

Eindrapport

Andersoortig toezicht op het Brzo:
verkenning van mogelijkheden door het
transparant delen van (zelfbeoordelings-)
informatie

"De tijd is er rijp voor"

In opdracht van het Rijksinstituut voor
Volksgezondheid en Milieu

Oosterbeek, 14 december 2018

Uw kenmerk: Z/110035/01

Inhoud

Managementsamenvatting	4
1. Inleiding	10
2. Doel, resultaat, onderzoeksvragen en aanpak	12
2.1 Inleiding	12
2.2 Doel en resultaat	12
2.3 Onderzoeksvragen	12
2.4 Onderzoeksaanpak	13
3. Risicogestuurd toezicht Brzo	15
3.1 Inleiding	15
3.2 Toezicht op Brzo-tankopslagbedrijven	15
3.3 Programmatisch en risicogestuurd toezicht op Brzo-tankopslagbedrijven	18
3.4 Gewenste ontwikkelingen risicogestuurd toezicht	20
3.5 Ingezette ontwikkelingen binnen Brzo	20
3.6 Ontwikkelingen binnen Programma Duurzame Veiligheid 2030	21
4. De Safety Maturity Tool (SMT)	23
4.1 Inleiding	23
4.2 Aanleiding en doel van de SMT	23
4.3 Onderdelen en onderbouwing van de SMT.....	23
4.4 Gebruikers en uitvoering van de SMT	26
4.5 De werking van de SMT	27
4.6 Draagvlak voor de SMT en het gezamenlijk streven naar meer veiligheid	28
4.7 Vergelijking van de SMT met Landelijke Benadering Risicobedrijven (Brzo-aanpak)	29
5. SMT in toezicht	31
5.1 Inleiding	31
5.2 Verkende mogelijkheden van gebruik SMT-informatie in risicogestuurd toezicht	31
5.3 Voorwaarden voor gebruik van SMT in risicogestuurd toezicht	32
5.4 Gefaseerde ontwikkeling van inzicht en overtuiging van gedeeld belang	33
6. Risicogestuurd toezicht door andere Rijkstoezichthouders.....	34
6.1 Inleiding	34
6.2 ILT, DNB en IGJ als bron van inspiratie	34
6.3 Risicogestuurd toezicht en informatie uit zelfbeoordelings- en zelfreguleringsinstrumenten.....	35
6.4 Context: doel van het toezicht en de relatie tussen toezichthouder en instelling	37
6.5 Tussenbalans: evenwicht tussen de wet, behoefte aan informatie en de toezichtsrelatie	38

7. Conclusies	40
7.1 Inleiding	40
7.2 Is de SMT bruikbaar in risicogestuurd toezicht?	40
7.3 Beschikbaarheid van SMT-informatie op basis van afspraken met de VOTOB	40
7.3 Beschikbaarheid van SMT-informatie zonder waarborgen	41
8. Ontwikkelrichtingen	44
8.1 Inleiding	44
8.2 Ontwikkelrichting 1: Pilot Uitwisseling SMT (pilot US)	44
8.3 Ontwikkelrichting 2: Brzo+ DataLab	46

Bijlagen

1. Geïnterviewde organisaties
2. Organisaties vertegenwoordigd in workshop
3. Bestudeerde documenten

Managementsamenvatting

Inleiding

In de loop van 2018 is een verkenning uitgevoerd naar mogelijkheden van het gebruik van zelfbeoordelingsinformatie in andersoortig (risicogestuurd) toezicht op bedrijven die vallen onder het Besluit risico's zware ongevallen 2015 (hierna: Brzo). Dit toezicht wordt uitgevoerd door verschillende inspectiediensten die met elkaar samenwerken in het programma Brzo+. Namens het programma is de Inspectie Sociale Zaken en Werkgelegenheid (hierna: ISZW) opdrachtgever voor deze verkenning.

De directe aanleiding van de verkenning is het werk in 'Roadmap 3': Transparantie als drijvende kracht voor veiligheid. Roadmap 3 is onderdeel van het Programma Duurzame Veiligheid 2030, een samenwerkingsverband tussen overheden, bedrijven en kennisinstellingen met als doel de duurzame verbetering van veiligheid in de (petro)chemische industrie. Het samenwerkingsverband van inspectiediensten, het programma Brzo+, is geïnteresseerd in de mogelijkheden van het transparant delen van informatie in relatie tot veiligheid.

In deze samenvatting wordt, beknopt, toegelicht het doel en de aanpak van de verkenning, de conclusies van de verkenning en ontwikkelrichtingen voor de toekomst.

Doel en aanpak van de verkenning

De verkenning had tot doel vast te stellen of het delen van de uitkomsten van het zogenaamde Safety Maturity Tool (SMT) van de Nederlandse Vereniging van Tankopslagbedrijven (VOTOB) kan bijdragen aan het risicogestuurd toezicht op het Brzo. De SMT is een auditinstrument waarmee jaarlijks de stand van zaken rond veiligheid wordt vastgesteld bij de terminals van alle leden van de VOTOB op de drie elementen van veiligheid: de techniek, het veiligheidssysteem en de veiligheidscultuur.

In deze verkenning is onderzocht of en hoe in het Brzo-toezicht gebruik kan worden gemaakt van de SMT voor inrichting van risicogestuurd toezicht. Daarvoor zijn verkend het wettelijk kader voor het toezicht, de aard en achtergrond van de SMT, de bruikbaarheid van de SMT vanuit het perspectief van het Brzo-toezicht en vanuit het perspectief van de gebruikers van de SMT.

Daarnaast is bij onderdelen van drie Rijksinspectiediensten op andere domeinen, verkend of en hoe zij gebruik maken van zelfbeoordelings- en zelfreguleringsinformatie in risicogestuurd toezicht. De drie betrokken Rijksinspectiediensten zijn Inspectie Leefomgeving & Transport (IL&T), afdeling Veilige Mobiliteit; De Nederlandsche Bank (DNB), divisie Toezicht Pensioenfondsen; de Inspectie Gezondheidszorg & Jeugd (IGJ), afdeling Risicodetectie & Ontwikkeling. De uitkomsten van dit deel van de verkenning zijn inspiratiebron geweest voor de ontwikkelrichtingen en voorwaarden voor ontwikkelingen.

Tot slot is verkend welke ontwikkelrichtingen er zijn voor de integratie van de SMT in het risicogestuurd toezicht op het Brzo.

De verkenning is uitgevoerd door documentstudie, interviews en een workshop met stakeholders in het vraagstuk: de leden van de VOTOB en de verschillende inspectiediensten verantwoordelijk voor het toezicht op het Brzo.

De informatie uit de SMT is bruikbaar voor risicogestuurd toezicht

De SMT is, onder voorwaarden, bruikbaar voor risicogestuurd toezicht. Dit geldt voor de aanpak van de SMT-audit en voor de informatie uit de SMT-audits. Brzo-toezicht zou de inhoud en aanpak van de SMT kunnen benutten als mogelijk voorbeeld voor het verder verbeteren van de inspectiemethodiek voor het Brzo. Met name de SMT-aanpak van de cultuurscan biedt mogelijkheden om de cultuurscan binnen het Brzo verder vorm te geven. Ook de informatie uit de SMT-audits is bruikbaar en kan input zijn voor risicogestuurd toezicht op het Brzo. De SMT biedt namelijk inzicht in dezelfde aspecten van een bedrijf (software, hardware, mindware) als die waarin Brzo-inspecties inzicht bieden. Deze conclusie wordt onderschreven in de workshop. 'De tijd is er rijp voor' aldus de deelnemers.

Om SMT-informatie goed te kunnen benutten, moet aan de volgende voorwaarden worden voldaan:

- Brzo-toezichthouders krijgen de gelegenheid de kwaliteit van de audit-methodiek en informatie goed te verifiëren. Door Brzo-inspecteurs nauw te betrekken bij deze verificatie, ontstaat vertrouwen in de waarde van de methodiek voor het toezicht. Zonder dat vertrouwen ontstaat het risico dat zij SMT-informatie niet structureel zullen betrekken in het bepalen van de inspectie-agenda per Brzo-bedrijf.
- Binnen het kader van samenwerkingsprogramma Brzo+, wordt een risicoanalysemethodiek ontwikkeld waarin de SMT-informatie een zinvolle plaats inneemt.
- Op voorhand moet voor alle betrokkenen, maar met name voor de VOTOB-leden duidelijk zijn op welke wijze SMT-informatie wordt gebruikt en van invloed is op het toezicht en eventuele handhaving.
- De ervaring die het Brzo-toezicht opdoet met het gebruik van de SMT in risicogestuurd toezicht wordt ingezet in een bredere ontwikkeling naar een grotere doelgroep bedrijven. Want de huidige groep VOTOB-leden is te klein om een specifieke aanpak voor deze groep te legitimeren.
- Er moet sprake zijn van wederkerige transparantie: de kennis die Brzo-toezichthouders ter beschikking krijgen door het gebruik van de SMT-informatie in risicoanalyses, moet ook worden gedeeld met de VOTOB zodat ook de VOTOB-leden daarvan kunnen leren.

Beschikbaarheid van SMT-informatie op basis van afspraken met de VOTOB

Brzo-toezicht kan de informatie uit de SMT op twee manieren verwerven.

Opvragen van informatie zonder waarborgen

De eerste manier is dat de SMT-informatie wordt opgevraagd bij bedrijven waardoor de overdracht van SMT-informatie een (semi-)verplicht karakter krijgt als onderdeel van het Brzo-toezicht. Hierbij wordt geen onderscheid gemaakt tussen opvragen zonder en met vordering. In beide gevallen is er sprake van een zekere noodzaak de informatie ter beschikking te stellen: in het geval van een vordering is het bedrijf verplicht de informatie aan de inspectie te geven; in het geval van opvragen zonder vordering is het bedrijf niet verplicht maar kan, door te weigeren, de indruk wekken niet transparant te willen zijn over de veiligheid en daarmee extra aandacht opwekken bij inspectiediensten.

Bij deze keuze ontstaat, binnen de huidige verhoudingen, een aanzienlijk risico dat een deel van de VOTOB-leden de SMT-audit vooral zullen gaan gebruiken om te voorkomen dat zij door Brzo-inspecties als risico worden beschouwd of niet meer mee willen doen aan de SMT-audit. In dat geval verliest de SMT haar oorspronkelijke functie voor de VOTOB-leden: samen leren ten behoeve van de veiligheid.

Beschikbaar stellen van informatie met waarborgen

De tweede manier is door afspraken te maken met de VOTOB over de vrijwillige levering van informatie. In dat geval verwachten de VOTOB-leden een zekere wederkerigheid door het bieden van een aantal waarborgen:

- Het ter beschikking stellen van SMT-informatie mag niet leiden tot het verlies van een level playing field voor VOTOB-leden. Dit betekent dat vrijwillig delen van SMT-informatie niet mag leiden tot door méér handhaving bij VOTOB-leden door Brzo-toezichthouders omdat dit meer inzicht geeft in potentiële overtredingen.
- SMT-informatie van individuele bedrijven mag niet openbaar worden gemaakt. Bedrijven vrezen dat dit zal leiden tot negatieve publiciteit over het bedrijf, wat schadelijk is voor de relatie tussen het bedrijf en haar omgeving. Ook vrezen de VOTOB-leden dat dit zal leiden tot concurrentie op veiligheid omdat dit het samen leren in de weg zal staan.

Wanneer voor deze weg wordt gekozen, is het belangrijk dat wordt vastgesteld welke waarborgen kunnen worden gegeven en welke (bestuurlijke) afspraken daarover moeten worden gemaakt. Deze moeten namelijk passen binnen het wettelijk kader en de daarop gebaseerde Landelijke Handhavingstrategie Brzo. Ook afspraken over openbaarmaking van informatie moeten worden gemaakt binnen de wettelijke kaders waarbinnen de verschillende gezagen opereren binnen het Brzo-toezicht.

Beschikbaarheid van SMT-informatie op basis van wederzijds vertrouwen

Door de complexiteit van het toezicht op de Brzo, is het denkbaar dat goede waarborgen over het gebruik van de SMT-informatie niet kunnen worden gegeven. Welke mogelijkheid blijft dan over? Hoe kan de SMT-informatie dan worden gedeeld zonder vordering of waarborgen? En onder welke voorwaarden zal de risico-informatie op basis van de SMT ook daadwerkelijk worden gebruikt?

Op basis van deze verkenning trekken wij de conclusie dat vrijwillige uitwisseling van SMT-informatie wordt bevorderd wanneer wederzijds vertrouwen wordt versterkt tussen het Brzo-toezichthouders en de VOTOB-leden. De volgende voorwaarden dragen bij aan wederzijds vertrouwen:

1. Er is sprake van gemeenschappelijk belang in een zo goed mogelijke borging van de veiligheid in de bedrijven.
2. Het Brzo-toezicht gaat zorgvuldig om met de SMT-informatie door goed toezicht, rechtvaardige handhaving en een maximale borging van de vertrouwelijkheid binnen de kaders van de wet.
3. Brzo-toezichthouders hebben kunnen vaststellen dat SMT-informatie van goede kwaliteit is, verkregen via een kwalitatief goede audit-methodiek.
4. Risico-informatie mede gebaseerd op de SMT-informatie, wordt door het Brzo-toezicht ook gedeeld met de VOTOB zodat sprake is van wederzijds leren.

Ad. 1. Gemeenschappelijk belang van bedrijven en inspectie

Uit de verkenning bij DNB en IGJ komt naar voren dat deze inspectiediensten het uitgangspunt van een gemeenschappelijk belang een belangrijke pijler vinden van een constructieve en open toezichtsrelatie. Zij gaan daar overigens niet zonder meer vanuit. Dit moet wel blijken uit de wijze waarop de instellingen laten zien dat zij werkelijk streven naar goede kwaliteit zorg of een evenwichtige bedrijfsvoering door daarop steeds weer de juiste maatregelen te treffen. Als dat niet blijkt, volgen er maatregelen.

Vertaald naar Brzo-toezicht en de VOTOB-leden, betekent dit dat VOTOB-leden die dat hebben laten blijken, bijvoorbeeld in eerdere Brzo-inspecties en de SMT-resultaten, ook vanuit een gemeenschappelijk belang worden benaderd. Binnen de kaders van het Brzo krijgen zij te maken met een handhavingsaanpak die blijk geeft van hun inspanningen om de veiligheid te verbeteren. Het Brzo-toezicht laat zien maximaal gebruik te maken van de beschikbare discretionaire ruimte binnen de handhaving om positieve inspanningen te belonen, overigens binnen de kaders van hun verantwoordelijkheid.

Ad 2. Het Brzo-toezicht gaat zorgvuldig om met SMT-informatie

Uit de verkenning is gebleken dat VOTOB-leden zich zorgen maken over méér handhaving omdat Brzo-toezichthouders beschikken over bedrijfsspecifieke informatie uit de SMT en daarmee het verlies van een level playing field. Daarom moet het Brzo-toezicht laten zien hoe het vrijwillig delen van SMT-informatie inderdaad leidt tot beter inzicht in de risico's en daarom tot meer effectief toezicht en handhaving binnen de hele branche, niet alleen bij de VOTOB-leden. Bedrijven die de zaken goed voor elkaar hebben, krijgen vanzelf minder te maken met handhaving dan bedrijven die tot de risicocategorie behoren.

De kwaliteit en transparantie van de risicoanalyses zijn hierbij van groot belang. In lijn met de voorbeelden bij ILT, IGJ en DNB, betekent dit dat hiervoor expertise zou moeten worden georganiseerd.

Om te voorkomen dat (de dreiging van) handhaving een versturende rol gaat spelen in de ontwikkeling van wederzijds vertrouwen en transparantie, is het denkbaar de uitwisseling van SMT-informatie, in eerste instantie, te beperken tot dat deel van de SMT waarvoor geen wettelijk kader is dat kan leiden tot handhaving: de cultuurscan van de SMT. Informatie over de veiligheidscultuur is interessant voor een risico-analyse maar aan de ontwikkeling van een veiligheidscultuur worden geen wettelijke eisen gesteld. In de workshop gaven deelnemers aan, ook graag de onderdelen techniek (hardware) en systeem (software) te willen betrekken omdat deze onderdelen beter aansluiten bij de taken van het toezicht.

Een laatste voorwaarde die ook werd benadrukt in de workshop met inspecteurs, VOTOB-leden en experts was dat er bestuurlijke afspraken zouden moeten worden gemaakt over de handhaving op bedrijven die SMT-informatie ter beschikking stellen. Dit om te borgen dat gemaakte afspraken over handhaving tussen inspectiediensten en de VOTOB ook op termijn kunnen worden nagekomen. Deze bestuurlijke afspraken zouden bijvoorbeeld kunnen worden gemaakt in het Bestuurlijk Omgevingsberaad met de Minister, het Openbaar Ministerie en de Omgevingsdiensten.

Ad 3. Het vertrouwen in de kwaliteit van de SMT-informatie

Het Brzo-toezicht moet dus maatregelen treffen die het vertrouwen wekken van betrokken bedrijven. Het vergt ook vertrouwen van het Brzo-toezicht in de kwaliteit van de SMT-informatie. Alleen dan heeft het zin om te investeren in de beschikbaarheid en het gebruik van de informatie.

Om dit vertrouwen te winnen, moeten Brzo-inspecteurs de gelegenheid krijgen de kwaliteit van de SMT-informatie te verifiëren. Daarnaast is het behulpzaam wanneer de VOTOB open staat voor kritiek op de SMT en laat zien te willen acteren op die kritiek. Op die manier kan de VOTOB het vertrouwen van het Brzo-toezicht in de SMT ook versterken.

Ad 4. Wederzijds leren door het delen van risico-informatie

Een vierde mogelijkheid het om wederzijds vertrouwen te versterken, is wederkerigheid in het delen van informatie: door informatie uit risicoanalyses voor het Brzo-toezicht te delen met de VOTOB-leden ontstaat wederkerigheid. Het Brzo-toezicht stelt de uitkomsten van risicoanalyses op (sub-)sector beschikbaar aan de branche zodat de hele sector baat heeft bij het beschikbaar stellen van informatie. Binnen de VOTOB worden deze risicoanalyses vervolgens vertaald naar verbetervoorstellen voor de leden. Een voorbeeld van een dergelijke aanpak is hoe DNB onderzoeksinformatie ter beschikking stelt die instellingen helpt te verbeteren of benchmarks uitvoert en deelt op basis waarvan instellingen weten waar zij staan.

Een andere vorm van wederkerigheid is transparantie over de risicoanalyses. Het Brzo-toezicht zou bereid kunnen zijn SMT-experts kritisch te laten kijken naar de Brzo-risicoanalyses en onderliggende methodes om zelf ook te leren van de kennis die er in de sector aanwezig is. Door zelf te laten zien te willen luisteren en leren, geven de Brzo-toezichthouders het goede voorbeeld van transparantie en wederzijds leren voor de sector.

Ontwikkelrichting 1: Pilot Uitwisseling SMT (pilot US)

Vertrouwen is noodzakelijk om SMT-informatie effectief te kunnen gebruiken voor Brzo-risicoanalyses zonder dat de SMT haar functie verliest als leermiddel voor VOTOB-leden. Maar het opbouwen van vertrouwen kost tijd. Om wederzijds vertrouwen te krijgen in de kwaliteit van de SMT-audit en in de GIR-informatie is het nuttig dat Brzo-inspecteurs en de VOTOB-bedrijven veel gelegenheid krijgen om, in een setting buiten de handhaving, kennis te nemen van elkaars werkwijze.

