbrandweer aanwezig is, moeten er ook duidelijke afspraken zijn over de opleiding en training van alle bemanningsleden van deze gezamenlijke bedrijfsbrandweer (niveau van opleiding, trainingsuren, enzovoort). Dit is noodzakelijk omdat een gezamenlijke bedrijfsbrandweer vaak bemant wordt vanuit verschillende bedrijven.

# Initiatief. Samen investeren in of delen van technische uitrusting en faciliteiten om calamiteiten te bestrijden

Ongeacht het feit of er al dan niet een aanwijzing bedrijfsbrandweer is bij een of meer van de bedrijven, is het nodig om als bedrijf in te zetten op nodige technische uitrusting en faciliteiten in geval van calamiteiten. Het kan daarbij gaan om BHV-verzamelplaatsen, schuilplaatsen al

<sup>&</sup>lt;sup>2</sup> Als een bedrijfsbrandweer aanwezig is, en er is een calamiteit bij een nabijgelegen bedrijf dat niet is aangesloten bij deze bedrijfsbrandweer, mag deze bedrijfsbrandweer wettelijk gezien het incident bij het niet-aangesloten bedrijf niet bestrijden.

dan niet voorzien met waterschermen, noodstroomvoorzieningen, enzovoort. Als cluster van bedrijven kan men ervoor kiezen om hier gezamenlijk op in te zetten.

Zo kan men gezamenlijk investeren in deze technische uitrusting en faciliteiten door het delen van de aankoopkosten en onderhoudskosten. Door het bundelen van financiële middelen kan men meer hoogwaardige uitrusting en faciliteiten aankopen dan wanneer een enkel bedrijf hierin moet investeren. Bij deze gezamenlijke investering wordt de cluster van bedrijven als geheel bekeken, zoals bijvoorbeeld de som van het aantal werknemers van de gecombineerde bedrijven waarvoor potentiële BHV-verzamelplaatsen voorzien moeten worden in het geval van een calamiteit. Ook bijvoorbeeld de opslagplaats van de uitrusting, of de locatie en bereikbaarheid van schuil- en verzamelplaatsen moet bekeken worden in functie van de coalitie van bedrijven. Zo moeten schuil- en verzamelplaatsen gemakkelijke bereikbaar zijn voor alle bedrijven.

Men hoeft niet per se gezamenlijk te investeren. Men kan als cluster van bedrijven ook technische uitrusting en faciliteiten om calamiteiten te bestrijden met elkaar delen. Er kunnen afspraken gemaakt worden om beroep te doen op de uitrusting en faciliteiten van een nabijgelegen bedrijf tijdens een crisissituatie. Hierbij moeten duidelijke procedures opgesteld worden, en moet men rekening houden met de mogelijkheid dat een crisissituatie verschillende bedrijven gelijktijdig kan beïnvloeden. Men mag met andere woorden als bedrijf niet zelf in de problemen komen als een bepaalde faciliteit of uitrusting gedeeld of uitgeleend wordt aan een nabijgelegen bedrijf tijdens een crisissituatie.

#### Initiatief. Early-warning systeem bij calamiteiten

Een van de kritische elementen bij calamiteiten en crisisrespons is het tijdig communiceren van informatie naar relevante stakeholders (Berger-Sabbatel & Journé, 2018). Bij geclusterde bedrijven is het door de geografische nabijheid cruciaal om elkaar tijdig te waarschuwen in geval van een calamiteit. Een early-warning systeem wordt opgezet om nabijgelegen bedrijf reeds in een zeer vroeg stadium te informeren in geval van (mogelijkheid op) een calamiteit. daarbij bijvoorbeeld over het informeren over een onvoorziene temperatuursverhoging in een van de processen, of over een securitydreiging zoals een indringer op het terrein. Zo kan het nabijgelegen bedrijf al eventuele maatregelen treffen, zoals het stopzetten van activiteiten of het stilleggen van processen. Als er (nog) geen maatregelen genomen worden zijn ze ten minste in een zekere staat van alertheid. Tijdige waarschuwing kan voorkomen dat een incident leidt tot impact (letsel/schade) bij een buurbedrijf, of dit kan voorkomen dat een incident leidt tot een domino-effect of een keteneffect.