Op basis van de informatie uit de workshop met deskundige vertegenwoordigers van Brzo-inspectiediensten, VOTOB-leden en de SMT-auditors, kunnen globale stappen worden geformuleerd voor de pilot. Voor elke stap is meer vertrouwen nodig in elkaars werkwijze en het nut van transparante uitwisseling zodat transparantie kan worden vergroot. Daarom zal elke stap moeten worden afgerond met een go-no go moment waarop wordt bepaald of de uitkomsten van de stap voldoende zijn voor een vervolg.

De pilot bestaat uit vijf fases met ieder een aantal stappen. Deze fases zijn:

Fase 1: voorbereiding van de pilot

Fase 2: kennismaking en verkenning van de kwaliteit en waarde van beschikbare informatie en de wijze waarop informatie kan worden uitgewisseld

Fase 3: ontwerpen van toepassingen van SMT-informatie in risicogestuurd toezicht op Brzo

Fase 4: uitvoering pilot de met de ontwikkelde toepassingen en de afspraken die zijn gemaakt omtrent de uitwisseling van informatie

Fase 5: evaluatie

Op basis van de uitkomsten van dit onderzoek zijn fase 1 en 2 nader uitgewerkt. De volgende fases moeten worden uitgewerkt op basis van de uitkomsten van fase 1. Hier wordt volstaan met een globale omschrijving van het doel van fases 3 tot en met 5.

Ontwikkelrichting 2: Brzo+ DataLab

In de tweede ontwikkelrichting ligt de focus vooral op de ontwikkeling van een bredere, kwalitatief sterke risicoanalyse voor Brzo-toezicht waarbij informatie uit de SMT één van de bronnen is. Deze ontwikkelrichting is gebaseerd op de organisatiekenmerken van risicoanalyses uitgevoerd door IGJ, DNB en ILT.

In deze ontwikkelrichting worden de risicoanalyses ten behoeve van het toezicht op het Brzo ondergebracht in een datalab, vooralsnog aangeduid als 'Brzo+ Datalab'. Dit is een nieuw in te richten kennisorganisatie van de gezamenlijke Brzo-toezichthouders, die nauw verbonden is met het Brzo+ samenwerkingsprogramma en die gevoed wordt met data van de Brzo-toezichthouders en data van derden zoals de VOTOB. Het Brzo+ Datalab is een neutrale organisatie met expertise op het terrein van data-analyse (IGJ- en ILT-model) en Brzo-expertise (het DNB-model) en staat als separate kennisorganisatie op afstand van de individuele Brzo-toezichthouders. Deze organisatie doet risicoanalyses op basis van een combinatie van GIR-informatie, SMT-informatie en andere relevante informatie op sector- en op bedrijfsniveau. Daarnaast biedt het de mogelijkheid duurzaam te investeren in de ontwikkeling van data-analyse voor Brzo-toezicht.

In het kader van transparantie en het leereffect, zouden de data-analyses die worden uitgevoerd door deze neutrale organisatie, ook beschikbaar kunnen worden gesteld aan sector- en brancheorganisaties als de VOTOB.

Dit Brzo+ Datalab kan overigens voor toezicht op alle Brzo-bedrijven functioneren. Daarmee is geborgd dat het gebruik van de SMT-informatie niet alleen gevolgen heeft voor de leden van de VOTOB maar voor alle Brzo-bedrijven. Daarnaast kan, vanuit het Datalab, initiatief worden genomen ook andere bronnen van zelfbeoordelingsinformatie te benutten voor risicoanalyse.

1. Inleiding

Dit is het eindrapport van de verkenning naar mogelijkheden van andersoortig (risicogestuurd) toezicht door de gezamenlijke inspectiediensten betrokken in het toezicht op bedrijven die vallen onder het Besluit risico's zware ongevallen 2015 (hierna: Brzo). Doel van deze verkenning is het vaststellen van nieuwe mogelijkheden voor risicogestuurd toezicht op bedrijven die onder het Brzo vallen (hierna: Brzo-bedrijven), door het transparant delen van gegevens tussen bedrijfsleven en de betrokken inspectiediensten. Deze inspectiediensten werken samen in het programma Brzo+. Namens het programma is de Inspectie Sociale Zaken en Werkgelegenheid (hierna: ISZW) opdrachtgever voor deze verkenning.

De directe aanleiding van de verkenning is het werk in 'Roadmap 3': Transparantie als drijvende kracht voor veiligheid. Roadmap 3 is onderdeel van het Programma Duurzame Veiligheid 2030, een samenwerkingsverband tussen overheden, bedrijven en kennisinstellingen met als doel de duurzame verbetering van veiligheid in de (petro)chemische industrie. Het samenwerkingsverband van inspectiediensten, het programma Brzo+, is geïnteresseerd in de mogelijkheden van het transparant delen van informatie in relatie tot veiligheid.

Door in te zetten op het transparant delen van informatie, willen Brzo+-inspectiediensten (hierna: Brzo-toezicht) een belangrijke ambitie realiseren: een steeds effectievere inzet van de altijd beperkte toezichtscapaciteit door een andere, meer risicogestuurde inrichting van toezicht. Om effectief risicogestuurd toezicht te kunnen houden, hebben toezichthouders goede informatie nodig voor hun risicoanalyses. Deze risicoanalyses moeten inzichten bieden in die elementen binnen bedrijven die prioriteit moeten krijgen in het toezicht. Door gebruik te maken van relevante, betrouwbare informatie in risicoanalyses, kan meer betrouwbaar en meer precies worden vastgesteld wat de risico's zijn in de Brzo-bedrijven.

Brzo-bedrijven zijn van hun kant steeds actiever in het systematisch zelf beoordelen van hun veiligheidsniveau. Brancheorganisaties zijn hierbij betrokken door het ontwikkelen van branchespecifieke vragenlijsten en zogenaamde self assessment tools. Voorbeelden hiervan zijn de Veiligheidsladder en de Safety Maturity Tool.

Er is verkend hoe informatie uit één van de self assessment tools, de Safety Maturity Tool (hierna: SMT) een bijdrage kan leveren aan risicogestuurd Brzo-toezicht. De SMT wordt gebruikt door petrochemische tankopslagbedrijven die lid zijn van de Vereniging van Nederlandse Tankopslagbedrijven (hierna: VOTOB).

Ook is verkend wat het Brzo-toezicht kan leren van andere toezichthoudende organisaties die gebruikmaken van risicogestuurd toezicht. Daarbij is specifiek gekeken hoe bedrijven gebruikmaken van informatie uit zelfbeoordelingsinstrumenten of andere instrumenten voor zelfregulering.

Dit rapport is het resultaat van de verkenning op deze twee onderdelen en is als volgt opgebouwd. Na een toelichting op het doel, het resultaat en de aanpak van de verkenning (hoofdstuk 2) wordt de context van de onderzoeksvragen beknopt beschreven: de huidige aanpak en de beoogde ontwikkelingen van risicogestuurd toezicht door de drie belangrijkste inspectiediensten, samenwerkend in het programma Brzo+ (hoofdstuk 3). Vervolgens wordt ingegaan op de achtergrond, de opbouw, het gebruik en het draagvlak van de SMT (hoofdstuk 4). In hoofdstuk 5 wordt ingegaan op de bruikbaarheid van SMT-informatie voor risicogestuurd toezicht: toegelicht worden de mogelijkheden van informatiegebruik, de voorwaarden voor gebruik en risico's van gebruik voor risicogestuurd toezicht.

In hoofdstuk 6 wordt beschreven hoe andere toezichthoudende diensten gebruikmaken van informatie uit zelfbeoordelingsinstrumenten en andere instrumenten voor zelfregulering. Hoofdstuk 7 bevat de conclusies van dit onderzoek. In het laatste hoofdstuk (8) worden twee ontwikkelrichtingen beschreven naar t gebruik van informatie uit de SMT voorrisicoanalyses ten behoeve van het Brzo-toezicht.

2. Doel, resultaat, onderzoeksvragen en aanpak

2.1 Inleiding

Dit hoofdstuk beschrijft het doel, het resultaat en de onderzoeksvragen die leidend zijn geweest voor deze verkenning. Ook wordt beknopt de aanpak toegelicht.

2.2 Doel en resultaat

Het doel van de verkenning is tweeledig:

Doel 1: Inzicht bieden in de mate waarin en wijze waarop de Safety Maturity Tool (SMT) van de Vereniging van Nederlandse Tankopslagbedrijven (VOTOB) geschikte informatie biedt voor risicogestuurd Brzo-toezicht.

Doel 2: Inzicht bieden in de wijze waarop (een selectie van) andere toezichthouders invulling hebben gegeven aan risicogestuurd toezicht om daaruit aanwijzingen en leerpunten te destilleren voor de inrichting van risicogestuurd Brzo-toezicht.

Het resultaat van het onderzoek is een rapport met de volgende onderwerpen:

1. Een analyse van het type informatie dat door VOTOB-bedrijven wordt beschouwd in de SMT met een beoordeling van deze informatie op bruikbaarheid voor de inrichting van risicogestuurd Brzo-toezicht¹ (hoofdstukken 3 tot en met 6).
2. Een analyse van risicogestuurd toezicht door andere toezichthoudende overheidsorganisaties met inzichten en leerpunten voor Brzo-toezicht voor inrichting van risicogestuurd toezicht (hoofdstuk 7).
3. Conclusies en aanbevelingen met een reflectie op en een synthese van het geheel van de bevindingen van het onderzoek (hoofdstuk 8).

2.3 Onderzoeksvragen

Voor deze verkenning zijn een hoofdvraag voor het gehele onderzoek en onderzoeksvragen per doel geformuleerd. De hoofdvraag is:

Hoofdvraag voor het hele onderzoek:

Op welke wijze kan in het Brzo-toezicht invulling worden gegeven aan een (meer) risicogestuurde toezichtsvorm bij de (petro)chemische tankopslagbedrijven door het delen van zelfbeoordelingsinformatie van deze bedrijven?

¹ Onder 'bruikbaarheid' wordt hier verstaan 'mogelijkheden om beredeneerd invulling te geven aan toezicht op tankopslagbedrijven in de preventiefase, de fase waarin zich (nog) geen incident heeft voorgedaan'.

De onderzoeksvragen per doel:

Doel 1

Is de Safety Maturity Tool (verder: SMT) bruikbaar in risicogestuurd toezicht bij (petro)chemische tankopslagbedrijven door de samenwerkende inspectiediensten in het programma Brzo+?

Deelvragen:

1. Wat is risicogestuurd toezicht op het Brzo? (definitiekwestie/afkadering)
2. Wat is de SMT? (toelichting c.q. achtergrondinformatie)
3. Hoe komt de SMT tot stand?
4. Hoe wordt de SMT in de praktijk toegepast/uitgevoerd?
5. Hoe breed wordt de SMT toegepast onder leden van de VOTOB?
6. Wat is de gebruikersdoelgroep van de SMT en hoe onderscheiden deze tankopslagbedrijven zich van tankopslagbedrijven die geen gebruikmaken van de SMT? In hoeverre is daarin een ontwikkeling te zien?
7. Hoe betrouwbaar zijn de uitkomsten van de SMT en hoe onderscheidt het instrument zich hierin van de audittools voor het toezicht op het Brzo (bestaande uit de NIM, de veiligheidscultuurtool TNO en de hardwaretool) die nu wordt ontwikkeld door de Landelijke Benadering Risicobedrijven?
8. Welke informatie uit de SMT is geschikt voor risicogestuurd toezicht op het Brzo?
9. Is een andere vorm en inrichting mogelijk van het Brzo-toezicht waarbij de SMT bruikbaar is als risicogestuurde informatiebron? Zo ja, wat moet daarvoor gebeuren?

Doel 2

Wat kan het Brzo-toezicht leren van de wijze waarop toezichthoudende overheidsorganisaties in andere domeinen risicogestuurd toezicht hebben ingericht?

Deelvragen:

- Op welke wijze maken andere toezichthoudende organisaties (De Nederlandsche Bank, Inspectie Leefomgeving en Transport, Inspectie Gezondheidszorg en Jeugd) gebruik van risicogestuurd toezicht en wat kan Brzo-toezicht hiervan leren?
- Op welke wijze hebben de toezichthoudende organisaties risicogestuurd toezicht ingericht?
- In hoeverre, op welke wijze en onder welke voorwaarden maken de toezichthoudende organisaties gebruik van informatie uit self assessment tools en andere instrumenten voor zelfregulering?

2.4 Onderzoeksaanpak

De verkenning is aangepakt in de volgende stappen:

- Stap 1:* Startbijeenkomst met de opdrachtgever om het doel, de onderzoeksvragen en de aanpak nader te specificeren.
- Stap 2:* Interviews en documentstudie. In de bijlagen is een overzicht van geïnterviewde personen en bestudeerde documenten opgenomen.
- Stap 3:* Conceptrapportage.
- Stap 4:* Workshop met afgevaardigden van het Brzo-toezicht en de VOTOB ter toetsing van onderzoeksresultaten en ter verkenning van mogelijkheden voor vervolg.
- Stap 5:* Eindrapportage.

Het onderzoek voor deze verkenning heeft plaatsgevonden door documentstudie en kwalitatieve interviews met een selectie van vertegenwoordigers van het Brzo-toezicht en de VOTOB.

Voor deze kwalitatieve aanpak is gekozen om breed inzicht te krijgen in de werking van de SMT en de mogelijkheden voor inzet van de informatie uit de tool voor risicogestuurd Brzo-toezicht. Daar waar nodig, zijn verdiepende vragen gesteld. De beoordeling van de SMT is dan ook gebaseerd op het expert judgement van geïnterviewden en de onderbouwing van de SMT in toelichtende documentatie.

Een beperking van deze kwalitatieve onderzoeksmethode is dat niet is vastgesteld of de beelden en meningen die naar voren kwamen in de interviews, een representatief beeld geven. Daarom is ervoor gekozen de uitkomsten van de verkenning te toetsen op juistheid en herkenbaarheid en te verrijken in een bijeenkomst met een bredere vertegenwoordiging van betrokken inspectiediensten en de VOTOB. Deze bijeenkomst heeft plaatsgevonden op 2 november 2018.

Het onderzoek is begeleid door een begeleidingsgroep bestaande uit een afgevaardigde van de VOTOB en van de Inspectie SZW.

3. Risicogestuurd toezicht Brzo

3.1 Inleiding

Het huidige beleid en de huidige aanpak ten aanzien van risicogestuurd toezicht op Brzo-bedrijven vormen het startpunt voor het mogelijk toekomstig gebruik van de SMT als informatiebron in risicogestuurd toezicht. Daarom wordt in dit hoofdstuk een beknopte beschrijving gegeven van de huidige aanpak en de gewenste ontwikkelingen in risicogestuurd toezicht.

Het hoofdstuk wordt afgerond met gewenste ontwikkelingen binnen het kader van het Programma Duurzame Veiligheid 2030. Dit programma vormt de aanleiding voor het voorliggende onderzoek en speelt een belangrijke rol in de ontwikkelingen rond Brzo-regelgeving, toezicht en de relatie tussen overheid en bedrijven.

3.2 Toezicht op Brzo-tankopslagbedrijven

Context voor dit onderzoek: doelgroep en wettelijk kader

Dit onderzoek heeft betrekking op Nederlandse tankopslagbedrijven die als lid van de VOTOB de SMT gebruiken. Alle VOTOB-leden zijn tevens Brzo-bedrijven. Het gaat om een groep van 28 tankopslagbedrijven die een subset vormen van de totale groep van ca. 400 Brzo-bedrijven in Nederland.² Onderstaand volgt een korte schets van het wettelijk kader voor tankopslagbedrijven dat de basis vormt voor het toezicht. Deze is beperkt tot het deel dat relevant is vanuit de onderzoeksvraag: het Besluit risico's zware ongevallen 2015 (Brzo) en de Arbeidsomstandighedenwet en daaraan gerelateerde wet- en regelgeving. Er is overlap tussen beide wettelijke kaders: bepaalde ongewenste handelingen of situaties kunnen zowel een overtreding van het Brzo als van de Arbeidsomstandighedenwet zijn. Voor het Brzo zijn naast ISZW ook de Brzo-omgevingsdiensten, de veiligheidsregio's en Rijkswaterstaat (als waterkwaliteitsbeheerder) aangewezen als toezichthouder. Voor de Arbeidsomstandighedenwet is ISZW de toezichthouder.

Besluit risico's zware ongevallen 2015 (Brzo)

Vanwege de hoeveelheid gevaarlijke stoffen vallen petrochemische tankopslagbedrijven onder het Brzo.³ Het Brzo en de Regeling risico's zware ongevallen 2015 (Rrzo) hebben als doel het voorkomen en beheersen van zware ongevallen met gevaarlijke stoffen. Het Brzo is de implementatie van de Europese Seveso III-richtlijn (2012/18/EU). Het is te zien als doelregelgeving. Dit blijkt bijvoorbeeld uit artikel 5, lid 1:

De exploitant treft alle maatregelen die nodig zijn om zware ongevallen te voorkomen en de gevolgen daarvan voor de menselijke gezondheid en het milieu te beperken.

Het besluit stelt verder onder meer als eis dat een Brzo-bedrijf een veiligheidsbeheerssysteem heeft dat gebaseerd is op een evaluatie van de risico's en afgestemd is op de gevaren, de industriële werkzaamheden en de complexiteit van de organisatie. Het veiligheidsbeheerssysteem (VBS) moet zeven VBS-elementen bevatten.⁴

² Op peildatum 1 juni 2018 waren er 409 Brzo-bedrijven in Nederland (Bron: Brzo+).

³ Alle tankopslagbedrijven die lid zijn van de VOTOB vallen onder het Brzo. Ze vallen in de zwaarste categorie (de zogeheten hogedrempelinrichtingen).

⁴ i) De organisatie en het personeel, ii) De identificatie en beoordeling van de gevaren van zware ongevallen, iii) De controle op de exploitatie, iv) De wijze waarop wordt gehandeld bij wijzigingen, v) De planning voor noodsituaties, vi) Het toezicht op de prestaties en vii) Controle en analyse.

Artikel 5, lid 2 van het Brzo stelt verder:

De exploitant kan te allen tijde aantonen aan de aangewezen toezichthouders dat hij alle noodzakelijke maatregelen heeft getroffen.

Het goed inrichten van het VBS behoort tot deze noodzakelijke maatregelen.

Stelsel toezicht Brzo-bedrijven

Verschillende inspectiediensten en bevoegde gezagen zijn betrokken bij toezicht op Brzo-bedrijven. De 12 provinciebesturen zijn bevoegd gezag vanuit het milieudomein voor de Brzo-bedrijven in hun provincie. Zij hebben het toezicht en de handhaving gemandateerd aan zes Brzo-omgevingsdiensten. Naast het toezicht op het Brzo voeren deze Brzo-omgevingsdiensten ook het toezicht vanuit de milieuwetgeving uit (Wabo, Wet milieubeheer). De 25 veiligheidsregio's zijn verantwoordelijk voor het toezicht op de aangewezen bedrijfsbrandweren en de voorbereiding op de rampenbestrijding en crisisbeheersing. Naast de omgevingsdiensten en de veiligheidsregio's, is ISZW verantwoordelijk voor toezicht op het Brzo. Deze dienst houdt ook toezicht op de naleving van de Arbeidsomstandighedenwet bij Brzo-bedrijven.

Daarnaast houden Rijkswaterstaat en een deel van de 21 waterschappen toezicht op de waterkwaliteit. ISZW is, naast Rijkswaterstaat, de enige landelijk opererende Brzo-toezichthouder. Door de vele partijen met verschillende (deel)verantwoordelijkheden, waarvan sommige centraal, maar de meeste decentraal werken, is het toezicht complex en gefragmenteerd.⁵

Brzo+ en andere samenwerkingsverbanden

Om het toezicht en de handhaving op het Brzo te organiseren zijn er meerdere samenwerkingsverbanden. Op strategisch en tactisch niveau is het samenwerkingsprogramma Brzo+ van belang. Dit is een samenwerkingsprogramma van Brzo-omgevingsdiensten, ISZW, veiligheidsregio's, waterkwaliteitsbeheerders, ILT en het Openbaar Ministerie. Deze samenwerking leidt tot diverse producten zoals de Landelijke Handhavingsstrategie Brzo (zie hieronder), de Landelijke Benadering Risicobedrijven en de ranking van Brzo-bedrijven (zie paragraaf 3.5). De deelname van het Openbaar Ministerie richt zich met name op de aansluiting op en scheiding tussen de strafrechtelijke en de bestuursrechtelijke handhaving van het Brzo. De samenwerking op het gebied van opsporing vindt plaats binnen de Strategische Milieukamer en de gewone Milieukamer.⁶

Handhaving en de Landelijke Handhavingsstrategie Brzo

Zoals hierboven is aangegeven moet een Brzo-bedrijf altijd aan de toezichthouders kunnen aantonen dat het alle noodzakelijke maatregelen heeft getroffen. Dat betekent dat als niet op een correcte wijze uitvoering wordt gegeven aan een VBS, er in beginsel sprake is van een overtreding van het Brzo, artikel 5, eerste lid. Uit de jurisprudentie is een beginselplicht tot handhaving af te leiden. De beginselplicht houdt in dat als een bedrijf een wettelijk voorschrift overtreedt, het bevoegde bestuursorgaan daartegen dient op te treden. Voor de handhaving bij Brzo-bedrijven zoals de tankopslagbedrijven is de Landelijke Handhavingsstrategie Brzo leidend.

De gezamenlijke Brzo-toezichthouders hebben een Landelijke Handhavingsstrategie Brzo ontwikkeld.⁷ Elke Brzo-toezichthouder, zoals ISZW, provincies c.q. Brzo-omgevingsdiensten en de veiligheidsregio's, heeft zich gecommitteerd aan deze landelijk uniforme handhavingsstrategie.

⁵ Onderzoeksraad voor Veiligheid, Veiligheid Brzo-bedrijven, Lessen na Odfjell, 2 maart 2017, zie Bijlage E, pagina 146 voor een schematisch overzicht van het Brzo-stelsel.

⁶ Onderzoeksraad voor Veiligheid, Veiligheid Brzo-bedrijven, Lessen na Odfjell, 2 maart 2017.

⁷ LAT RB (nu: Brzo+), Landelijke Handhavingsstrategie Brzo, 14 januari 2013.

Deze beschrijft onder meer welke toezichthouder bij welke overtreding handhavend optreedt, en heeft als uitgangspunt dat er altijd een handhavingsactie volgt door de Brzo-toezichthouder(s) als er sprake is van een overtreding.

Wanneer een bedrijf op één of meerdere onderdelen volgens de NIM 2-systematiek (goed-redelijk-matig-slecht) een 'matig', of 'slecht' scoort, is er sprake van een overtreding en volgt handhaving. Er vindt afstemming plaats tussen de Brzo-toezichthouders over de overtredingen en de handhaving. De uiteindelijke handhaving wordt gedaan door één van de Brzo-toezichthouders: door ISZW, door de Brzo-omgevingsdienst of door de veiligheidsregio.

Handhaving is gedefinieerd als het toepassen van of dreigen met dwang in geval van geconstateerde niet-naleving gericht op een individueel geval.⁸ Het is te onderscheiden in strafrechtelijke handhaving en bestuursrechtelijke handhaving. Het doel van de inzet van handhaving in het kader van de Landelijke Handhavingsstrategie Brzo is:

- het beëindigen van de ongewenste situatie;
- het bestraffen van de overtreding, en
- het voorkomen van herhaling in de toekomst.

Handhaven is niet hetzelfde als sanctioneren. Ook het versturen van een waarschuwingsbrief valt onder handhaving. In een waarschuwingsbrief vraagt de toezichthouder de overtreder (de gevolgen van) een overtreding ongedaan te maken binnen een in de brief genoemde termijn en waarin ook wordt gemeld, dat een specifiek handhavingsinstrument kan worden ingezet als binnen de gestelde termijn geen gehoor is gegeven aan het verzoek om (de gevolgen van) een overtreding ongedaan te maken.

De inspecteurs van ISZW zijn buitengewoon opsporingsambtenaar waardoor zij de mogelijkheid hebben om overtredingen via het strafrecht aan te pakken. Via de route van het strafrecht raakt ook het Openbaar Ministerie (OM) betrokken. Het OM kan onafhankelijk van ISZW of de andere toezichthouders een eigen afweging maken ten aanzien van de inzet van het handhavingsinstrumentarium.

Gemeenschappelijke Inspectieruimte (GIR)

De Gemeenschappelijke Inspectieruimte (GIR) is het gezamenlijke informatieregistratiesysteem van de Brzo-toezichthouders. Het bevat onder meer per bedrijf de inspectieplanning, de bevindingen uit de aangekondigde Brzo-inspecties en de overtredingen. De GIR is in ontwikkeling en bevatte ten tijde van dit onderzoek nog niet alle inspectiegegevens, onder meer omdat er nog geen afspraken waren over het opnemen van gegevens uit onaangekondigde en niet-routinematige inspecties en bijvoorbeeld incidenten. Daarnaast is de registratie ook om andere redenen incompleet. De GIR is opgezet als registratie- en rapportagesysteem en voor de afstemming tussen verschillende Brzo-toezichthouders. Het is niet opgezet als 'datawarehouse' voor risicogerichte data-analyses. Een nieuw te bouwen informatiesysteem (nieuwe GIR) moet invulling geven aan de actuele wensen en eisen van de Brzo-toezichthouders. Beoogde veranderingen ten opzichte van de huidige GIR zijn (niet uitputtend):⁹

- Het eenmalig registeren van inspectiegegevens in de nieuwe GIR (en niet meer ook in eigen inspectiesystemen).
- Toename van volledigheid en betrouwbaarheid van inspectiegegevens (conform vastgelegde afspraken).

⁸ Ibidem.

⁹ Bronnen: interview projectleider LBR, Brzo+, Project Initiatie Document Landelijke Benadering Risicobedrijven (LBR), 23 februari 2016.

- De aansluiting tussen praktijk en theorie dient te worden verbeterd. Daarbij is de gebruikte beoordelingsterminologie niet altijd eenduidig waardoor soms verwarring ontstaat bij het invullen en interpretatie van gegevens.
- Standaardisering van de vastlegging van inspectieresultaten, waardoor deze gegevens gebruikt kunnen worden voor collectieve monitoring en benchmarking (data-analyse).

De oplevering van de nieuwe GIR is voorzien in 2019/2020.

3.3 Programmatisch en risicogestuurd toezicht op Brzo-tankopslagbedrijven

Het toezicht op Brzo-bedrijven, waaronder ook de tankopslagbedrijven, vindt plaats via een combinatie van een programmatische en een risicogestuurde aanpak. Het is een combinatie en een samenspel van vooraf (wettelijk of bestuurlijk) vastgestelde elementen en risicogestuurde elementen. Onderstaand lichten we dit toe aan de hand van de belangrijkste elementen.

Wettelijk kader

Het Brzo schrijft de inspectiefrequentie voor, dit is een bepalend element. De tankopslagbedrijven zijn vanwege de hoeveelheid gevaarlijke stoffen alle zogeheten hogedrempelbedrijven. Volgens het Brzo moet een hogedrempelbedrijf jaarlijks worden geïnspecteerd. Hiervan mag worden afgeweken wanneer er een inspectieprogramma wordt opgesteld op grond van een systematische evaluatie van de risico's op zware ongevallen die zich bij de bedrijven kunnen voordoen. Lagedrempelbedrijven moeten eens in de drie jaar worden geïnspecteerd.

Bestuurlijk inspectieprogramma en bestuurlijke keuzes

Het bevoegd gezag milieu, de ISZW en de veiligheidsregio stellen in beginsel gezamenlijk een bestuurlijk vastgesteld inspectieprogramma op.¹⁰ Vaststelling vindt in de regel plaats met de vaststelling van het provinciale handavingsprogramma. Het komt in de praktijk voor dat er verschillen zijn in de bestuurlijke prioriteiten van de drie toezichthouders. Bijvoorbeeld wanneer een provincie een Brzo-omgevingsdienst opdraagt om ook lagedrempelinrichtingen, die in een lagere risicocategorie vallen, elk jaar te inspecteren terwijl ISZW of de veiligheidsregio dit niet als prioriteit beschouwt. De inzet van toezichtcapaciteit is ook een bestuurlijke keuze. Specifiek voor ISZW speelt de capaciteit en beschikbaarheid van haar inspecteurs een rol. De beschikbare capaciteit is voor de Brzo-omgevingsdiensten en voor de veiligheidsregio's minder een issue. ISZW zet de beschikbare toezichtcapaciteit daar in waar men risico's verwacht en waar het verwachte effect van het toezicht het grootst is.¹¹ Het kan betekenen dat ISZW voor bepaalde bedrijven een andere afweging maakt dan bijvoorbeeld het bevoegd gezag milieu c.q. de provincie. Door de verschillende bestuurlijke afwegingen zijn er regionaal verschillen in de inzet van de verschillende inspectiediensten.¹²

Toezichtmodel

De gezamenlijke Brzo-toezichthouders bepalen voor elk Brzo-bedrijf het aantal inspectiedagen voor één inspectieteam dat ze in een bepaald jaar nodig achten met behulp van het zogeheten landelijk toezichtmodel.¹³ Het toezichtmodel is een instrument om de inspectiecapaciteit te bepalen en vormt daarmee een onderdeel van de inspectiemethodiek.

¹⁰ Bron: Brzo+, Proces 5. Opstellen bestuurlijk inspectieprogramma (BIP).

¹¹ Brzo+, Monitor naleving en handhaving Brzo-bedrijven 2017, 22 mei 2018.

¹² Brzo+, Monitor naleving en handhaving Brzo-bedrijven 2017, 22 mei 2018, p 17.

¹³ Toezichtmodel Brzo'99, 12 juni 2008.

Factoren die worden meegewogen in het toezichtmodel zijn de grootte, de complexiteit en de risico's van het bedrijf, in combinatie met het functioneren van het VBS. Met het toezichtmodel bepalen de inspectieteams per Brzo-bedrijf het gemiddeld aantal inspectiedagen per jaar. Afhankelijk van de omstandigheden maken ze een keuze hoe de dagen worden verdeeld over de tijd. De dagen kunnen worden verdeeld over bijvoorbeeld twee inspecties per jaar of worden gecombineerd tot een uitgebreidere inspectie. Het toezichtmodel zegt nog niets over de inhoud van de inspecties (zie hieronder bij Meerjareninspectieprogramma). Het huidige toezichtmodel is ongeveer tien jaar in gebruik en wordt momenteel herzien, omdat het verouderd is en niet meer voldoet.¹⁴ Het sluit onder meer niet meer aan op de nieuwe ontwikkeling van de inspectiemethodiek van Nieuwe Inspectiemethodiek 2 (NIM 2) naar de Landelijke Benadering Risicobedrijven (LBR), zie paragraaf 3.4.

Meerjareninspectieprogramma

Op basis van de wettelijk bepaalde toezichtfrequentie, bestuurlijke keuzes die al dan niet zijn vastgelegd in een bestuurlijk inspectieprogramma, de uitkomst van het toezichtmodel en de eigen inzichten vanuit de inspecties bepalen de diverse Brzo-inspectieteams per Brzo-bedrijf een meerjareninspectieprogramma. Dit meerjareninspectieprogramma is erop gericht om systematisch in een periode van vijf jaar alle VBS-elementen te inspecteren en ook de diverse installaties van het bedrijf aan bod te laten komen. Ten slotte zijn er ook specifieke thema's, zoals bijvoorbeeld 'ageing', die meegenomen worden in het meerjareninspectieprogramma. De Brzo-inspectieteams hebben de mogelijkheid om op basis van waarnemingen bij het Brzo-bedrijf het meerjareninspectieprogramma aan te passen. Dit kan na elke Brzo-inspectie.

Ranking van Brzo-bedrijven

Een relatief nieuw element in het Brzo-toezicht is de ranking van Brzo-bedrijven. In 2015 zijn de gezamenlijke Brzo-toezichthouders gestart met het opstellen van een ranking van alle Brzo-bedrijven. Er was bij hen behoefte aan een integraal vergelijkend beeld van veiligheidsrelevante informatie over de Brzo-bedrijven. Op basis van inspectieresultaten komen de Brzo-toezichthouders nu voor elk Brzo-bedrijf tot een score op de onderdelen VBS (vergelijkbaar met 'software' in de SMT), technische integriteit en toepassing stand van de techniek (vergelijkbaar met 'hardware' in de SMT) en veiligheidscultuur (vergelijkbaar met 'mindware' in de SMT, zie paragraaf 4.3). Op deze wijze is het voor de Brzo-toezichthouders duidelijk welke bedrijven relatief slecht en welke relatief goed scoren. De ranking is een aanvulling op het toezichtmodel, maar voor zover bekend is er geen procedure die de ranking eenduidig vertaalt naar de inhoud van de inspecties of inspectiecapaciteit. Brzo-bedrijven zijn in de regel op de hoogte van het bestaan van deze ranking, maar de uitkomst van de ranking is vertrouwelijk en hun absolute of relatieve positie op deze ranglijst wordt niet met hen gedeeld of anderszins openbaar gemaakt. De ranking is uitsluitend voor intern gebruik binnen het Brzo-toezicht. Het intersubjectief bepaalde beeld dient voor de toezichthouders als input voor risicogestuurd toezicht.

Risicoanalyses

Elk van de toezichthouders maakt eigen thematische risicoanalyses die input bieden voor de keuzes bij het Brzo-toezicht. Dit gebeurt door gespecialiseerde afdelingen, zowel centraal (ISZW) als decentraal (bevoegd gezag milieu, veiligheidsregio's). Er is op dit moment geen landelijke integrale Brzo-risicoanalysemethodiek. Ook is er niet een landelijk werkende organisatie die op basis van de risicodata input levert voor risicogestuurd toezicht op Brzo-bedrijven.

¹⁴ Programma Impuls Omgevingsveiligheid, Overzicht voor het jaar 2017, 1 november 2016.

3.4 Gewenste ontwikkelingen risicogestuurd toezicht

Ontwikkeling naar informatiegestuurd werken

De toezichthouders zijn bezig met het (verder) ontwikkelen van informatiegestuurd toezicht. Hierbij spelen onder meer de (door)ontwikkeling van de LBR (opvolger NIM 2) en de GIR een rol. Diverse betrokkenen geven aan dat een belangrijke stap is de doorontwikkeling van de GIR naar een database geschikt voor data-analyse. Een gezamenlijk Brzo-datalab zou vervolgens 'slimme' integrale data-analyses kunnen uitvoeren voor de Brzo-toezichthouders om het risicogestuurd toezicht verder te verbeteren.

Gebruik van bedrijfsinformatie door de toezichthouders

Toezichthouders maken bij inspecties nu al gebruik van door het bedrijf zelf geregistreerde informatie, zoals bijvoorbeeld een onderhoudsregistratie en auditinformatie. Een deel van deze informatie moeten bedrijven verplicht vastleggen (onderhoudsregistraties), andere informatie wordt op vrijwillige basis bijgehouden door het bedrijf. Alle voor toezicht relevante bedrijfsinformatie kan worden opgevraagd bij het bedrijf. Wanneer het bedrijf de informatie niet vrijwillig zou willen afstaan, hebben inspecteurs ook de bevoegdheid informatie te vorderen. Dit gebeurt zelden.

Discretionaire ruimte

In de interviews wordt aangegeven dat het wellicht mogelijk is om de Brzo-inspecteurs meer discretionaire ruimte te geven bij de beoordeling van een onwenselijke situatie en de daarop volgende aanpak bij een Brzo-bedrijf. Als er evident sprake is van een overtreding, dan volgt er handhaving. Maar als het een grijs gebied betreft en er is vertrouwen in het Brzo-bedrijf, bijvoorbeeld vanwege een aantoonbaar goede trackrecord (ranking), dan zou het meer aan de professionele inschatting van de inspecteur overgelaten kunnen worden welke aanpak leidt tot naleving en verbetering. Het kan betekenen dat situaties die door de inspecteurs voorheen als overtreding werden genoteerd, nu als tekortkoming worden genoteerd, met een bijpassende corrigerende aanpak. Een dergelijke ruimere invulling van de discretionaire ruimte vereist steun vanuit het management en het beleidsdepartement. Het vraagt ook om politiek-bestuurlijke bewustwording dat een Brzo-bedrijf weliswaar alle noodzakelijke maatregelen moet treffen, maar dat 100% veiligheid niet bestaat.

Andere ontwikkelingen maken onderdeel uit van de bredere ontwikkelingen in het Brzo-veld (zie paragraaf 3.5) en binnen het Programma Duurzame Veiligheid 2030 (zie paragraaf 3.6).

3.5 Ingezette ontwikkelingen binnen Brzo

Landelijke Benadering Risicobedrijven (LBR)

Een landelijke projectgroep LBR (Landelijke Benadering Risicobedrijven) ontwikkelt nu een nieuwe inspectiemethodiek voor Brzo-bedrijven. Deze nieuwe inspectiemethodiek (werktitel 'LBR') gaat de huidige NIM 2-methodiek vervangen, naar verwachting, in 2019. Onderdeel van de nieuwe inspectiemethodiek is een nieuwe versie van de GIR. De LBR is nog niet geïmplementeerd en de precieze opzet ervan is nog niet gepubliceerd. Dit maakt dat er op dit moment alleen uitspraken gedaan kunnen worden over de intenties en de wensen.

Het doel van de nieuwe inspectiemethodiek is dat het toezicht op en handhaving bij risicovolle bedrijven nog meer integraal, risicogestuurd en efficiënt wordt. Het betreft onder meer een verbreding van toezicht op het VBS (NIM 2) naar toezicht op het VBS, op techniek en op cultuur. Het is de bedoeling dat de toezichthouders met de LBR de inspectielast per bedrijf bepalen op basis van het risicopotentieel, de mate van veiligheidsbeheersing, cultuur en integriteit installaties alsmede naleefgedrag.

Hiermee zal met de LBR de risicogestuurde benadering op een bredere basis gestoeld zijn dan met de NIM 2-inspectiemethodiek. De inspecteurs en het management van de toezichthouders hebben onder meer de volgende wensen (niet uitputtend):¹⁵

- Toezicht door inspecteurs meer ter plekke bij het bedrijf (in plaats van administratief/op afstand).
- Niet meer dubbel registreren van toezicht- en handhavingsinformatie, dus niet zowel in de GIR als in een eigen systeem. De GIR wordt vervangen door een nieuw registratiesysteem.
- Het nieuwe registratiesysteem (nieuwe GIR) zal naast het VBS-deel, ook een techniekmodule (technische procesveiligheidsaspecten) en een cultuurmodule zal bevatten (30 vragen op basis van opzet door TNO). Het zal naar verwachting in september 2019 operationeel zijn.
- Vermindering van het aantal beoordelingskwalificaties.¹⁶
- Vereenvoudiging van het Brzo-inspectierapport. Met name het benoemen van zaken die op orde zijn kan compacter.