#### Initiatief. Uniforme evacuatiealarmen

Als het door een calamiteit nodig is om gebouwen of de omgeving te verlaten, worden evacuatiealarmen gebruikt. Bij geclusterde bedrijven is het aan te raden om uniforme geluidssignalen te gebruiken, om verwarring te voorkomen en zodat bij nabijgelegen

bedrijven de evacuatie gelijktijdig kan plaatsvinden. Als er geen uniforme alarmen gebruikt worden, is het noodzakelijk dat de omliggende bedrijven zeer goed op de hoogte zijn van elkaars geluidssignalen en de betekenis ervan.

#### Reactieve parameter: Gezamenlijke noodorganisatie en crisiscommunicatie

#### Initiatief. Gezamenlijk noodplan

Binnen een cluster wordt de noodorganisatie best niet gecoördineerd en uitgevoerd op het niveau van de individuele bedrijven, maar wel op clusterniveau. Op deze manier kan er tijdens een crisissituatie snel en adequaat gereageerd en ingegrepen worden, waarbij alle bedrijven gelijktijdig en op een zelfde manier betrokken worden (Perry et al., 2003).

Zo kan er een gezamenlijk noodplan opgesteld worden waarin de te nemen stappen in geval van een crisissituatie worden beschreven op clusterniveau. Dit gezamenlijk noodplan omvat duidelijke procedures en afspraken om op een gezamenlijke manier adequaat te reageren op een crisissituatie. Ook de verschillende rollen en verantwoordelijkheden moeten hierin duidelijk vastgelegd worden, zodat de taken duidelijk zijn en men weet wat er verwacht wordt (van zichzelf en van anderen) tijdens een noodgeval.

Belangrijk is om de inhoud van dit gezamenlijke noodplan op regelmatige basis te evalueren. Dit kan bijvoorbeeld tweejaarlijks, of wanneer er zich belangrijke wijzigingen voordoen binnen de cluster, bijvoorbeeld bij de uitbreiding van een bestaande fabriek, of als een nieuw bedrijf zich dichtbij komt vestigen.

Ook communicatie van dit plan naar relevante stakeholders is belangrijk. Zo moet bijvoorbeeld de reguliere brandweer op de hoogte zijn van de gemaakte afspraken tussen de verschillende bedrijven.

#### Initiatief. Clusterbreed bedrijfshulpverleningsteam (BHV-team)

Naast een BHV-team binnen de individuele bedrijven, is binnen een cluster ook het opzetten van een clusterbreed BHV-team aan te raden, waar werknemers van de verschillende bedrijven deel van uitmaken. Zeker wanneer er een gezamenlijk noodplan opgesteld is, kan een clusterbreed BHV-team tijdens een crisissituatie de activiteiten coördineren, en de verschillende bedrijven harmoniseren tot een goed samenwerkend team. Investeren in een clusterbreed BHV-team leidt bovendien tot het bundelen van kennis en middelen waardoor de professionaliteit en kwaliteit van de hulpverlening stijgt.

Ook hier moeten de taken en verantwoordelijkheden vastgelegd worden, zodat een clusterbreed BHV-team een duidelijk zicht heeft op hun bedrijfsoverschrijdende rollen en verantwoordelijkheden in geval van een calamiteit.

Gezamenlijke afspraken over het opleidings- en trainingsniveau van een clusterbreed BHV-team zijn nodig, zodat iedereen op een gelijkaardig en hoog kennis- en kundeniveau bevindt.

Verder is het nodig dat dit clusterbreed BHV-team regelmatig gezamenlijk oefeningen organiseert om hun werking te evalueren en te optimaliseren.

#### Initiatief. Gezamenlijke evacuatie- en rampenbestrijdingsoefeningen

Naast het organiseren van evacuatie- en rampenbestrijdingsoefeningen in de individuele bedrijven, is het nodig om in een cluster op regelmatige tijdstippen evacuatie- en rampenbestrijdingsoefeningen te organiseren waaraan de verschillende bedrijven uit de cluster deelnemen. Een calamiteit binnen een clusterbedrijf heeft immers bijna altijd ook een impact op de buurbedrijven. Gezamenlijke evacuatie- en rampenbestrijdingsoefeningen zorgen voor een betere voorbereidheid in geval van een calamiteit.

Ook andere relevante stakeholders – binnen en buiten de cluster – worden hier best bij betrokken, zoals het havenbedrijf en/of spoorwegbedrijf indien aanwezig, de eventuele (gezamenlijke) bedrijfsbrandweer, de plaatselijke autoriteiten, omwonenden, enzovoort.