Meer gebruik van bedrijfsinformatie door de toezichthouders

De diverse gremia binnen de Brzo-samenwerking (onder meer de strategische klankbordgroep, het managementoverleg Brzo) zijn geïnteresseerd in uitbreiding van het gebruik van bedrijfsinformatie voor toezicht en handhaving.¹⁷ Zij signaleren allen een mogelijk knelpunt dat kan ontstaan wanneer inspectiediensten zouden handhaven direct naar aanleiding van vrijwillig afgestane bedrijfsinformatie. Er wordt erkend dat dit een negatief effect kan hebben op de bereidheid tot openheid en een werkbare toezichtsrelatie. Het vormt volgens meerdere geïnterviewden uit bedrijfsleven en inspectiediensten op dit moment een belemmering om het structureel gebruik van vrijwillig verzamelde bedrijfsinformatie in het toezicht nu al verder te ontwikkelen.

Nieuwe Landelijke Handhavingsstrategie Brzo

Bij de implementatie van de Landelijke Handhavingsstrategie Brzo in 2013-2014 was al een evaluatie voorzien. Sommige toezichthouders hebben zelf al een evaluatie gedaan. Op dit moment (2018) loopt de integrale evaluatie door het programma Brzo+. Deze evaluatie moet de basis leggen voor een nog op te stellen nieuwe Landelijke Handhavingsstrategie Brzo. De huidige strategie bevat nog geen richtlijnen over hoe toezichthouders omgaan met monitoringinformatie die (vrijwillig) door bedrijven wordt verstrekt, zoals de SMT, en die mogelijk zicht biedt op tekortkomingen.

3.6 Ontwikkelingen binnen Programma Duurzame Veiligheid 2030

Tijdens de High Level Conference over duurzame veiligheid in de (petro)chemische industrie op 14 september 2016 hebben overheid, bedrijfsleven en wetenschap besloten om structureel te gaan samenwerken. Centraal doel van deze samenwerking is het doel de veiligheid in de (petro)chemische sector duurzaam te hebben verbeterd in 2030.

¹⁵ Bronnen: interview projectleider LBR. Programma Impuls Omgevingsveiligheid, Overzicht voor het jaar 2017, 1 november 2016.

¹⁶ De NIM 2-classificatie in goed-redelijk-matig-slecht (zie paragraaf 3.2) wordt vervangen door een beoordeling in 'goed' of 'slecht', waarbij de kwalificatie 'slecht' inhoudt dat er sprake is van een overtreding. Ook de huidige driedeling 'geschikt', 'geïmplementeerd' en 'gedocumenteerd' zal met de nieuwe methodiek vervallen en worden vervangen door 'is het geschikt' en 'wordt het toegepast'. De huidige drie categorieën overtredingen blijven in stand (kort samengevat: 1. onmiddellijke dreiging, 2. geen onmiddellijke dreiging en 3. zeer geringe dreiging).

¹⁷ Dit is in februari 2018 in een themabijeenkomst van de Brzo-toezichthouders aan de orde gekomen. (Bron: interview projectleider LBR).

Hiertoe hebben de drie partijen het Programma Duurzame Veiligheid 2030 opgestart. Binnen dit programma is de weg naar 2030 uitgestippeld langs vijf roadmaps:

1. Duurzaam assetmanagement.
2. Integrale uitvoering van beleid.
3. Transparante en beveiligde chemiesector.
4. Ruimte voor (petro)chemieclusters.
5. Hoogwaardig kennissysteem chemie.

Het doel van Roadmap 3, het kader van voorliggende verkenning, is om in 2030:

- zodanig delen van informatie tussen bedrijven onderling en tussen bedrijven en overheid te hebben gerealiseerd dat daarmee de veiligheid duurzaam wordt verbeterd, en
- een zodanig niveau van transparantie naar de maatschappij te hebben gerealiseerd dat daarmee de maatschappelijk ervaren veiligheid duurzaam wordt verbeterd.

Binnen Roadmap 3 is een van de resultaatgebieden aangeduid als "Effectievere samenwerking tussen bedrijven en overheid op basis van transparantie en vertrouwen". Op basis van informatie die de bedrijven beschikbaar stellen, kunnen overheden hun taken op het gebied van beleidvorming, toezicht en kennisontwikkeling beter uitvoeren; taken die bijdragen aan gezamenlijke doelstellingen van de overheid en de bedrijven, zoals een veiligere chemiesector. Een cultuur van transparantie ligt hieraan ten grondslag, en hiervoor is een vertrouwensbasis nodig tussen bedrijven en overheid. Dit onderzoek naar het mogelijke gebruik van de SMT-informatie door de overheid valt binnen het genoemde resultaatgebied.

4. De Safety Maturity Tool (SMT)

4.1 Inleiding

In dit hoofdstuk wordt de SMT beschreven en vergeleken met de Landelijke Benadering Risicobedrijven (LBR, opvolger van NIM 2). De beschrijving van de SMT is gebaseerd op interviews met betrokkenen binnen de VOTOB en een vertegenwoordiger van het bedrijf dat heeft ondersteund bij de ontwikkeling van de SMT. Daarnaast is gebruik gemaakt van documentatie behorende bij de SMT en presentaties die de VOTOB heeft gegeven over de tool.

4.2 Aanleiding en doel van de SMT

In 2012 kampte de tankopslagterminal van Odfjell in Rotterdam met een onbeheerste veiligheidssituatie die ertoe leidde dat het bedrijf onder druk van de overheid de installaties stil legde. Het onderzoek van de Onderzoeksraad voor Veiligheid (2013) naar de incidenten, bracht aan het licht dat er sprake was van een structurele tekortkoming in de beheersing van de veiligheid en een slecht onderhoud aan de installaties van Odfjell.

Naar aanleiding van de stillegging bij Odfjell en de zeer negatieve publiciteit eromheen, besloten de leden van de VOTOB werk te maken van collectieve verbetering van de veiligheid in de branche. In 2012 stelden zij gezamenlijk het VOTOB Veiligheidsplan op. Als één van de onderdelen werd een assessment tool ontwikkeld.

Doel van de assessment tool is een meer transparant veiligheidsniveau in de individuele terminals en de sector als geheel. Deze transparantie moet bijdragen aan gezamenlijk leren voor een beter veiligheidsniveau. Daarom moeten de uitkomsten van de tool een basis bieden voor bedrijven om een verbeterplan op te stellen. Naast transparantie, heeft de VOTOB nog twee doelen met de ontwikkeling van de tool: het tonen van leiderschap op het terrein van veiligheid en tool om te kunnen communiceren met de toezichthoudende overheden.¹⁸

De ontwikkelde assessment tool kreeg de naam 'Safety Maturity Tool' (SMT). Er wordt gesproken van 'safety maturity' omdat de tool niet alleen inzicht moet bieden in het veiligheidsniveau van een bedrijf en de sector. De SMT moet ook laten zien hoe 'volwassen' een bedrijf omgaat met veiligheid. Deze keuze is gemaakt omdat de SMT een ontwikkelingsperspectief moet bieden voor bedrijven en de sector.

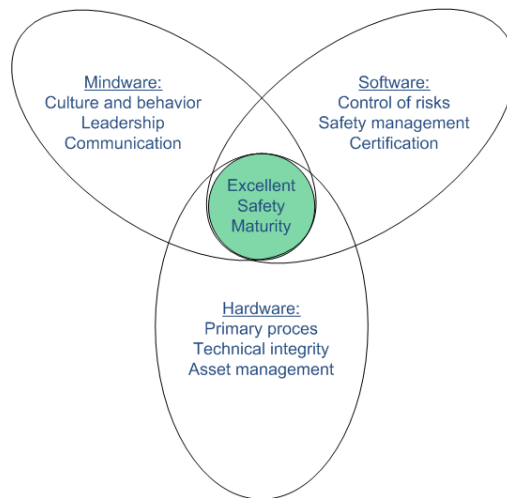
4.3 Onderdelen en onderbouwing van de SMT

Uitgangspunt van de SMT is dat veiligheid wordt gevormd door excellente bedrijfsvoering op drie complementaire onderdelen: de veiligheidscultuur (mindware), het veiligheidsbeheerssysteem (software) en de technische systemen (hardware)¹⁹.

De drie onderdelen zijn uitgewerkt naar 44 systeemelementen, gebaseerd op geldende regelgeving en andere dominante normeringssystemen. Deze elementen zijn vervolgens vertaald naar ongeveer 600 specifieke auditvragen.

¹⁸ VOTOB, S. de Bont, Safety Maturity Tool, the next step for improving safety performance, European Oil Storage Conference, juli 2013.

¹⁹ Er zijn geen verwijzingen aangetroffen naar documenten die deze benadering verder onderbouwen zoals wetenschappelijke inzichten of onderzoek.



Figuur: de drie elementen van de volwassen bedrijfsvoering

De elementen in de mindware zijn ontleend aan²⁰:

1. Hearts en Minds, lijst van onderwerpen die gebruikt wordt voor de module "Het begrijpen van uw cultuur".
2. TNO cultuurdimensies, de dimensies die TNO heeft gebruikt bij het vaststellen van het veiligheidscultuurniveau bij tankopslagbedrijven.

De elementen in de software zijn gebaseerd op een analyse van:

1. Veiligheidsbeheerssysteem (VBS) in het kader van het Brzo en conform de NTA 8620. Bij de onderverdeling in de systemen in gebruik gemaakt van de Aandachtspuntenlijst VBS die beschikbaar is op de website www.brzoplus.nl.
2. OHSAS 18001:2007, eisen aan een Arbomanagementsysteem.
3. BP Operating Management Systeem, het management systeem dat BP toepast.
4. Shell HSE management systeem, het management systeem dat Shell toepast.
5. CDI-T questionnaire 5th edition, deze vragenlijst wordt gebruikt binnen de branche voor het toetsen of wordt voldaan aan de belangrijkste (veiligheids- en gezondheids-)eisen.
6. ISO 55001, de internationale standaard voor asset management.

De elementen in de hardware zijn gebaseerd op een analyse gemaakt van:

1. Kennis opgedaan gebeurtenissen in de sector in 2012 (de aanleiding voor I2T project van de DCMR²¹ en het Landelijk Project Tankopslagsector).
2. Risico-indicatoren in de technische staat van het bedrijf die niet naar voren komen uit de analyse van eerdere incidenten maar waarvan wordt verwacht dat deze relevant zouden kunnen worden.

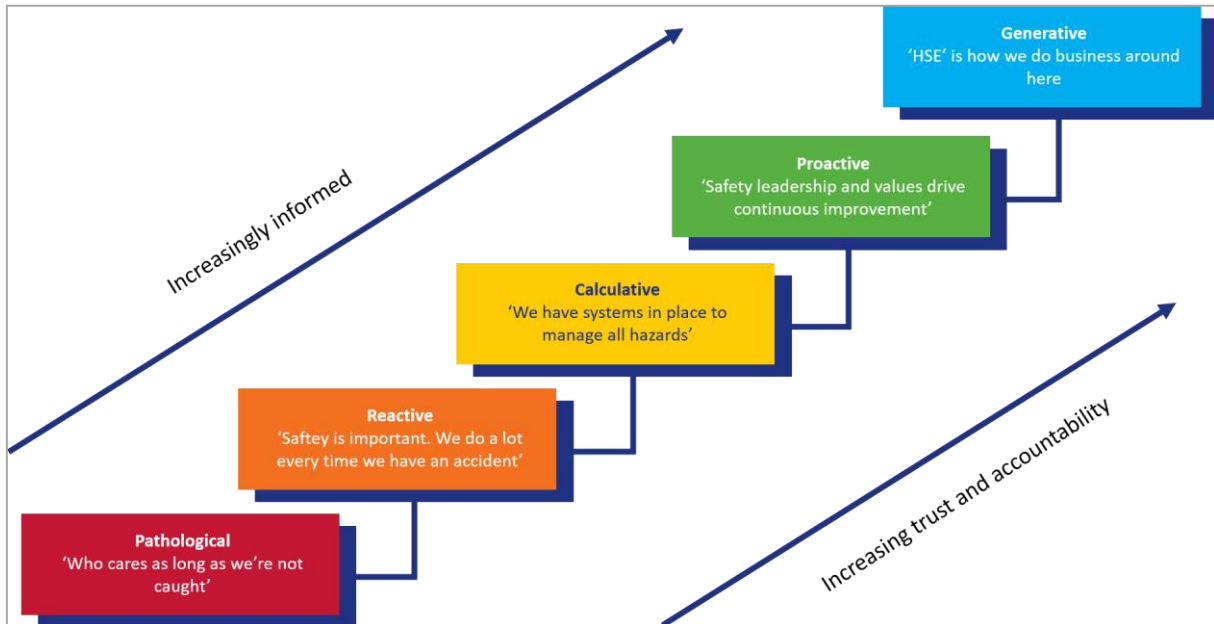
Het beoordelingssysteem in de SMT is gebaseerd op de principes van Parker, Lawrie en Hudson²². Zij hebben verschillende ontwikkelingsstadia benoemd voor de veiligheidscultuur van een bedrijf.

²⁰ RoyalHaskoningDHV, SMT Achtergrondrapportage, MD-AF20140948, september 2014.

²¹ DCMR in samenwerking met Veiligheidsregio Rotterdam Rijnmond en de Inspectie SZW, project I2T (Intensivering Inspectie Tankopslag), 2012.

²² Parker, D., M. Lawrie and P.T.W. Hudson. 2006. A framework for understanding the development of organisational safety culture.

Deze ontwikkelingsstadia zijn, in de theorie van Parker, Lawrie en Hudson, bepalend voor de wijze waarop het bedrijf met veiligheid omgaat.



Figuur: de veiligheidsladder van Parker, Lawrie en Hudson

De vijf ontwikkelingsfasen van de veiligheidscultuur van Parker, Lawrie en Hudson zijn ook vertaald naar een beoordelingsschaal voor hardware en software. Door alle elementen te beoordelen op deze vijf ontwikkelstadia (in een schaal van 1 tot en met 5), ontstaat een totaal beeld van de volwassenheid van een bedrijf in relatie tot de veiligheid. Niveau 3 betekent dat het bedrijf voldoet aan relevante regelgeving waaronder het Brzo.

Volwassenheid	0% 20%	40%	60%	80%	100%
Aspect	1 Slecht	2 Matig	3 Redelijk	4 Goed	5 Uitstekend
Mindware	Wat maakt het uit zolang we niet gepakt worden.	Veiligheid is belangrijk, we doen er veel aan telkens wanneer we een ongeluk hebben.	We hebben systemen om alle gevaren te hanteren	Leiderschap en waarden op het gebied van veiligheid zijn de motor achter continue verbeteringen.	VGWM is hier onze manier van zaken doen.
Software	Essentiële procedures en systemen van een management systeem ontbreken	Onderdelen van het managementsysteem zijn deels beschreven.	Onderdelen van het managementsysteem zijn beschreven in procedures en instructies.	De onderdelen van het managementsysteem zijn volledig geïmplementeerd.	De onderdelen van het management systeem worden continu gereviewed en verbeterd.
Hardware	De veroudering is onomkeerbaar. Technisch rijp voor sloop.	De veiligheid van de installatie is incidenteel in gevaar.	Plaatselijk zichtbare veroudering. Veiligheid van de installatie is niet in gevaar.	Incidenteel beginnende veroudering.	Geen gebreken.

Figuur: de SMT-beoordelingsschaal²³

²³ VOTOB, S. de Bont, Volwassen Kijk op Veiligheid, 2015.

4.4 Gebruikers en uitvoering van de SMT

De SMT wordt gebruikt door alle 18 leden van de VOTOB. Dit is voorwaarde voor lidmaatschap. Alle leden zijn (petro)chemische tankopslagbedrijven. Zij zijn verantwoordelijk voor 28 terminals in Nederland die alle onder het Brzo vallen.

De SMT-audit bestaat uit de beantwoording van de vragen van de SMT. Deze vragen zijn zo geformuleerd dat deze ook kunnen worden beantwoord door bedrijven zonder ondersteuning van de externe auditor of expert. De gedachte hierachter is dat bedrijven goed kunnen doorgronden wat de norm is in de vragen.

De SMT-audit wordt jaarlijks door externe auditors uitgevoerd bij alle bij de VOTOB aangesloten terminals. De mindware en software wordt geauditeerd door RoyalHaskoningDHV, mede betrokken bij de ontwikkeling van de SMT. De hardware wordt geauditeerd door KIWA.

De audit duurt (voor de meeste terminals) in totaal 3 dagen. De eerste dag van de audit is de audit op hardware. De auditor²⁴ beoordeelt de technische veiligheid van drie door het bedrijf geselecteerde tanks. Hij doet dit aan de hand van ongeveer 250 vragen die met ja of nee moeten worden beantwoord. De geselecteerde tanks worden op papier en 'buiten' beoordeeld door een visuele inspectie en met vragen aan medewerkers van het bedrijf.

De twee laatste dagen van de audit worden besteed aan de beoordeling van de software. Deze wordt beoordeeld door controle van documenten en bevraging van medewerkers. De audit van de software wordt uitgevoerd aan de hand van ongeveer 350 vragen.

De mindware, tot slot, wordt uitgevoerd door een bedrijfsbrede enquête gebaseerd op de Hearts and Minds methodiek. Alle medewerkers en managers in het bedrijf ontvangen een vragenlijst waarin uiteenlopende vragen staan die inzicht bieden in de veiligheidscultuur. De antwoorden worden anoniem verwerkt en geanalyseerd op verschillende elementen.

De SMT geeft een overzicht van de stand van zaken van een groot aantal veiligheidsaspecten in een bedrijf en inzicht in de elementen waarin verbetering nodig is. Omdat de audits sinds 2013 worden uitgevoerd, krijgen bedrijven ook inzicht in hun eigen ontwikkeling.

De SMT biedt minder inzicht in de veiligheid op detailniveau. Daarom hebben de leden van de VOTOB in 2017 besloten de SMT aan te vullen met verdiepingsmodules. Deze verdiepingsmodules kunnen bedrijven kiezen in ruil voor de brede SMT-audit, maar alleen op elementen waar zij in de eerdere audit hoger dan een 4 hebben gescoord. Overigens kan slechts een beperkte selectie van elementen in de audit worden vervangen door een verdiepingsmodule. Het gaat om een selectie van software-elementen waarvan bekend is²⁵ dat wanneer die eenmaal op orde zijn, ze niet van het ene op het andere jaar sterk verslechteren. Voorbeelden van deze zogenaamde 'performance based systeemelementen' zijn: het veiligheidsbeleid, de veiligheidseisen en de veiligheidsdoelstellingen.

²⁴ Auditors worden niet specifiek geaccrediteerd voor de SMT omdat het geen geaccrediteerd beoordelingssysteem is. Voor SMT-audits, zet RoyalHaskoningDHV senior-adviseurs in gespecialiseerd in veiligheidssystemen. Dit zijn inhoudelijk specialisten met veel ervaring op de Brzo en veel kennis van de chemie en de sector.

²⁵ Dit is besloten op basis van ervaring. De bedrijven die bepaalde elementen een jaar mogen overslaan, zitten gemiddeld op niveau 4. De elementen die zij mogen overslaan zijn verplichte documenten die, als zij er eenmaal zijn, wel blijven. Voorbeelden zijn de beschrijving van het beleid en de aanpak van interne audits.

Er is voor gekozen deze verdiepingsmodules toe te voegen aan de SMT-audit om de effectiviteit van de audit te verhogen door bedrijven eigen keuzes te laten maken voor de verdiepingsmodules²⁶. Door zelf focus aan te kunnen brengen in de verdiepingsmodules, kan worden gekozen voor elementen waar de leerbehoefte van het bedrijf het grootst is en die goed aansluiten bij verbeteringen die het bedrijf wil doorvoeren. Gedachte hierbij is zo ook 'audit moeheid' te voorkomen die ontstaat wanneer bedrijven steeds dezelfde vragen moeten beantwoorden zonder zinvol leereffect.

Voor de verdiepingsmodules wordt maximaal een halve dag van de audittijd uitgetrokken om, onder leiding en in aanwezigheid van de auditor, verschillende onderwerpen te bespreken in teamverband. De keuze voor deze aanpak wordt als volgt toegelicht: "Door te discussiëren over de onderwerpen ontstaat een nog realistischer en voor de terminalmedewerkers een meer gedragen beeld van de besproken onderwerpen."²⁷ Wat wordt verstaan onder 'meer gedragen' wordt niet nader toegelicht.

Alle bedrijven ontvangen een rapport van de eigen audit. In het rapport krijgen zij een analyse van de laatste resultaten en een analyse van hun ontwikkeling sinds 2013. Voor alle elementen waarop een bedrijf lager dan 3 scoort, zo hebben de VOTOB-leden met elkaar afgesproken, moet het bedrijf een verbeterplan opstellen en uitvoeren. Het bestuur van de VOTOB ontvangt een afschrift van de verbeterplannen. De bureaustaf van de VOTOB controleert de score-ontwikkeling op de afgesproken normen.

In een gezamenlijke bijeenkomst wordt ook de vergelijking tussen bedrijven besproken. In deze bijeenkomst worden de resultaten van alle bedrijven gepresenteerd en naast elkaar gelegd. Deze vergelijking is niet anoniem. Deze gezamenlijke bijeenkomst heeft een aantal doelen:

- De VOTOB-leden bespreken de uitkomsten en de belangrijke leerpunten uit de audits.
- De VOTOB-leden stellen gezamenlijk vast welke bedrijven extra aandacht moeten geven aan de veiligheid om op een hoger niveau te komen.
- De leden bespreken het verloop en mogelijke verbeteringen in de SMT.

Bedrijven die te laag scoren op onderdelen, kunnen hulp vragen aan andere leden bij het formuleren van verbeterplannen en voor advies over implementatie. VOTOB-leden hebben afgesproken dat de gevraagde hulp in principe wordt verleend.

In 2017 hebben de VOTOB-leden met elkaar afgesproken dat alle leden op alle onderdelen gemiddeld minimaal een 3,0 moeten scoren. Leden die structureel achterblijven, kunnen geroeyeerd worden als lid.

4.5 De werking van de SMT

Zoals gezegd worden de SMT-audits sinds 2013 uitgevoerd. In 2017 zijn de resultaten van de SMT over de periode 2013–2017 geanalyseerd. De analyse laat zien dat de individuele terminals zich verbeteren op hardware en software. De prestaties op mindware blijven ongeveer gelijk.

²⁶ In de verdiepingsmodules worden meer mensen betrokken bij het vaststellen van het veiligheidsniveau en het formuleren van verbeteringen. Dit gebeurt door gespreksrondes over specifieke onderwerpen begeleid door de auditor. Door meer mensen te betrekken, ontstaat beter inzicht en worden breder gedragen verbeteringen geformuleerd. Groter draagvlak biedt meer zekerheid dat verbeteringen ook worden doorgevoerd en toegepast, is de redenering.

²⁷ RoyalHaskoningDHV en KIWA, Safety Maturity Tool Audits, Resultaten SMT audits (versie 1.0), 4 oktober 2017, blz. 9.

Over de specifieke prestaties op hardware is geconstateerd dat:

- De prestaties van de individuele terminals zijn verbeterd van de laagste met ongeveer een 2,5 (op de gehanteerde 5-puntschaal) in 2014 naar de laagste met ongeveer een 3,5 in 2017.
- De mediaan van de prestaties is omhoog gegaan van ongeveer 3 in 2013 naar ongeveer 3,7 in 2017.

De evaluatie heeft over de ontwikkelingen op software uitgewezen dat:

- De prestaties van de individuele terminals zijn ook op software gestegen van de laagste met ongeveer een 2,8 (op de gehanteerde 5-puntschaal) in 2013 naar de laagste met ongeveer een 3,5 in 2017.
- De mediaan²⁸ van de prestaties is omhoog gegaan van ongeveer 3,5 in 2013 naar ongeveer 4,5 in 2017.
- Het niveau van de individuele terminals is steeds dichterbij elkaar gekomen variërend van ongeveer een 3,4 tot ongeveer 4,7 in 2017. Dit verschil was het grootst in 2014 met een variatie van ongeveer 2,5 tot ongeveer 4,5.

In de evaluatie wordt geen nadere verklaring gegeven voor de ontwikkeling van de scores. Ook worden geen nadere acties geformuleerd op de geconstateerde ontwikkelingen.

4.6 Draagvlak voor de SMT en het gezamenlijk streven naar meer veiligheid

Draagvlak wordt in deze verkenning afgemeten aan de volgende elementen in het gebruik van de SMT:

1. De mate waarin VOTOB-leden gebruikmaken van de SMT.
2. De mate waarin VOTOB-leden hebben meegewerkt aan de ontwikkeling van de SMT.
3. De mate van medewerking van de terminals bij de audits.

De volgende informatie is gebaseerd op de evaluatie van de SMT²⁹ en de interviews met enkele leden en vertegenwoordigers van de VOTOB. Daarnaast is in de interviews verkend wat bijdraagt aan het draagvlak voor de SMT.

De SMT wordt door alle leden van de VOTOB gebruikt. Dit is een voorwaarde voor lidmaatschap. Uit de interviews komt het beeld naar voren dat de meeste leden van de VOTOB achter de beoogde doelen en vorm van de SMT staan. Dit beeld wordt onderstreept met het recente besluit van de leden, bedrijven die achterblijven in de scores op de SMT geroyeerd kunnen worden als lid van de VOTOB.

Dit draagvlak is ontstaan door het brede besef van de leden dat de tankopslagbranche moest laten zien dat zij veilig wil werken. Daarnaast is de SMT ontwikkeld in nauw overleg met de leden van de VOTOB. Zij waren vertegenwoordigd in de stuurgroep en de technische werkgroepen die de uitwerking van (onderdelen van) de SMT moesten beoordelen en aanscherpen. Ook nu nog worden aanpassingen in de SMT bedacht en vastgesteld met de leden.

²⁸ De mediaan is de middelste waarde in een reeks getallen die gerangschikt zijn naar grootte. Dat wil zeggen dat 50% van de getallen onder de mediaan ligt en 50% van de getallen onder de mediaan.

²⁹ RoyalHaskoningDHV en KIWA, Safety Maturity Tool Audits, Resultaten SMT audits (versie 1.0), 4 oktober, 2017.

Uit de evaluatie van de SMT in 2017 blijkt dat het draagvlak bij de VOTOB-leden niet automatisch tot uitdrukking komt bij de individuele terminals. Er wordt geconstateerd dat audits niet altijd goed worden voorbereid door de terminals en de deelname aan de sessies voor de verdiepingsmodules soms ook achterblijft. Dit wordt beschouwd als een verbeterpunt voor de SMT.

Tot slot wordt in de interviews aangegeven dat het draagvlak bij sommige leden van de VOTOB groter is dan bij andere leden. Dit verschil wordt verklaard op basis van de markt die leden bedienen. Leden die klanten hebben met veiligheid hoog in het vaandel zoals de grote petrochemische bedrijven, investeren zelf ook in veiligheid. Deze klanten vinden transparantie over veiligheid ook positief omdat zij zo kunnen laten zien dat zij het goed doen. Tankopslagbedrijven die vooral handelaren als klanten hebben, werken met lage marges en hebben klanten die veiligheid minder belangrijk vinden. Vooronderstelling is dat deze leden daarom minder zullen investeren in de veiligheid. Dit laatste is overigens niet getoetst in deze verkenning.

4.7 Vergelijking van de SMT met Landelijke Benadering Risicobedrijven (Brzo-aanpak)

In deze verkenning zijn de SMT en de Landelijke Benadering Risicobedrijven (LBR, opvolger van de NIM) vergeleken op hoofdlijnen. Dit is gedaan op grond van een beperkte documentenanalyse. Daarnaast is alle geïnterviewden gevraagd naar overeenkomsten en verschillen tussen de SMT-audit en de Brzo-inspectiemethodiek.

Belangrijkste overeenkomst tussen de SMT en het LBR zijn de onderwerpen van de inspectie: de SMT onderzoekt dezelfde onderwerpen als worden onderzocht in een Brzo-inspectie. Beide gaan in op de software (het VBS), de hardware (de technische veiligheid) en de mindware (de veiligheidscultuur). De onderdelen software en hardware in de SMT zijn onder andere gebaseerd op alle vigerende regelgeving voor tankopslagbedrijven, waaronder het Brzo. Deze wet- en regelgeving inclusief alle aspecten van het Brzo, is geoperationaliseerd naar auditvragen in de SMT. Het onderdeel mindware is gebaseerd op dezelfde methode als de TNO Cultuurscan die wordt gehanteerd in het kader van Brzo-toezicht.

Belangrijkste drie verschillen die geïnterviewden noemen tussen de SMT en toezicht op basis van het Brzo zijn (1) het doel, (2) de aanpak van inspectie en (3) de ingezette capaciteit voor het toezicht.

De SMT-audit heeft als doel een breed en algemeen overzicht te geven van de stand van de veiligheid in een bedrijf door op alle relevante punten in te gaan. Daarnaast heeft de SMT tot doel het individuele bedrijf en de leden van de VOTOB te ondersteunen bij het leren ten behoeve van de veiligheid.

Toezicht op basis van het Brzo is gericht op toetsing van de naleving van het Brzo. Daarbij gaat het niet in de eerste plaats om een algemeen overzicht maar op inzicht in de naleving op de belangrijkste risico's vastgelegd in de inspectie-agenda.

Ook de aanpak van de SMT en het Brzo-toezicht verschilt. Niet alles wordt in de SMT even diepgaand getoetst omdat het doel is het krijgen van een overzicht. Een aantal onderdelen worden wel gecontroleerd op de werkvloer, maar dit is niet de hoofdmoot van de audit. Gedachte hierachter is dat bedrijven zo een goed beeld krijgen van het veiligheidsniveau in het bedrijf over de hele linie en kunnen acteren op die elementen waar verbetering nodig is. Daarnaast is gezocht naar een aanpak waarin een goed evenwicht is aangebracht tussen de (capaciteits-)kosten van de audit enerzijds en de opbrengsten in termen van inzicht anderzijds.

Een ander verschil in aanpak tussen de SMT en toezicht in het kader van het Brzo, betreft de aanpak van toezicht op de hardware en mindware. Bij de audit van de hardware, inspecteert de SMT-auditor drie tanks die door de auditor zijn geselecteerd. Het betreft een tank net vóór onderhoud, een tank in onderhoud en een tank na onderhoud.

In een Brzo-inspectie bepalen de inspecteurs op een andere manier welke installaties zij inspecteren (zie paragraaf 3.3). Het voor elk Brzo-bedrijf door de gezamenlijke Brzo-toezichthouders opgestelde meerjareninspectieplan (MIP) vormt de leidraad. Net als bij een SMT-audit, zijn het de inspecteurs die de te inspecteren tanks selecteren. Het is niet per definitie een drietal tanks zoals bij de SMT. De inspectie kan ook een bepaald aspect betreffen dat voor meerdere tanks wordt onderzocht.

Tot slot wordt de mindware anders onderzocht. Terwijl de cultuurscan in de SMT-audit wordt uitgevoerd door middel van een enquête, wordt deze in de Brzo-inspectie uitgevoerd op basis van een gezamenlijke beoordeling door Brzo-inspecteurs aan de hand van een speciaal daarvoor ontwikkeld instrument (NIM inschattingmodule voor Veiligheidscultuur). Dit instrument bestaat uit 30 cultuurvragen, gevalideerd door TNO. De beoordeling wordt gedaan op basis van vraaggesprekken, observaties en bevindingen tijdens de inspectie.

Een inspectie in het kader van het Brzo is a priori specifiek en diepgaander, aldus geïnterviewden. Dit geldt vooral op twee punten: de technische inspectie van de installaties en inspectie van specifieke onderdelen van het VBS, zoals bijvoorbeeld de scenario-inspectie waar diepgaander wordt onderzocht of de ongevalsscenario's voor installaties op papier ook daadwerkelijk zijn geïmplementeerd. Naast dat naar de documentatie gekeken wordt, wordt de werking van een maatregel nagegaan (geschikt) en of de maatregel daadwerkelijk aanwezig is (geïmplementeerd).

Dat een Brzo-inspectie diepgaander is, hangt samen met het derde verschil: de beschikbare capaciteit. Terwijl de SMT-audit door één auditor in drie dagen wordt uitgevoerd, wordt een Brzo-inspectie doorgaans in een team van meerdere inspectiemedewerkers uitgevoerd in evenveel dagen, met uitschieter naar 12. Dit maakt het mogelijk méér te inspecteren dan in een SMT-audit.

5. SMT in toezicht

5.1 Inleiding

In dit hoofdstuk wordt ingegaan op de mogelijkheden, de risico's en de voorwaarden voor gebruik van SMT-informatie en kennis over SMT-instrumenten in het Brzo-toezicht. Daarin is vooral gekeken naar gemeenschappelijke beelden hierbij van de geïnterviewde vertegenwoordigers van de toezichthouders en de vertegenwoordigers en leden van VOTOB.

5.2 Verkende mogelijkheden van gebruik SMT-informatie in risicogestuurd toezicht

Onderscheid tussen drie niveaus van transparantie

In de gesprekken is verkend welke mogelijkheden geïnterviewden zien voor het beschikbaar stellen van informatie uit de SMT. Bij verkenning van de mogelijkheden en de daarbij behorende risico's en voorwaarden, onderscheiden de geïnterviewden drie niveaus van transparantie:

- Informatie op het niveau van de individuele terminals. In dat geval zou informatie uit de SMT worden gebruikt per terminal waarbij precies duidelijk is over welke terminal het gaat.
- Informatie op het niveau van individuele niveau van terminals maar zonder dat precies bekend is over welke terminal het gaat. Informatie uit de SMT waaruit kan worden opgemaakt over welke terminal het gaat, wordt uit de SMT verwijderd.
- Informatie uit de SMT als samenvatting van alle leden. Informatie wordt dan voor de hele groep samengevat en zo ter beschikking gesteld aan de toezichthouder.

Alle geïnterviewden zijn het er over eens dat naarmate de informatie meer inzicht biedt in de stand van de veiligheid in een individuele terminal, deze informatie meer mogelijkheden biedt in het toezicht en in het gezamenlijk leren van veiligheid. Ook kan informatie uit de SMT beter en preciezer worden gecombineerd met andere informatie uit het toezicht.

Mogelijkheden van het gebruik van de SMT en SMT-informatie

Geïnterviewden zien verschillende mogelijkheden voor het gebruik van SMT-informatie in het toezicht:

Mogelijkheid 1: Gebruik van informatie bij het inrichten van het toezicht, meer focus

Door de SMT-informatie te combineren met de informatie uit het toezicht, kan (nog) specifiekere worden vastgesteld welke risico's de meeste aandacht vragen bij individuele terminals en bij gezamenlijke leden van de VOTOB. Dit inzicht zou ondersteunend kunnen zijn bij het prioriteren van het Brzo-toezicht en het vaststellen van de toezichtagenda. Door deze prioritering zou de beschikbare capaciteit voor toezicht meer efficiënt kunnen worden ingezet.

Tegelijkertijd zou een effectieve focus van toezicht op de risico's ook nuttig kunnen zijn voor SMT-gebruikers. Wanneer toezicht zich focust op de risico's die blijken uit de SMT-informatie en toezicht meer informatie oplevert over de aard van deze risico's, kunnen bedrijven deze informatie benutten voor het ontwerp en de implementatie van beheersmaatregelen. Ook zou dit een extra stimulans kunnen zijn voor SMT-gebruikers snel en effectief werk te maken van de risico's die in de SMT-audit zijn vastgesteld.

Mogelijkheid 2: Kennisdelen en uitwisselen best practices vergroot inzicht en ontwikkeling beste methodes

Tweede mogelijkheid die alle geïnterviewden onderkennen is dat door het delen van informatie uit de SMT en deze te matchen met informatie uit het Brzo-toezicht van elkaar kan worden geleerd over de beste methodes om inzicht te krijgen in de veiligheid van een bedrijf. Zoals in hoofdstuk 4 toegelicht, worden in de SMT en het Brzo-toezicht verschillende methodes gehanteerd. Vooral bij het onderzoek naar de mindware, is vanuit het Brzo-toezicht belangstelling voor de aanpak in de SMT.

Maar ook de matching van informatie uit de SMT en informatie uit Brzo-toezicht zou eraan bij kunnen dragen de beide methodes te verbeteren. Want door een vergelijking van informatie uit de twee methodes kan worden vastgesteld of methodes een vergelijkbaar beeld opleveren of dat er verschillen zijn. Door verschillen nader te onderzoeken, kunnen methodes worden verbeterd om een scherper, meer vergelijkbaar beeld te krijgen. Het is zinvol om de uitkomsten van de SMT-audits te vergelijken met de Brzo-ranking om te beoordelen hoe SMT-informatie aansluit bij informatie uit Brzo-toezicht.

Mogelijkheid 3: Efficiënter delen van informatie voor toezicht door gebruik van SMT-informatie

Een derde mogelijkheid is het gebruik van SMT-informatie in toezicht ter vervanging van informatie die bedrijven nu, los van de SMT, beschikbaar moeten stellen aan Brzo-toezichthouders. Volgens geïnterviewde gebruikers van de SMT, overlapt de informatie uit de SMT voor een deel met de informatie die door Brzo-toezichthouders wordt opgevraagd.