Essentieel hierbij is nadien de gezamenlijke debriefing waarbij een nabespreking en evaluatie van de oefeningen plaatsvindt. Zo kunnen er gezamenlijk acties ondernomen worden om het noodplan te optimaliseren.

#### Initiatief. Communicatie tussen de clusterbedrijven in geval van calamiteiten

Binnen een cluster moet er duidelijk vastgelegd worden op welke manier de bedrijven (en eventuele andere relevante stakeholders) tijdens een noodsituatie in contact komen met elkaar, informatie kunnen uitwisselen, of om hulp vragen indien nodig. Dit is noodzakelijk om een adequate rampenbestrijding op clusterniveau te garanderen (Salasznyk et al., 2006). Het kan er bovendien voor zorgen dat effecten zich niet of beperkt uitbreiden naar nabijgelegen bedrijven.

#### Initiatief. Communicatie naar omwonenden in geval van calamiteiten

Bij calamiteiten met (en zelfs zonder) mogelijks effect buiten de bedrijfsmuren is een gezamenlijk communicatieplan aan te raden waarbij de cluster als één geheel naar buiten treedt. Zo kan men gezamenlijk op een eenduidige manier de omwonenden informeren of geruststellen (OVV, 2012).

### 8. Een optimaal gebruik van de tool

#### 8.1. Factoren die bijdragen aan een optimaal gebruik

Bij alle deelnemende actoren – de bedrijven zelf en eventuele andere relevante stakeholders – is het noodzakelijk dat er een zekere **bereidheid en motivatie** is om de veiligheid te verbeteren. Aangezien het gaat om een vrijwillige deelname is dit **commitment** noodzakelijk alvorens men gezamenlijk aan de slag gaat met de tool.

De tool beoogt dat men als cluster van bedrijven evolueert naar een samenwerkende gemeenschap. Hierbij is het cruciaal dat er een zekere mate van **vertrouwen** bestaat tussen de diverse partijen. Er moet bekeken worden op welke manier er op een vertrouwelijke manier samengewerkt kan worden, en hoe er kan omgegaan worden met eventueel wantrouwen tussen de verschillende bedrijven. Niet enkel tussen de bedrijven, maar ook naar eventuele andere stakeholders is dit vertrouwen belangrijk. Hoe betrek je bijvoorbeeld de overheid er op een vertrouwelijke manier bij?

Belangrijk is dat het invullen van de tool op een zo **objectief mogelijke** manier gebeurt en **naar alle eerlijkheid** wordt ingevuld. Enkel dan zullen de resultaten van de tool betrouwbaar zijn, en kan men met deze output op een optimale manier aan de slag. Zoals eerder beschreven (zie deel 3 gebruikers van de tool) is het nodig dat de personen die aan de slag gaan met de tool over **accurate en volledige kennis** beschikken om de veiligheidsparameters te scoren. Het is dus nodig dat men voldoende inzicht heeft in onder meer de eigen veiligheidsprestaties, de aanwezige risico's en mogelijke ongevalsscenario's binnen het bedrijf, en de werking van het eigen veiligheidsmanagement. Ook is het nodig de personen die aan de slag gaan met de tool **makkelijk toegang** hebben tot deze kennis binnen het bedrijf.

Aangezien de focus van de tool ligt op het *gezamenlijk* invullen en op het *gezamenlijk* tot resultaten komen, is een zekere **gelijkwaardigheid** tussen de partijen aangewezen **in termen van competentie**. Zowel de bedrijven als eventuele andere stakeholders die de tool gebruiken moeten bekwaam zijn om een correcte inschatting te maken van de huidige prestatie en de haalbaarheid van de veiligheidsparameters. Deze gelijkwaardigheid houdt ook in dat de nodige informatie die beschikbaar is binnen de individuele bedrijven begrijpelijk is voor alle partijen die de tool gebruiken.

#### 8.2. Uitdagingen en aandachtspunten

De mate van vertrouwen tussen de verschillende partijen is geformuleerd als een factor die bijdraagt aan het succes van de tool. Een belangrijke uitdaging is bijgevolg het **omgaan met eventueel wantrouwen** tussen de verschillende bedrijven, en tussen andere stakeholders die bij het invullen van de tool betrokken worden.