5.3 Voorwaarden voor gebruik van SMT in risicogestuurd toezicht

Uit de interviews komt een aantal belangrijke voorwaarden naar voren om informatie uit de SMT goed te kunnen benutten voor Brzo-toezicht:

- Het delen en gebruiken van SMT-informatie en kennis over het instrument verandert de verdeling van rollen en verantwoordelijkheden van toezichthouders en bedrijven niet: bedrijven zijn verantwoordelijk voor de veiligheid in bedrijven, toezichthouders zijn verantwoordelijk voor toezicht en handhaving op naleving van het Brzo in het belang van de veiligheid. Dit betekent dat het delen van SMT-informatie geen verkeerde verwachtingen moet wekken over de wijze waarop toezichthouders hun rol vervullen en dus optreden tegen overtredingen van het Brzo. De VOTOB-leden blijven verantwoordelijk voor de veiligheid in hun bedrijven en de kwaliteit van de SMT.
- Het delen van de informatie uit de SMT is geen wijziging van de toezichtrelatie tussen Brzo-toezichthouders en VOTOB-leden omdat het delen van de SMT-informatie en kennis over het instrument zichtbaar het gemeenschappelijk belang van de toezichthouders en de VOTOB-leden dient. Daarom is het nodig dat het delen van SMT-informatie:
 - zichtbaar bijdraagt aan een meer veiligheid bij VOTOB-leden door effectiever toezicht, meer handvatten voor adequate risicobeheersing en een extra impuls voor VOTOB-leden om de risico's geïdentificeerd met de SMT, zo snel mogelijk te verbeteren;
 - geen negatief effect heeft op het level playing field voor VOTOB-leden omdat zij zich kwetsbaar opstellen door hun transparantie;
 - het delen van de SMT-informatie en inzicht in het instrument gepaard gaat met kennisdeling vanuit de Brzo-toezichthouders over hun instrumenten en hun kennis van risico's;
 - zorgt voor erkenning bij Brzo-toezichthouders dat VOTOB-leden een positieve ontwikkeling hebben ingezet door het gebruik van de SMT en zich te conformeren aan de eisen die dit stelt aan VOTOB-leden.

- De informatie uit de SMT-audits moet betrouwbaar inzicht bieden in het veiligheidsniveau van een terminal. Alleen wanneer de informatie van goede kwaliteit is, is deze bruikbaar als input voor risicogestuurd toezicht.
- De wijze waarop de SMT-audits worden uitgevoerd moet van goede kwaliteit en consistent zijn zodat informatie uit de SMT ook over jaren een betrouwbare bron is voor risicogestuurd toezicht.
- De normen in de SMT moeten goed aansluiten bij de normen gesteld in het Brzo. Als er een te grote discrepantie is, is de informatie uit de SMT minder nuttig voor het toezicht op het Brzo. Dit is vooral belangrijk om de informatie uit de SMT te kunnen duiden binnen de kaders van het Brzo-toezicht en, vanuit die kaders, te bepalen wat de informatie betekent voor het toezicht op de Brzo-bedrijven.
- Het delen van de SMT-informatie mag geen ingrijpend effect hebben op het oorspronkelijk doel van de SMT voor de VOTOB-leden: gezamenlijk leren ten behoeve van de veiligheid door onderlinge transparantie en hulp. Dit doel kan op de achtergrond raken wanneer leden van de VOTOB vrezen voor meer handhaving als gevolg van de transparantie. Zij moeten ervan overtuigd raken dat delen van SMT-informatie daadwerkelijk bijdraagt aan meer effectieve en efficiënte zorg voor veiligheid.

Naast deze voorwaarden direct van toepassing op het gebruik van SMT-informatie en kennis over het instrument, wordt ook als voorwaarde gesteld dat de ontwikkeling van het gebruik van dit type informatie in het Brzo-toezicht, op termijn, kan worden uitgebreid naar een grotere groep Brzo-bedrijven. Want wanneer dit niet het geval is, is het de vraag of de groep VOTOB-leden niet te klein is om te investeren in deze ontwikkeling.

5.4 Gefaseerde ontwikkeling van inzicht en overtuiging van gedeeld belang

Zoals gesteld zien alle betrokken partijen positieve mogelijkheden voor het gebruik van SMT-informatie in Brzo-toezicht. Allen zien mogelijkheden voor samenwerking voor uitwisseling van kennis over methodes en best practices en uitwisseling van informatie uit de SMT en het toezicht ten behoeve van een gemeenschappelijk belang: de veiligheid van Brzo-bedrijven, te beginnen bij leden van de VOTOB.

Echter, daaraan worden voorwaarden gesteld. Op dit moment hebben betrokken partijen nog onvoldoende inzicht in de mate waarin aan deze voorwaarden kan worden voldaan. Daarnaast is nog niet voor alle betrokken partijen duidelijk hoe het delen van SMT-informatie en het gebruik van SMT-informatie in het toezicht bijdraagt aan een gedeeld belang: het borgen van de veiligheid bij tankopslagbedrijven.

De Brzo-toezichthouders zullen eerst zelf goed inzicht moeten krijgen in de kwaliteit van de SMT-audit, de SMT-informatie en de aansluiting van de audit bij de normen in het Brzo om te beoordelen of de informatie ook bruikbaar is in de aanpak van toezicht. Geïnterviewden geven aan dat de toezichthouders dit inzicht kunnen ontwikkelen door samenwerking tussen Brzo-toezichthouders en VOTOB-leden. Door samen dit inzicht te creëren ontstaat een gemeenschappelijk beeld van de match tussen de SMT en het Brzo dat ook kan bijdragen aan de ontwikkeling van de SMT.

VOTOB-leden moeten eerst goed inzicht krijgen hoe het transparant delen van SMT-informatie daadwerkelijk bijdraagt aan meer veiligheid in de sector zonder dat dit een aantasting betekent van het level playing field voor VOTOB-leden. Geïnterviewde vertegenwoordigers van Brzo-toezicht en vertegenwoordigers en leden van de VOTOB zijn het er over eens dat deze mogelijkheden vooral op het terrein van veiligheidscultuur het meest kansrijk is. Dit onderdeel is namelijk geen onderwerp van wetgeving, vormt daarom geen grond voor handhaving en biedt daarom de beste mogelijkheid om op een relatief gelijkwaardige, open manier om te gaan met informatie en van elkaar te leren.

6. Risicogestuurd toezicht door andere Rijkstoezichthouders

6.1 Inleiding

Dit hoofdstuk bevat de resultaten van een beknopt onderzoek bij onderdelen van andere Rijkstoezichthouders naar de wijze waarop zij risicogestuurd toezicht hebben ingericht en in welke mate zij gebruikmaken van informatie uit zelfbeoordelings- en zelfreguleringsinstrumenten, vergelijkbaar met de SMT. Doel van deze verkenning is geweest voorbeelden te vinden als inspiratie voor inrichting van toezicht met gebruikmaking van SMT-informatie. Er is geen vergelijking gemaakt met de wijze waarop risicogestuurd toezicht is vormgegeven binnen het Brzo-toezicht. In de verkenning zijn interviews afgenomen bij vertegenwoordigers van de Inspectie Leefomgeving & Transport (ILT), afdeling Veilige Mobiliteit, De Nederlandsche Bank (DNB), divisie Toezicht Pensioenfondsen, en de Inspectie Gezondheidszorg & Jeugd (IGJ), afdeling Risicodetectie & Ontwikkeling. Daarnaast is een beperkt aantal documenten bestudeerd.

Deze paragraaf start met een korte toelichting op de selectie van Rijksinspectiediensten. Vervolgens wordt ingegaan op thema's die naar voren zijn gekomen uit de verkenning die relevant zijn voor het vraagstuk rond het gebruik van SMT-informatie in risicogestuurd toezicht op Brzo-bedrijven. Tot slot wordt ingegaan op contextuele kenmerken van de geselecteerde diensten die van invloed zijn op de inrichting van toezicht en het gebruik van bedrijfsinformatie door de diensten.

6.2 ILT, DNB en IGJ als bron van inspiratie

Voorafgaand aan de verkenning is een selectie gemaakt van inspectiediensten met eigenschappen relevant voor deze studie: zij maken gebruik van risicoanalyses in de sturing van toezicht en zij houden toezicht op sectoren waarin veel gebruik wordt gemaakt van vormen van zelfregulering.

De selectie van betrokken Rijkstoezichthouders is gemaakt in overleg met de opdrachtgever. Argumenten voor de selectie zijn:

- ILT is bevraagd omdat zij ook een rol heeft in het toezicht op het Brzo. ILT is verantwoordelijk voor Wabo toezichtstaken bij de Rie categorie 4 bedrijven die onder het Ministerie van Defensie vallen³⁰. Binnen ILT is onderzocht hoe ILT vormgeeft aan informatieverwerking en risicoanalyses voor toezicht.
- DNB heeft al lang ervaring met risicogestuurd toezicht. DNB is in 2000 gestart met vormen van systeemtoezicht en in 2005 met vormen van risicogestuurd toezicht. In haar toezicht maakt DNB gebruik van allerlei informatiebronnen. Binnen DNB is het toezicht op de pensioenfondsen verkend.
- IGJ is betrokken in deze verkenning omdat deze dienst toezicht houdt op een veld waar intensief gebruik wordt gemaakt van allerlei vormen van zelfbeoordeling (intercollegiale visitatie) en -regulering zoals externe auditsystemen (HKZ, JCI) en klanttevredenheidsplatformen die openbaar zijn. Onderzocht is of en hoe IGJ gebruikmaakt van dit type informatie. Binnen IGJ is vooral onderzocht hoe inspecteurs worden voorzien van risico-informatie.

³⁰ <https://brzoplus.nl/brzo/brzo-deelnemende/ilt/>

6.3 Risicogestuurd toezicht en informatie uit zelfbeoordelings- en zelfreguleringsinstrumenten

In het onderzoek van geselecteerde rijktoezichthouders is een aantal thema's geïdentificeerd die mogelijk als voorbeeld en inspiratie kunnen dienen voor het Brzo-toezicht. Deze thema's zijn:

1. De plaats van risicoanalyses in de organisatie in relatie tot de inspecties.
2. Het gebruik van informatie voortkomend uit zelfbeoordelings- en zelfreguleringsinstrumenten.
3. De afspraken over informatiegebruik en vertrouwelijkheid tussen toezichthouder en de instellingen waarop zij toezicht houdt.

Ad 1. De plaats van risicoanalyses in de organisatie in relatie tot de inspecties

In de drie onderzochte diensten is de verwerking van informatie tot risicoanalyses ondergebracht in een ander onderdeel van de organisatie dan de inspecteurs die het toezicht uitvoeren. De reden hiervoor verschilt: in de ene organisatie is ervoor gekozen expertise op het terrein van data-analyse te clusteren, in de andere is ervoor gekozen bepaalde inhoudelijke expertise te clusteren.

De wijze waarop expertise is geclusterd verschilt. Binnen IGJ en ILT is ervoor gekozen experts op het terrein van data-analyse te clusteren in een apart onderdeel. Dit onderdeel bedient alle inspectieonderdelen van risico-informatie. Doel van clustering van data-analyse-expertise is dat deze clusters zoveel mogelijk veelsoortige informatie kunnen verwerken en omzetten naar informatie voor de inspecteurs. Bij ILT komt dit het meest expliciet naar voren in de keuze een 'Datalab' in te richten. Hiermee streeft ILT ernaar ook allerlei nieuwe inzichten op het terrein van data-analyse ('big data') zo snel mogelijk te betrekken in het werk van de inspectie. Binnen IGJ is alle data-analyse ondergebracht in een afdeling 'Risicodetectie & Ontwikkeling' (onderdeel van de Directie Bedrijfsvoering). De risicoanalyses van deze afdeling worden via een digitaal dashboard aangeboden aan de inspecteurs in de verschillende inspectieafdelingen van IGJ. Dit dashboard geeft inspecteurs in één oogopslag inzicht in de belangrijkste risicofactoren van een instelling. Op basis van dit dashboard maken IGJ-inspecteurs keuzes over welke instellingen en welke onderwerpen prioriteit krijgen in hun programma. Binnen IGJ en ILT bepalen de inspecteurs hoe zij de informatie uit de risicoanalyses gebruiken bij toezicht.

DNB heeft voor een ander organisatie-model gekozen. Binnen DNB is expliciet gekozen de inhoudelijke risicoanalyses te laten doen door inhoudelijk experts op specifieke, inhoudelijke onderdelen van de verschillende toezichtsdomeinen. Deze experts zijn ondergebracht in expertisecentra, gescheiden van de organisatieonderdelen waarin het 'accounthouderschap' is ondergebracht. Doel van deze scheiding is te borgen dat het toezicht wordt gevoed vanuit verschillende expertisegebieden zonder dat één expertisegebied gaat overheersen in het toezicht op instellingen. In de woorden van één van de geïnterviewden: "Elke expert vindt zijn eigen expertisegebied vaak belangrijker dan andere gebieden. Maar een accounthouder moet risico's op verschillende inhoudelijke gebieden kunnen afwegen." Accounthouders bij DNB, divisie Pensioenfondsen, zijn meer generalistisch opgeleide mensen, die de opdracht hebben gekregen het algemene doel van het toezicht in het oog te houden: borging van een evenwichtige bedrijfsvoering van pensioenfondsen'. De divisie Toezicht Pensioenfondsen heeft twee zogenaamde expertisecentra: het Expertisecentrum Financiële Risico's Pensioenfondsen en het Expertisecentrum Operationele en IT-risico's. In een dialoog tussen de expertisecentra en de accounthouderafdelingen wordt bepaald welke risico's worden geadresseerd in het toezicht binnen de pensioenfondsen. De accounthouders hebben daarin de eindverantwoordelijkheid. Zij maken de afweging tussen verschillende risico's in relatie tot het maatschappelijk belang waarop DNB toezicht houdt.

Ad 2. Het gebruik van informatie voortkomend uit zelfreguleringsinstrumenten

Geen van de onderzochte Rijkstoezichthouders maakt gebruik van informatie uit (van oorsprong) zelfbeoordelings- en zelfreguleringsinstrumenten voor risicoanalyses, tenzij deze informatie verplicht onderdeel uitmaakt van de informatie die een instelling moet aanleveren. Voorbeelden van dit type informatie binnen het toezicht op pensioenfondsen zijn de accountantsverklaringen en de rapportages van actuarissen voor pensioenfondsen. Aan deze verklaringen en de functies die de verklaringen opstellen, worden wettelijke eisen gesteld. Bij toezicht op ziekenhuizen gaat het om informatie die ziekenhuizen moeten rapporteren op grond van richtlijnen die zijn vastgesteld door wetenschappelijke verenigingen voor medisch specialisten.

Daarnaast maken de diensten gebruik van openbaar beschikbare informatie zoals jaarverslagen van bedrijven en informatie uit media. Deze informatie wordt vooral gebruikt voor risicoanalyses op macro- en mesoniveau. Binnen DNB en IGJ wordt dit type informatie ook gebruikt voor de risicoanalyses per instelling.

Overigens geven alle geïnterviewden aan dat inspecteurs de mogelijkheid hebben alle informatie op te vragen bij een instelling, die zij nodig denken te hebben om zich een goed beeld te kunnen vormen. Inspecteurs van IGJ vragen daarom wel eens om een medewerkerstevredenheidsonderzoek of informatie over klanttevredenheid. Deze informatie wordt echter niet beschouwd als structureel nodig voor risicoanalyses en wordt daarom niet standaard opgevraagd. DNB vraagt in haar toezicht regelmatig extra informatie op wanneer deze relevant wordt geacht. Deze informatie wordt betrokken in de risicoanalyse voor de specifieke instelling of de groep instellingen waar de informatie is opgevraagd.

Ad 3. De afspraken over informatiegebruik en vertrouwelijkheid tussen toezichthouder en de instellingen

De bestudeerde inspectiediensten maken geen gebruik van informatie die zij zouden krijgen op basis van vrijwilligheid. De informatie die zij ontvangen krijgen zij altijd binnen het gestelde wettelijk kader en wordt verplicht ter beschikking gesteld aan de toezichthouder. Uit deze verkenning zijn geen vrijwillige afspraken naar voren gekomen tussen de betrokken Rijkstoezichthouders en de sectoren of instellingen waarop zij toezicht houden, over hoe zij omgaan met informatie van te inspecteren instellingen. Geïnterviewden geven aan alle informatie op te vragen die nodig wordt geacht voor een goede risicoanalyse. Deze informatie moeten instellingen verplicht beschikbaar stellen. Hoe ver zij hierin gaan, verschilt per dienst. In alle gevallen is de kwaliteit van het toezicht leidend. Deze afweging wordt zorgvuldig gemaakt in verband met de administratieve lasten. Overwegingen rond de gevoeligheid van de informatie voor de positie van de instelling, spelen geen rol, aldus geïnterviewden, tenzij hier wettelijke kaders voor zijn vastgesteld.

De wet vormt het kader voor de keuzes die de diensten maken rond openbaarheid van gegevens. Het algemeen kader is de Wet openbaarheid van bestuur (Wob), specifieke kaders liggen vast in wetgeving voor de verschillende toezichtsdomeinen. Deze domeinspecifieke wetgeving regelt alle uitzonderingen op de Wob.

Binnen de kaders van de Wob en domeinspecifieke wetgeving, maken IGJ, DNB en ILT de afweging of openbaarmaking van informatie bijdraagt aan het algemeen belang enerzijds of dat openbaarmaking het werk van de inspectiedienst hindert, anderzijds. In deze afweging wordt betrokken de mate waarin openbaarmaking bijdraagt aan naleving. Onderdeel hiervan is de afweging of openbaarmaking kan leiden tot een minder coöperatieve, meer gesloten houding van de instellingen waarop toezicht wordt gehouden. Een aanname hierbij is dat een minder coöperatieve, meer gesloten houding van een instelling het toezicht bemoeilijkt en de bereidheid tot naleving doet afnemen.

Voor zover kon worden nagegaan, maken ILT, DNB en IGJ geen onderliggende informatie (actief) openbaar zoals de informatie die instellingen aan de toezichthouder beschikbaar moeten stellen. In de afweging over de relatie tussen toezichthouder en instellingen wordt eerder gekozen voor beperkte openbaarmaking en wordt gevoelige informatie alleen openbaar gemaakt wanneer dat wettelijk is voorgeschreven. Zo is toezichtsinformatie van DNB voornamelijk op een geaggregeerd niveau openbaar. Op grond van de Wet financieel toezicht is DNB verplicht tot geheimhouding van alle informatie die zij heeft ontvangen van instellingen onder toezicht.³¹ DNB maakt sancties die zij oplegt, wel openbaar.

Voor IGJ is voorgeschreven dat inspectierapporten en handhavingsbrieven openbaar worden gemaakt. IGJ maakt rapporten over incidenten en ongelukken alleen actief openbaar wanneer deze veel maatschappelijke of politieke aandacht krijgen. IGJ maakt sancties die zij oplegt, niet actief openbaar.³²

ILT kiest ervoor alle feitelijke constatering, oordelen en sancties actief openbaar te maken. Alle onderliggende informatie wordt niet openbaar gemaakt. Uitzonderingen zijn milieu-informatie die verplicht openbaar gemaakt moet worden, en bedrijfsvoeringsinformatie die onderdeel uitmaakt van het toezichtsdomein.³³ In haar visie op openbaarheid, stelt ILT expliciet dat zij in haar afweging meeneemt of openbaarmaking een positief of negatief effect zal hebben op de naleving van regelgeving.

Alle onderzochte Rijkstoezichthouders hebben te maken met aanpassingen van wet- en regelgeving rond openbaarheid van informatie in het kielzog van maatschappelijke en politieke discussies. Zo heeft de Tweede Kamer recent wetgeving aangenomen die IGJ opdraagt toezichtsrapportages rond gemelde incidenten of calamiteiten openbaar te maken terwijl deze verplichting er eerst niet was. De regelgeving is aangepast mede naar aanleiding van verschillende Wob-verzoeken die waren afgewezen door de rechter. Welke specifieke gegevens wel en welke niet openbaar gemaakt moeten worden, is nog niet vastgesteld.

Tot slot hebben DNB en IGJ afspraken met andere inspectiediensten over het delen van informatie en expertise. Zo hebben DNB en de Autoriteit Financiële Markten (AFM) afspraken gemaakt over de uitwisseling van informatie in een samenwerkingsconvenant. Dit convenant regelt het toezicht op sectoren en instellingen waar zij allebei een verantwoordelijkheid hebben. Deze afspraken zijn gemaakt om administratieve lasten te beperken. IGJ heeft een vergelijkbare afspraak met de Nederlandse Zorgautoriteit (NZa), ook in het kader van beperking van administratieve lasten. Deze afspraken bepalen niet hoe inspectiediensten omgaan met openbaarheid van of handhaving op uitgewisselde informatie. Daarvoor is het wettelijk kader voor betrokken diensten bepalend.

6.4 Context: doel van het toezicht en de relatie tussen toezichthouder en instelling

In deze verkenning is gebleken dat de onderzochte Rijkstoezichthouders hun afwegingen over het opvragen en openbaar maken van informatie altijd plaatsen in de context van het doel van hun toezicht (naleving) en de meest effectieve relatie met de instellingen waarop zij toezicht houden. Een effectieve relatie is er één, aldus geïnterviewden, met een open, coöperatieve opstelling van de organisaties waarop toezicht wordt gehouden. Gedachte hierachter is dat een open, coöperatieve houding bijdraagt aan de transparantie van de instelling en acceptatie van aanwijzingen van de toezichthouder. Een afwerende, antagonistische houding daarentegen leidt tot meer geslotenheid en weerstand en dus minder effectief toezicht.

³¹ DNB, Visie DNB toezicht, 2014 – 2018, blz. 22.

³² <https://www.igj.nl/onderwerpen/openbaarmaking>

³³ ILT, Een nieuwe ILT-visie op openbaarheid, 24 mei 2016, blz. 11.

Om deze open, coöperatieve houding te bewerkstelligen, hanteren IGJ en DNB een aantal uitgangspunten in de relatie met de instellingen waarop zij toezicht houden:

- Uitgangspunt is dat de instellingen intrinsiek gemotiveerd zijn om hetzelfde doel na te streven als de toezichthouder: pensioenfondsen streven ook naar een zo stabiel mogelijke bedrijfsvoering, zorginstellingen willen goede zorg leveren.
- Er wordt prudent omgegaan met toezichtsinstrumenten en terminologie die weerstand oproepen bij instellingen. Daarom besteedt IGJ bij uitzondering aandacht aan het sterftecijfer in toezichtsgesprekken met zorginstellingen. Dit leidt, aldus geïnterviewde, vooral tot emotionele reacties en weerstand binnen de instellingen. Daarom wordt ervoor gekozen vergelijkbare indicatoren te gebruiken die evenveel zeggen over de kwaliteit van de zorg, maar minder weerstand oproepen.
- Handhaving wordt beschouwd als het eindstation in een traject en wordt alleen ingezet als een instelling niet reageert op andere instrumenten van de toezichthouder. Daarbij kiezen de toezichthouders DNB en IGJ, wanneer zij sanctioneren, eerder voor handhaving gericht op herstel door het opleggen van een last onder dwangsom. Boetes worden uitgedeeld voor situaties die niet meer te herstellen zijn zoals het niet tijdig rapporteren van zaken aan de inspectie. DNB spreekt overigens niet van handhaving maar van 'mitigatie'.

6.5 Tussenbalans: evenwicht tussen de wet, behoefte aan informatie en de toezichtsrelatie

- DNB, IGJ en ILT hebben ervoor gekozen data- en risicoanalyse ten behoeve van toezicht onder te brengen in aparte organisatieonderdelen. Hiermee brengen de diensten een expliciete scheiding aan tussen het genereren van sturingsinformatie voor toezicht en het feitelijk toezicht. De keuzes hiervoor worden verschillend onderbouwd. IGJ en ILT willen met een speciale expertafdeling voor data-analyse kunnen blijven inspelen op de snelle ontwikkelingen op dat terrein. DNB wil borgen dat tegelijk risicoanalyses worden uitgevoerd met voldoende expertise en dat de accounthouders vanuit een brede blik, een afgewogen oordeel kunnen geven over welke risico's prioriteit moeten krijgen in het toezicht.
- Voor het opvragen, het gebruik en het openbaar maken van informatie vormt de wet het enige bindende kader voor de betrokken inspectiediensten. Alle informatie die bedrijven aanleveren in het kader van toezicht, is geformaliseerd in een verplichting. In deze verkenning zijn geen andersoortige afspraken aangetroffen over de levering van informatie tussen de onderzochte Rijkstoezichtshouders en de instellingen. Informatie uit zelfbeoordelings- en zelfreguleringsinstrumenten wordt dan ook niet gebruikt, tenzij het instrument is verankerd in een wettelijk kader.
- Ook voor openbaarmaking van informatie is de wet het enige kader. Hierover zijn geen andersoortige afspraken aangetroffen in deze verkenning. Wel lijkt het erop dat diensten voornamelijk informatie openbaar maken die zij zelf hebben geproduceerd. Informatie aangeleverd door bedrijven lijkt geen rechtstreeks onderdeel te zijn van openbaarmaking tenzij daartoe een wettelijke verplichting geldt, en ook niet opvraagbaar in het kader van de Wob. Echter, dit zou nader onderzocht moeten worden.
- Alle betrokken diensten kiezen ervoor uiterst zorgvuldig om te gaan met informatie die zij opvragen bij de instellingen waarop zij toezicht houden. Dit is onderdeel van een bredere benadering van de toezichtsrelatie: om goed toezicht te kunnen houden is het belangrijk dat instellingen een constructieve, open houding aannemen in de relatie met de toezichthouder. Gedachte hierachter is dat een open, coöperatieve houding bijdraagt aan de transparantie van de instelling en acceptatie van aanwijzingen van de toezichthouder.
- Om deze open, constructieve houding te bevorderen, hanteren de diensten de volgende uitgangspunten in het toezicht:

- De toezichthouder en de instellingen hebben een gedeeld belang: een goede borging van veiligheid (ILT), goede zorg (IGJ) of financiële soliditeit en een integere bedrijfsvoering bij pensioenfondsen (DNB). Instellingen zijn intrinsiek gemotiveerd dit belang te dienen.
- In de toepassing van toezichtsinstrumenten en in de communicatie met de instellingen wordt zorgvuldig afgewogen welke bijdragen en welke afdoen aan de gewenste houding van instellingen.
- Handhaving wordt beschouwd als een eindstation in verschillende stappen die de dienst zet om instellingen te bewegen tot naleving. Diensten benutten hierbij maximaal hun discretionaire ruimte binnen de wettelijke kaders. Alleen wanneer is gebleken dat een instelling niet de gewenste verbeteringen wil doorvoeren, wordt een handhavingstraject gestart. Daarbij is de handhaving in de eerste plaats gericht op verbetering door het opleggen van een last onder dwangsom. Boetes worden opgelegd als de situatie niet meer is te herstellen, zoals overschrijding van een termijn voor rapportage.

7. Conclusies

7.1 Inleiding

In deze verkenning is onderzocht of en hoe in het Brzo-toezicht gebruik kan worden gemaakt van de SMT voor inrichting van risicogestuurd toezicht. Daarvoor zijn verkend het wettelijk kader voor het toezicht, de aard en achtergrond van de SMT en de bruikbaarheid van de SMT vanuit het perspectief van het Brzo-toezicht en vanuit het perspectief van de gebruikers van de SMT. Daarnaast is onderzocht hoe andere Rijkstoezichthouders vorm en inhoud geven aan risicogestuurd toezicht, in het bijzonder hoe zij daarbij gebruikmaken van informatie uit zelfbeoordelings- en zelfreguleringsinstrumenten. Tot slot is verkend welke ontwikkelrichtingen er zijn voor de integratie van de SMT in het risicogestuurd toezicht op het Brzo.

7.2 Is de SMT bruikbaar in risicogestuurd toezicht?

De SMT is, onder voorwaarden, bruikbaar voor risicogestuurd toezicht. Dit geldt voor de aanpak van de SMT-audit en voor de informatie uit de SMT-audits. Brzo-toezicht zou de inhoud en aanpak van de SMT kunnen benutten als mogelijk voorbeeld voor het verder verbeteren van de inspectie-methodiek voor het Brzo. Met name de SMT-aanpak van de cultuurscan biedt mogelijkheden om de cultuurscan binnen het Brzo verder vorm te geven. Ook de informatie uit de SMT-audits is bruikbaar en kan input zijn voor risicogestuurd toezicht op het Brzo. De SMT biedt namelijk inzicht in dezelfde aspecten van een bedrijf (software, hardware, mindware) als die waarin Brzo-inspecties inzicht bieden. Deze conclusie wordt onderschreven in de workshop. 'De tijd is er rijp voor' aldus de deelnemers.

Om SMT-informatie goed te kunnen benutten, moet aan de volgende voorwaarden worden voldaan:

- Brzo-toezichthouders krijgen de gelegenheid de kwaliteit van de audit-methodiek en informatie goed te verifiëren. Door Brzo-inspecteurs nauw te betrekken bij deze verificatie, ontstaat vertrouwen in de waarde van de methodiek voor het toezicht. Zonder dat vertrouwen ontstaat het risico dat zij SMT-informatie niet structureel zullen betrekken in het bepalen van de inspectie-agenda per Brzo-bedrijf.
- Binnen het kader van samenwerkingsprogramma Brzo+, wordt een risicoanalysemethodiek ontwikkeld waarin de SMT-informatie een zinvolle plaats inneemt.
- Op voorhand moet voor alle betrokkenen, maar met name voor de VOTOB-leden duidelijk zijn op welke wijze SMT-informatie wordt gebruikt en van invloed is op het toezicht en eventuele handhaving.
- De ervaring die het Brzo-toezicht opdoet met het gebruik van de SMT in risicogestuurd toezicht wordt ingezet in een bredere ontwikkeling naar een grotere doelgroep bedrijven. Want de huidige groep VOTOB-leden is te klein om een specifieke aanpak voor deze groep te legitimeren.
- Er moet sprake zijn van wederkerige transparantie: de kennis die Brzo-toezichthouders ter beschikking krijgen door het gebruik van de SMT-informatie in risicoanalyses, moet ook worden gedeeld met de VOTOB zodat ook de VOTOB-leden daarvan kunnen leren.

7.3 Beschikbaarheid van SMT-informatie op basis van afspraken met de VOTOB

Brzo-toezicht kan de informatie uit de SMT op twee manieren verwerven:

Opvragen van informatie zonder waarborgen

De eerste manier is dat de SMT-informatie wordt opgevraagd bij bedrijven waardoor de overdracht van SMT-informatie een (semi-)verplicht karakter krijgt als onderdeel van het Brzo-toezicht. Hierbij wordt geen onderscheid gemaakt tussen opvragen zonder en met vordering.

In beide gevallen is er sprake van een zekere noodzaak de informatie ter beschikking te stellen: in het geval van een vordering is het bedrijf verplicht de informatie aan de inspectie te geven; in het geval van opvragen zonder vordering is het bedrijf niet verplicht maar kan, door te weigeren, de indruk wekken niet transparant te willen zijn over de veiligheid en daarmee extra aandacht opwekken bij inspectiediensten.

Bij deze keuze ontstaat, binnen de huidige verhoudingen, een aanzienlijk risico dat een deel van de VOTOB-leden de SMT-audit vooral zullen gaan gebruiken om te voorkomen dat zij door Brzo-inspecties als risico worden beschouwd of niet meer mee willen doen aan de SMT-audit. In dat geval verliest de SMT haar oorspronkelijke functie voor de VOTOB-leden: samen leren ten behoeve van de veiligheid.

Beschikbaar stellen van informatie met waarborgen

De tweede manier is door afspraken te maken met de VOTOB over de vrijwillige levering van informatie. In dat geval verwachten de VOTOB-leden een zekere wederkerigheid door het bieden van een aantal waarborgen:

- Het ter beschikking stellen van SMT-informatie mag niet leiden tot het verlies van een level playing field voor VOTOB-leden. Dit betekent dat vrijwillig delen van SMT-informatie niet mag leiden tot door méér handhaving bij VOTOB-leden door Brzo-toezichthouders omdat dit meer inzicht geeft in potentiële overtredingen.
- SMT-informatie van individuele bedrijven mag niet openbaar worden gemaakt. Bedrijven vrezen dat dit zal leiden tot negatieve publiciteit over het bedrijf, wat schadelijk is voor de relatie tussen het bedrijf en haar omgeving. Ook vrezen de VOTOB-leden dat dit zal leiden tot concurrentie op veiligheid omdat dit het samen leren in de weg zal staan.

Wanneer voor deze weg wordt gekozen, is het belangrijk dat wordt vastgesteld welke waarborgen kunnen worden gegeven en welke (bestuurlijke) afspraken daarover moeten worden gemaakt. Deze moeten namelijk passen binnen het wettelijk kader en de daarop gebaseerde Landelijke Handhavingsstrategie Brzo. Ook afspraken over openbaarmaking van informatie moeten worden gemaakt binnen de wettelijke kaders waarbinnen de verschillende gezagen opereren binnen het Brzo-toezicht.

7.3 Beschikbaarheid van SMT-informatie zonder waarborgen

Door de complexiteit van het toezicht op de Brzo, is het denkbaar dat goede waarborgen over het gebruik van de SMT-informatie niet kunnen worden gegeven. Welke mogelijkheid blijft dan over? Hoe kan de SMT-informatie dan worden gedeeld zonder vordering of waarborgen? En onder welke voorwaarden zal de risico-informatie op basis van de SMT ook daadwerkelijk worden gebruikt?

Op basis van deze verkenning trekken wij de conclusie dat vrijwillige uitwisseling van SMT-informatie wordt bevorderd wanneer wederzijds vertrouwen wordt versterkt tussen het Brzo-toezichthouders en de VOTOB-leden. De volgende voorwaarden dragen bij aan wederzijds vertrouwen:

1. Er is sprake van gemeenschappelijk belang in een zo goed mogelijke borging van de veiligheid in de bedrijven.
2. Het Brzo-toezicht gaat zorgvuldig om met de SMT-informatie door goed toezicht, rechtvaardige handhaving en een maximale borging van de vertrouwelijkheid binnen de kaders van de wet.
3. Brzo-toezichthouders hebben kunnen vaststellen dat SMT-informatie van goede kwaliteit is, verkregen via een kwalitatief goede audit-methodiek.
4. Risico-informatie mede gebaseerd op de SMT-informatie, wordt door het Brzo-toezicht ook gedeeld met de VOTOB zodat sprake is van wederzijds leren.

Ad. 1. Gemeenschappelijk belang van bedrijven en inspectie

Uit de verkenning bij DNB en IGJ komt naar voren dat deze inspectiediensten het uitgangspunt van een gemeenschappelijk belang een belangrijke pijler vinden van een constructieve en open toezichtsrelatie. Zij gaan daar overigens niet zonder meer vanuit. Dit moet wel blijken uit de wijze waarop de instellingen laten zien dat zij werkelijk streven naar goede kwaliteit zorg of een evenwichtige bedrijfsvoering door daarop steeds weer de juiste maatregelen te treffen. Als dat niet blijkt, volgen er maatregelen.

Vertaald naar Brzo-toezicht en de VOTOB-leden, betekent dit dat VOTOB-leden die dat hebben laten blijken, bijvoorbeeld in eerdere Brzo-inspecties en de SMT-resultaten, ook vanuit een gemeenschappelijk belang worden benaderd. Binnen de kaders van het Brzo krijgen zij te maken met een handhavingsaanpak die blijkt geeft van hun inspanningen om de veiligheid te verbeteren. Het Brzo-toezicht laat zien maximaal gebruik te maken van de beschikbare discretionaire ruimte binnen de handhaving om positieve inspanningen te belonen, overigens binnen de kaders van hun verantwoordelijkheid.

Ad 2. Het Brzo-toezicht gaat zorgvuldig om met SMT-informatie

Uit de verkenning is gebleken dat VOTOB-leden zich zorgen maken over méér handhaving omdat Brzo-toezichthouders beschikken over bedrijfsspecifieke informatie uit de SMT en daarmee het verlies van een level playing field. Daarom moet het Brzo-toezicht laten zien hoe het vrijwillig delen van SMT-informatie inderdaad leidt tot beter inzicht in de risico's en daarom tot meer effectief toezicht en handhaving binnen de hele branche, niet alleen bij de VOTOB-leden. Bedrijven die de zaken goed voor elkaar hebben, krijgen vanzelf minder te maken met handhaving dan bedrijven die tot de risicocategorie behoren.

De kwaliteit en transparantie van de risicoanalyses zijn hierbij van groot belang. In lijn met de voorbeelden bij ILT, IGJ en DNB, betekent dit dat hiervoor expertise zou moeten worden georganiseerd.

Om te voorkomen dat (de dreiging van) handhaving een verstorende rol gaat spelen in de ontwikkeling van wederzijds vertrouwen en transparantie, is het denkbaar de uitwisseling van SMT-informatie, in eerste instantie, te beperken tot dat deel van de SMT waarvoor geen wettelijk kader is dat kan leiden tot handhaving: de cultuurscan van de SMT. Informatie over de veiligheidscultuur is interessant voor een risicoanalyse maar aan de ontwikkeling van een veiligheidscultuur worden geen wettelijke eisen gesteld. In de workshop gaven deelnemers aan, ook graag de onderdelen techniek (hardware) en systeem (software) te willen betrekken omdat deze onderdelen beter aansluiten bij de taken van het toezicht.

Een laatste voorwaarde die ook werd benadrukt in de workshop met inspecteurs, VOTOB-leden en experts was dat er bestuurlijke afspraken zouden moeten worden gemaakt over de handhaving op bedrijven die SMT-informatie ter beschikking stellen.

Dit om te borgen dat gemaakte afspraken over handhaving tussen inspectiediensten en de VOTOB ook op termijn kunnen worden nagekomen. Deze bestuurlijke afspraken zouden bijvoorbeeld kunnen worden gemaakt in het Bestuurlijk Omgevingsberaad met de Minister, het Openbaar Ministerie en de Omgevingsdiensten.

Ad 3. Het vertrouwen in de kwaliteit van de SMT-informatie

Het Brzo-toezicht moet dus maatregelen treffen die het vertrouwen wekken van betrokken bedrijven. Het vergt ook vertrouwen van het Brzo-toezicht in de kwaliteit van de SMT-informatie. Alleen dan heeft het zin om te investeren in de beschikbaarheid en het gebruik van de informatie. Om dit vertrouwen te winnen, moeten Brzo-inspecteurs de gelegenheid krijgen de kwaliteit van de SMT-informatie te verifiëren. Daarnaast is het behulpzaam wanneer de VOTOB open staat voor kritiek op de SMT en laat zien te willen acteren op die kritiek. Op die manier kan de VOTOB het vertrouwen van het Brzo-toezicht in de SMT ook versterken.

Ad 4. Wederzijds leren door het delen van risico-informatie

Een vierde mogelijkheid het om wederzijds vertrouwen te versterken, is wederkerigheid in het delen van informatie: door informatie uit risicoanalyses voor het Brzo-toezicht te delen met de VOTOB-leden ontstaat wederkerigheid. Het Brzo-toezicht stelt de uitkomsten van risicoanalyses op (sub-)sector beschikbaar aan de branche zodat de hele sector baat heeft bij het beschikbaar stellen van informatie. Binnen de VOTOB worden deze risicoanalyses vervolgens vertaald naar verbetervoorstellen voor de leden. Een voorbeeld van een dergelijke aanpak is hoe DNB onderzoeksinformatie ter beschikking stelt die instellingen helpt te verbeteren of benchmarks uitvoert en deelt op basis waarvan instellingen weten waar zij staan.