Ook kunnen nog andere uitdagingen optreden. Zo kunnen er bij het invullen van de tool **verschillen** zijn **in de percepties** van de bedrijven wat betreft de huidige prestatie en de haalbaarheid van de te scoren veiligheidsparameters en -initiatieven. In geval van discrepanties is het nodig dat de bedrijven op een onderbouwde manier tot een consensus komen.

Als aandachtspunt geldt dat de tool niet gebruikt mag worden om een bepaald niveau van veiligheid of een bepaald niveau van inspanningen wat betreft veiligheid aan te tonen. De tool is immers **geen** *compliance check* en mag dus ook niet voor dit doel gebruikt worden.

Een volgend aandachtspunt is het **vervolgtraject**. Bedrijven moeten immers aan de slag met de resultaten om ook werkelijk tot een hoger veiligheidsniveau te komen. Ondersteuning van de bedrijven kan nodig zijn om concreet aan de slag te gaan met de resultaten van de tool, en gezamenlijk verbeterplannen op te stellen.

Tot slot richt de tool zich enkel op veiligheidsmaatregelen die de bedrijven zelf kunnen nemen om veiligheid te optimaliseren. Er zijn echter ook **opportuniteiten voor andere stakeholders** om de veiligheid binnen een cluster van bedrijven te verbeteren. Zo zijn er bijvoorbeeld voor de toezichthouder kansen weggelegd om tijdens inspecties de bedrijven niet te bekijken als op zichzelf staande, individuele bedrijven, maar wel als bedrijven die deel uitmaken van een cluster.

## 9. Referentielijst

Alileche N., Cozzani V., Reniers G., Estel L. (2015). Thresholds for domino effects and safety distances in the process industry: A review of approaches and regulations. Reliability Engineering & System Safety, 143: 74-84. <a href="https://doi.org/10.1016/j.ress.2015.04.007">https://doi.org/10.1016/j.ress.2015.04.007</a>

Antonsen S., Skarholt. K, Ringstad A.J. (2012). The role of standardization in safety management: A case study of a major oil & gas company. Safety Science, 50(10): 2001–2009.

Berger-Sabbatel A., Journé B. (2018). Organizing Risk Communication for Effective Preparedness: Using Plans as a Catalyst for Risk Communication. In: Bourrier M., Bieder C. (eds.) Risk Communication for the Future. Towards Smart Risk Governance and Safety Management. Springer. <a href="https://doi.org/10.1007/978-3-319-74098-0\_3">https://doi.org/10.1007/978-3-319-74098-0\_3</a>

Casciano M., Khakzad N., Reniers G., Cozzani V. (2019). Ranking chemical industrial clusters with respect to safety and security using analytic network process. Process Safety and Environmental Protection, 132: 200-213. https://doi.org/10.1016/j.psep.2019.10.024

Meyer T., Reniers, G. (2016). Engineering Risk Management, 2nd ed. De Gruyter: Berlin.

Nivolianitou Z., Konstandinidou M., Michalis C. (2006). Statistical analysis of major accidents in petrochemical industry notified to the major accident reporting system (MARS). Journal of Hazardous Materials, A137: 1-7. https://doi.org/10.1016/j.jhazmat.2004.12.042

Onderzoeksraad voor Veiligheid (OVV) (2012). Brand bij Chemie-Pack te Moerdijk. Den Haag.

Onderzoeksraad voor Veiligheid (OVV) (2018). Chemie in samenwerking: Veiligheid op het industriecomplex Chemelot. Den Haag.

Perry R.W., Lindell M.K. (2003). Preparedness for emergency response: guidelines for the emergency planning process. Disasters, 27(4): 336-350. <a href="https://doi.org/10.1111/j.0361-3666.2003.00237.x">https://doi.org/10.1111/j.0361-3666.2003.00237.x</a>

Porter M. (1998). Clusters and the New Economics of Competition. Harvard Business Review.

Reniers G.L.L., Dullaert W. (2008). Knock-on accident prevention in a chemical cluster. Expert Systems with Applications, 34: 42-49. <a href="https://doi.org/10.1016/j.eswa.2006.08.033">https://doi.org/10.1016/j.eswa.2006.08.033</a>

Rosmuller N., Stohr, P., Kappetijn, K., Flohr, R. (2019). Interregional industrial disaster abatement in the Netherlands: the need for public-private partnerships. Chemical Engineering Transactions, 77: 493-498. <a href="https://doi.org/10.3303/CET1977083">https://doi.org/10.3303/CET1977083</a>

Salasznyk P.P., Lee E.E., List G.F., Wallace W.A. (2006). A systems view of data integration for emergency response. International Journal of Emergency Management, 3(4): 313-331. https://doi.org/10.1504/IJEM.2006.011299 Swuste P., van Nunen K., Reniers G. (2018). Domino-effecten bij chemische bedrijven en clusters, een literatuuroverzicht van de kennisontwikkeling. Tijdschrift voor toegepaste Arbowetenschap, 31(4): 131-147.

Swuste P., van Nunen K., Reniers G., Khakzad N. (2019). Domino-effects in chemical factories and clusters: An historical perspective and discussion. Process Safety and Environmental Protection, 124: 18-30. https://doi.org/10.1016/j.psep.2019.01.015

van Nunen K., Reniers G., Swuste P. (2019). Verkennende studie naar (petro)chemische clusters en veiligheid: Veiligheidsparameters binnen (petro)chemische clusters en losstaande (petro)chemische bedrijven. Beschikbaar via <a href="https://repository.tudelft.nl">https://repository.tudelft.nl</a>

van Nunen K., Swuste P., Reniers G., Schmitz P. (2020). Safety in (petro)chemical clusters and stand-alone companies. Chemical Engineering Transactions, 82: 73-78. https://doi.org/10.3303/CET2082013

## **Appendix**

**Aanleiding** 

niveau te realiseren

TU Delft & Universiteit Antwerpen

voor Veiligheid

TU Delft

ongevallen.
Stakeholders

· Best practices hebben getoond dat er

binnen een cluster potentie is om gezamenlijk een hoger veiligheids-

· Studie naar veiligheidsparameters

van (petro)chemische geclusterde en losstaande bedrijven. Onderzoeksraad

 Aanbeveling: meer samenwerken om onderlinge risico's te

· Aanbeveling: instrumentarium

Toezicht en Handhaving (VTH) te

 Literatuuronderzoek laat zien dat er internationaal meer besef komt

over de rol die domino-effecten kunnen spelen bij majeure

 Signalen dat er geen eenduidig beeld is over Artikel 8 uit het Brzo

t.a.v. de reductie van onderlinge

om via Vergunningverlening.

sturen op het beperken van onderlinge risico's.

Deze studie werd uitgevoerd in opdracht van het Ministerie van Infrastructuur en Waterstaat, en maakt onderdeel uit van het bredere clusterbeleid binnen de (petro)chemische industrie. De huidige studie situeert zich binnen spoor 1 (focus op bedrijven), ontwikkeling tool 1 'Veiligheidsparameters'.

# Clusterbeleid binnen de (petro)chemische industrie

Met clusterbeleid werken we aan het versterken van de (omgevings)veiligheid. Wij streven naar een duurzame samenwerking, waarbij leren van elkaar, transparantie t.a.v. onderlinge risico's en gezamenlijk werken aan maatschappelijke doelstellingen centraal staan.

#### TU Delft ontwikkelt 2 tools: Veiligheldsparameters 2 Aanpak Versterken van veiligheid door elkaar te Onderzoek naar de uitvoerbaargeven aan waar de om binnen een cluster informatie ondersteunen in gemeenschappelijke heid, het effect en de potentie van meeste veiligheidswinst breed te delen over o.a. onderlinge belangen, zoals het omgaan met Artikel 8 uit het Brzo met bedrijven te behalen is binnen een risico's, samen te werken en van onderlinge risico's met een domino-aanwijzing cluster. elkaar te leren. Spoor 1: focus op bedrijven (TU Delft) **Bedrijven** Eindrapportage door onafhankelijke partij Overheidsorganisaties Spoor 2: focus op overheidsorganisaties Een duurzame samenwerking binnen chemische clusters op het gebied van Verkenning van Aanbevelingen voor een Conclusies en Scope beperkt zich tot aanbevelin-(omgevings)veiligheid en andere handelingsperspectief voor Artikel 8 uit het gen die zich richten op transparantie aanbevelingen maatschappelijke doelen alle betrokken partijen Brzo met stakeholders door bestuurlijke en samenwerking om zware

ongevallen te voorkomen

beoordelingscommissie