Een andere vorm van wederkerigheid is transparantie over de risicoanalyses. Het Brzo-toezicht zou bereid kunnen zijn SMT-experts kritisch te laten kijken naar de Brzo-risicoanalyses en onderliggende methodes om zelf ook te leren van de kennis die er in de sector aanwezig is. Door zelf te laten zien te willen luisteren en leren, geven de Brzo-toezichthouders het goede voorbeeld van transparantie en wederzijds leren voor de sector.

8. Ontwikkelrichtingen

8.1 Inleiding

In deze paragraaf wordt een voorstel gedaan voor twee ontwikkelrichtingen om invulling te geven aan de voorwaarden voor uitwisseling van SMT-informatie en risicoanalyses in het Brzo-toezicht. De eerste richting is de start van een beperkte pilot waarin SMT-informatie wordt ingezet voor risicoanalyses. De tweede ontwikkelrichting betreft de ontwikkeling van een onafhankelijk expertisecentrum voor risicoanalyses voor het toezicht op de Brzo.

8.2 Ontwikkelrichting 1: Pilot Uitwisseling SMT (pilot US)

Vertrouwen is noodzakelijk om SMT-informatie effectief te kunnen gebruiken voor Brzo-risicoanalyses zonder dat de SMT haar functie verliest als leermiddel voor VOTOB-leden. Maar het opbouwen van vertrouwen kost tijd. Om wederzijds vertrouwen te krijgen in de kwaliteit van de SMT-audit en in de GIR-informatie is het nuttig dat Brzo-inspecteurs en de VOTOB-bedrijven veel gelegenheid krijgen om, in een setting buiten de handhaving, kennis te nemen van elkaars werkwijze.

Op basis van de informatie uit de workshop met deskundige vertegenwoordigers van Brzo-inspectiediensten, VOTOB-leden en de SMT-auditors, kunnen globale stappen worden geformuleerd voor de pilot. Voor elke stap is meer vertrouwen nodig in elkaars werkwijze en het nut van transparante uitwisseling. Daarom zal elke stap moeten worden afgerond met een go-no go moment waarop wordt bepaald of de uitkomsten van de stap voldoende zijn voor een vervolg.

De pilot bestaat uit vijf fases met ieder een aantal stappen. Deze fases zijn:

Fase 1: Voorbereiding.

Fase 2: Kennismaking en verkenning.

Fase 3: Ontwerp voor toepassen van SMT-informatie in risicogestuurd toezicht op Brzo.

Fase 4: Uitvoering pilot.

Fase 5: Evaluatie.

Op basis van de uitkomsten van dit onderzoek zijn fase 1 en 2 nader uitgewerkt. De volgende fases moeten worden uitgewerkt op basis van de uitkomsten van fase 1. Hier wordt volstaan met een globale omschrijving van het doel van fases 3 tot en met 5.

Fase 1: Voorbereiding

De eerste fase van de pilot heeft vooral tot doel het uitwerken van afspraken over de inrichting van de pilot die kunnen rekenen op draagvlak bij de belangrijkste deelnemende partijen. Uit deze verkenning komt naar voren dat afspraken over de volgende zaken zeer belangrijk zijn voor het slagen van de pilot:

- De selectie van organisaties en personen die deelnemen aan de pilot. Zoals eerder beschreven is het belangrijk dat deze organisaties en mensen enthousiast zijn over de uitwisseling van informatie ten behoeve van de veiligheid.
- De rol en positie van de projectleider. Omdat de eerste fasen van de pilot vooral tot doel hebben elkaar te leren kennen en onderling vertrouwen te kweken, is het zinvol een onafhankelijke, ter zake kundige projectleider te benoemen zonder belang in de uitkomsten. Door diens onafhankelijkheid is de projectleider dan beter in staat belangen van partijen te wegen en te bemiddelen in de loop van de pilot.

- De informatie die zal worden uitgewisseld. Alle betrokken partijen moeten duidelijkheid hebben over welke informatie beschikbaar zal zijn binnen het kader van de pilot en, daarmee, onder het embargo van de pilot valt. Zo kan bijvoorbeeld worden afgesproken dat de uitwisseling zich beperkt tot het cultuurdeel van de SMT en de inspectiegegevens.
- De wijze waarop betrokken partijen omgaan met informatie die wordt uitgewisseld en kan worden beschouwd als vertrouwelijk. Alle betrokken partijen moeten ervan uit kunnen gaan dat het embargo op hun informatie alleen onder zeer specifieke omstandigheden (bijvoorbeeld bij een ongeval) kan worden opgeheven.
- De wijze waarop partijen zullen omgaan met de rol en verantwoordelijkheid van inspecteurs binnen de pilot. Daarbij is het belangrijk dat er afspraken worden gemaakt over hoe inspectiediensten omgaan met zaken die zij tegenkomen in de pilot waarop handhaving mogelijk is. Het moet duidelijk zijn onder welke omstandigheden en langs welk proces inspectiediensten in dat geval besluiten tot handhaving. Deze afspraken moeten worden zijn afgestemd met het bevoegde gezag voor de verschillende diensten.

Om gemaakte afspraken te borgen, kunnen deze worden vastgelegd, bijvoorbeeld in een convenant waarin de leiding van betrokken organisaties zich committeren aan de pilot.

Fase 2: Kennismaking en verkenning

Om de kans van slagen zo groot mogelijk te maken, moet de pilot worden gestart met een beperkte werkgroep van inspecteurs, bedrijven en SMT-auditors die dit zien als een kans om van elkaar te leren. Deze werkgroep kan geleidelijk worden uitgebreid.

Fase 2 bestaat uit drie stappen:

Stap 1: Wederzijds verkenning van aanpak en instrumenten voor de hele sector

Doel van deze stap is dat Brzo-inspecteurs en SMT-experts inzicht krijgen in de kwaliteit van elkaars aanpak op sectorniveau. Gedachte achter deze eerste kennismaking is dat nader inzicht in elkaars aanpak leidt tot meer vertrouwen in de waarde van de aanpak.

Deze vergelijking moet vooral het karakter hebben van een eerste uitwisseling van informatie. Dit kan in de eerste stap door een vergelijking op papier van de Ranking, een ranglijst van bedrijven op basis van uitkomsten van Brzo-toezicht, en de resultaten van de SMT-audits. Brzo-inspecteurs en SMT-auditors analyseren gezamenlijk de overeenkomsten en verschillen van de twee aanpakken en resultaten. Ook neemt men gezamenlijk de tijd om vragen te stellen over de verschillende aanpakken.

Stap 2: Wederzijdse verkenning van informatie op bedrijfsniveau

Ook deze stap heeft tot doel wederzijds inzicht in de kwaliteit van elkaars aanpak maar dan meer specifiek dan in de voorgaande stap, namelijk voor individuele bedrijven. Betrokken Brzo-inspecteurs en SMT-auditors doen een gezamenlijke analyse van de overeenkomsten en verschillen tussen informatie uit de GIR en de SMT-audit voor individuele bedrijven. Door meerdere jaren te vergelijken, is vast te stellen of de vergelijking consistent is en niet per toezicht- of auditronde anders is.

De vergelijking wordt gemaakt voor bedrijven die hiervoor toestemming hebben gegeven. Vooraf worden afspraken gemaakt over hoe met de informatie wordt omgegaan in het kader van Brzo-inspecties. De Brzo-inspecteurs geven daarbij aan hoe zij om zullen gaan met handhaving op basis van de informatie verworven in deze stap.

Stap 3: Wederzijdse verkenning van elkaars werkwijze in de praktijk

Een derde stap is om Brzo-inspecteurs en SMT-auditors met elkaar mee te laten lopen in de uitvoering van inspecties en audits. Doel van deze stap is dat inspecteurs, auditors en betrokken bedrijven inzicht krijgen in de praktijk van de inspectie- en auditaanpak. Deze 'meeloopsessies' moeten resulteren in gezamenlijke evaluatie van de SMT in relatie tot het Brzo-toezicht. Belangrijk hierbij is dat de meelopende inspecteurs en auditors ook open staan voor leerpunten voor de eigen methodiek en deze leerpunten delen met elkaar en de betrokken bedrijven.

Fase 3: Ontwerp voor toepassen van SMT-informatie in risicogestuurd toezicht op Brzo

Wanneer fase 1 succesvol is afgerond en Brzo+ en de VOTOB besluiten dat risicogestuurd toezicht met SMT-informatie in belang is van de veiligheid binnen de sector, kan de volgende fase van de pilot starten. Deze fase behelst het eerste ontwerp voor risicoanalyses op basis van SMT-informatie.

Welke informatie uit de SMT daadwerkelijk wordt benut in de risicoanalyses wordt, idealiter, in samenspraak met de VOTOB bepaald. Daarnaast ondersteunt het de ontwikkeling van vertrouwen wanneer de VOTOB mag meekijken met het ontwerp. Ten slotte bevat het ontwerp de afspraken over hoe de uitkomsten van deze risicoanalyses zullen worden gedeeld met de VOTOB ten behoeve van wederzijdse transparantie en leren.

Eén van de mogelijke afspraken over wederzijdse transparantie en leren, werd gedaan in de workshop met deskundigen: bedrijven zouden een onderwerp kunnen aandragen voor de inspectieagenda voor hun bedrijf zodat dit onderwerp door de inspecteurs onder de loep wordt genomen. Op deze manier kunnen bedrijven ook zelf accenten aanbrengen in wat zij graag zouden willen verbeteren.

Fase 4: Uitvoering van de pilot

Doel van deze fase is daadwerkelijk uitvoeren van risicoanalyses voor Brzo-toezicht mede op basis van SMT-informatie. Ook in deze fase zal de VOTOB moeten worden betrokken, bijvoorbeeld door SMT-auditors als reviewer te laten meekijken hoe deze risicoanalyses worden gedaan. Met hen wordt vervolgens geëvalueerd hoe (1) de risicoanalyses kunnen worden verbeterd en (2) welke leerpunten de risicoanalyses opleveren voor de SMT.

Fase 5: Evaluatie

De pilot wordt, vanzelfsprekend, afgerond met een evaluatie. In deze evaluatie moeten, onder andere, de volgende vragen centraal staan:

- Bieden risicoanalyses met informatie uit de SMT inderdaad beter zicht op de risico's in de sector?
- Komen de risicoanalyses met informatie uit de SMT ook ten goede aan de ontwikkeling en het gebruik van de SMT als zelfbeoordelingsinstrument ter lering en verbetering van de veiligheid?

Op basis van de antwoorden op deze vragen kan worden bepaald of de uitkomsten van de pilot aanleiding zijn voor verdere institutionalisering van risicoanalyses op basis van SMT-informatie.

8.3 Ontwikkelrichting 2: Brzo+ DataLab

In de tweede ontwikkelrichting ligt de focus vooral op de ontwikkeling van een bredere, kwalitatief sterke risicoanalyse voor Brzo-toezicht waarbij informatie uit de SMT één van de bronnen is. Deze ontwikkelrichting is gebaseerd op de organisatiekenmerken van risicoanalyses uitgevoerd door IGJ, DNB en ILT.

In deze ontwikkelrichting worden de risicoanalyses ten behoeve van het toezicht op het Brzo ondergebracht in een datalab, vooralsnog aangeduid als 'Brzo+ Datalab'. Dit is een nieuw in te richten kennisorganisatie van de gezamenlijke Brzo-toezichthouders, die nauw verbonden is met het Brzo+ samenwerkingsprogramma en die gevoed wordt met data van de Brzo-toezichthouders en data van derden zoals de VOTOB. Het Brzo+ Datalab is een neutrale organisatie met expertise op het terrein van data-analyse (IGJ- en ILT-model) en Brzo-expertise (het DNB-model) en staat als separate kennisorganisatie op afstand van de individuele Brzo-toezichthouders. Deze organisatie doet risicoanalyses op basis van een combinatie van GIR-informatie, SMT-informatie en andere relevante informatie op sector- en op bedrijfsniveau. Daarnaast biedt het de mogelijkheid duurzaam te investeren in de ontwikkeling van data-analyse voor Brzo-toezicht.

In het kader van transparantie en het leereffect, zouden de data-analyses die worden uitgevoerd door deze neutrale organisatie, ook beschikbaar kunnen worden gesteld aan sector- en brancheorganisaties als de VOTOB.

Dit Brzo+ Datalab kan overigens voor toezicht op alle Brzo-bedrijven functioneren. Daarmee is geborgd dat het gebruik van de SMT-informatie niet alleen gevolgen heeft voor de leden van de VOTOB maar voor alle Brzo-bedrijven. Daarnaast kan, vanuit het Datalab, initiatief worden genomen ook andere bronnen van zelfbeoordelingsinformatie te benutten voor risicoanalyse.

Bijlage 1 – Geïnterviewde organisaties

Vertegenwoordigers van de volgende organisaties zijn geïnterviewd in stap 2 van het onderzoek:

- Bureau Brzo+
- De Nederlandsche Bank (DNB)
- Inspectie Gezondheid en Jeugd (IGJ)
- Inspectie Leefomgeving & Transport (IL&T)
- Inspectie Sociale Zaken en Werkgelegenheid (Inspectie SZW)
- Ministerie van Sociale Zaken en Werkgelegenheid
- Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
- Royal HaskoningDHV
- Standic B.V.
- Vopak Management Netherlands B.V.
- De Vereniging van Nederlandse Tankopslagbedrijven (VOTOB)

Bijlage 2 – Organisaties vertegenwoordigd in workshop

In de workshop op 2 november 2018 waren de volgende organisaties vertegenwoordigd:

- Bureau Brzo+
- DCMR Milieudienst Rijnmond
- Inspectie Sociale Zaken en Werkgelegenheid (Inspectie SZW)
- Koole Terminals B.V.
- Oiltanking Amsterdam B.V.
- Omgevingsdienst Midden- en West-Brabant
- Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
- RoyalHaskoningDHV
- Standic B.V.
- Veiligheidsregio Rotterdam-Rijnmond
- De Vereniging van Nederlandse Tankopslagbedrijven (VOTOB)
- Vesta Terminals B.V.
- Vopak Management Netherlands B.V.

Bijlage 3 – Bestudeerde documenten

- AFM, Toezichtaanpak van de AFM, 3 mei 2017
- AFM en DNB, Handhavingsbeleid van de AFM en DNB, 10 juli 2008
- Bokhorst, M. en J. van Erp, Van transparantie naar responsiviteit, ontwikkeling van de omgevingsgerichtheid van toezichthouders, september 2017
- Brzo+, Deelproducten in Clusters Landelijke Benadering Risicobedrijven, 19 september 2017
- Brzo+, Monitor naleving en handhaving Brzo-bedrijven 2017, 22 mei 2018
- Brzo+, Project Initiatie Document Landelijke Benadering Risicobedrijven (LBR), 23 februari
- Brzo+, Ranking veiligheidsprestaties Brzo-bedrijven, 9 november 2017
- Brzo+, Werkwijzer Brzo 1999, Aandachtspuntenlijst Tankopslaginspecties, versie 2
- Civil Aviation Authority, Just Culture, EC Regulation 376/2014 on the Reporting, Analysis and Follow Up of Occurrences in Civil Aviation, 2015
- DCMR Milieudienst Rijnmond in samenwerking met VRR en Inspectie SZW, Rapportage project IT2 (Intensivering Inspectie Tankopslag), 11 oktober 2012
- DNB, brochure 'gedrag en cultuur in de Nederlandse financiële sector', 2016
- DNB, organogram, 2017
- DNB, Proportional and effective supervision
- DNB, Toezichtthema's DNB en AFM 2017: pensioenfondsen
- DNB, Toezicht Vooruitblik 2017
- DNB, Visie DNB toezicht 2014 – 2018
- GAIN Workinggroup E, A roadmap to just culture: enhancing the safety environment, september 2004
- Inspectie Gezondheidszorg, Toezicht op IIT, bevindingen vanuit de praktijk, 5 oktober 2016
- Inspectie Gezondheidszorg, Meerjarenbeleidsplan 2016 - 2019
- Inspectie Gezondheidszorg en Jeugd, IGJ Jaarbeeld 2017
- Inspectie Gezondheidszorg en Jeugd, organogram, 2017
- Inspectie Gezondheidszorg en Jeugd, Zo houdt de inspectie de komende jaren toezicht op de verpleeg(huis)zorg, Toezichtvisie op verpleegzorg, juli 2016
- Inspectie Gezondheidszorg en Jeugd, Werkplan 2018
- Inspectie Leefomgeving & Transport, organogram, 2017
- Inspectie SZW, Jaarplan 2018
- LAT Risicobeheersing bedrijven, Landelijke Handhavingsstrategie Brzo 1999
- LAT Risicobeheersing Bedrijven, Tussenrapport Tankopslag, Inspecties van PSG 29, 14 januari 2013
- Ministerie van Infrastructuur en Milieu, Rapportenbundel behorend bij Staat van de Veiligheid Majeure risicobedrijven 2016, 13 juni 2016
- Ministerie van Veiligheid en Justitie, Beleidsreactie inspectierapport KMIde certificering van jeugdbescherming en jeugdreclassering door het Keurmerkinstituut, kenmerk: 2070260, 18 april 2017
- NEN, Safety Culture Ladder Manual, Working safely together, juli 2016

- NIVEL, Conceptueel kader voor de ontwikkeling van toezicht op samenwerking in de zorg en ondersteuning van kwetsbare cliënten thuis, 2016
- Onderzoeksraad voor Veiligheid, Veiligheid Brzo-bedrijven, lessen na Odfjell, 2 maart 2017
- Programma Impuls Omgevingsveiligheid, Impuls Omgevingsveiligheid 2015 – 2018, 1 november 2016
- RIVM, Handreiking voor inspectie van Brzo-bedrijven, Indicatoren en het veiligheidsbeheersysteem, RIVM rapport 2015-0048
- Sixma, H. en D. de Boer, Hoe kan de Inspectie patiëntervaringen benutten? Bruikbaarheid CQ-index voor Risicogestuurd Toezicht IGZ, Kwaliteit in Zorg, nummer 1, 2016
- Stuurgroep Programma Duurzame Veiligheid, Plan van Aanpak Programma Duurzame Veiligheid 2030, Roadmap 3: Transparantie als drijvende kracht voor veiligheid, 22 juni 2017
- Vereniging van Financieringsondernemingen in Nederland, open brief met reactie op Consultatie Wet transparantie toezicht financiële markten, 29 juli 2016
- VOTOB, Safety Maturity Tool, the next step for improving safety performance, European Oil Storage Conference, 31 januari 2014
- VOTOB, Safety Maturity Tool, achtergronddocument, september 2014
- VOTOB, Safety Maturity Tool, resultaten SMT-audits, 4 oktober 2017
- VOTOB, Evaluatie van vijf jaar SMT, 2018
- VOTOB, VOTOB Protocol Safety Maturity Tool, 8 maart 2018
- VOTOB, Voorstel voor [aanpassing van] aanpak van SMT 2018, 8 maart 2018
- Wingerde, K. van, e.a. De praktijk van toezicht in een neoliberaal tijdperk, een casestudy van de taakuitvoering bij de handhaving van arbeidsomstandigheden, 2018