Handreiking BLIC vooruit

Beter Leren van Informatie in de Chemie

Safety Deal

Praktische toepassing van geavanceerde data-analyse-technologie ter verbetering van de procesveiligheid



Brightsite

Transforming industry

Auteurs: Esta de Goede (Sitech) en Johan van Middelaar (TNO) namens de deelnemers aan de Safety Deal BLIC vooruit

Funding: Deze Safety Deal is financieel ondersteund vanuit de Subsidieregeling Versterking Omgevingsveiligheid van het Ministerie van Infrastructuur en Waterstaat uitgevoerd door de Rijksdienst voor Ondernemend Nederland en de bijdragen van de deelnemende partijen.

Maart 2024

Rijksdienst voor Ondernemend Nederland

Samenvatting

Chemelot wil in 2025 de veiligste, meest competitieve en duurzame chemiesite van Europa zijn. Safety Deal 'BLIC vooruit' – Beter Leren van Informatie in de Chemie door vooruitkijken – is een initiatief van Brightsite dat zich richt op de ontwikkeling van een voorspellend model voor procesveiligheid. Binnen BLIC vooruit is een stappenplan ontwikkeld om zwakke signalen en patronen te vinden in fabrieksdata met behulp van innovatieve technieken zoals artificial intelligence (AI). Deze zwakke signalen en patronen kunnen uiteindelijk een model vormen waarmee incidenten voorspeld én voorkomen kunnen worden.

Gebruikmaken van data met AI-technieken
Bedrijven op een chemiesite als Chemelot beschikken over heel veel data, daar wordt echter slechts een klein gedeelte van gebruikt voor veiligheidsdoeleinden. Het voorkomen van incidenten is nu vooral gericht op het naderhand verklaren waarom en hoe een incident heeft kunnen plaatsvinden, er wordt nog maar weinig onderzoek gedaan naar voorspellende modellen voor incidenten. Met de opkomst van AI ontstond het idee of het mogelijk is om, met behulp van AI, informatie uit al deze fabrieksdata te halen. En hoe zou deze data vervolgens gebruikt kunnen worden om de veiligheid van processen te optimaliseren? In een eerder, kleinschaliger project naar procesveiligheid (met één databron, van één bedrijf en met één AI-techniek) is het gelukt om verborgen patronen in veiligheidsdatasets te identificeren met behulp van AI. Patronen die door mensen niet worden gezien. Binnen BLIC vooruit zijn we dit breder gaan trekken en verder gaan ontwikkelen.

Samenwerken in een praktijkgemeenschap
Voor het uitvoeren van BLIC vooruit is een praktijkgemeenschap, een zogenaamde Community of Practice (CoP), opgericht op Chemelot. Deze CoP, met de naam Early Warning Coalitie (EWC) bestaat uit tien partijen: SABIC, Envalior, AnQore, USG, Sitech, TNO, Chemelot Site Permit (CSP), Maastricht University, TU Delft en Safety Delta Nederland. Samenwerking in een CoP kan het leerproces versnellen, omdat bedrijven direct van elkaar leren en niet ieder bedrijf elke stap en elk proces afzonderlijk hoeft te doorlopen. Gezamenlijk proberen we de stap te maken van leren van het verleden naar het voorkomen van incidenten in de toekomst. Dat doen we door te experimenteren met verschillende soorten data(bronnen) en verschillende soorten geavanceerde data-analysetechnieken in te zetten om leerpotentieel en zwakke signalen te vinden. Hierbij wordt, vanaf het begin, rekening gehouden met de mensen die uiteindelijk met de systemen gaan werken, zoals procesoperators in de fabrieken. Daarom wordt er vanaf de werkvloer meegedacht over het model, zodat het nuttig en bruikbaar is in de praktijk.

Handreiking met stappenplan
Met wat we hebben geleerd tijdens BLIC vooruit willen we fabriekseigenaren helpen om de procesveiligheid te verbeteren met behulp van AI. Daartoe hebben we een stappenplan gemaakt. In deze Handreiking staat bovendien beschreven hoe de eerste stappen op deze route genomen kunnen worden, zodat bedrijven niet zelf opnieuw het wiel hoeven uit te vinden. Ook het opzetten en inrichten van een CoP is opgenomen in deze handreiking, evenals de eerste ervaringen van de deelnemers aan de CoP op Chemelot.

We hopen dat u met deze handreiking aan de slag gaat om de veiligheid van uw processen verder te verbeteren.

Inhoudsopgave

Samenvatting 2

Inleiding 4

Stappenplan 6

1. Opzetten en inrichten van een praktijkgemeenschap (CoP) 7
1.1 Voorbereiding: Waar gaat het om? 7
1.1.1 Voorwaarden die het succes van een praktijkgemeenschap bepalen 7
1.1.2 Blokkades 8
1.2 Uitvoering: Hoe doe je dat? 9
1.3 Resultaat: Hoe is het bij Chemelot gegaan? 9

2. Selectie van databronnen met leerpotentieel (zwakke signalen) 12
2.1 Voorbereiding: Waar gaat het om? 12
2.2 Uitvoering: Hoe doe je dat? 13
2.3 Resultaat: Hoe is het bij Chemelot gegaan? 15

3. Selectie van geschikte en effectieve analysetechnieken 17
3.1 Voorbereiding: Waar gaat het om? 17
3.2 Uitvoering: Hoe doe je dat? 17
3.3 Resultaat: Hoe is het bij Chemelot gegaan? 18

4 Identificeren van zwakke signalen in Big Data 20
4.1 Voorbereiding: Waar gaat het om? 20
4.2 Uitvoering: Hoe doe je dat? 20
4.3 Resultaat: Hoe is het bij Chemelot gegaan? 20

5. Vaststellen van leerpotentieel 31
5.1 Voorbereiding: Waar gaat het om? 31
5.2 Uitvoering: Hoe doe je dat? 32
5.3 Resultaat: Hoe is het bij Chemelot gegaan? 33

6 Delen en communiceren van leerpotentieel binnen een CoP 35
6.1 Voorbereiding: Waar gaat het om? 35
6.2 Uitvoering: Hoe doe je dat? 35
6.3 Resultaat: Hoe is het bij Chemelot gegaan? 36

Bijlage A: Waar staan we met betrekking tot leren van eigen informatie? 37

Bijlage B: Geanonimiseerd NDA format ‘BLIC vooruit’ 39

Bijlage C: Enquête ‘begrip voor elkaar’ 44

Bijlage D: Lijst met afkortingen 46

Inleiding

In een eerdere ‘Safety Deal’[1] is er aangetoond dat het haalbaar is om zwakke signalen (weak signals) in Big Data te identificeren, in één databron (wachtverslagen) van één bedrijf (AnQore) met één AI techniek (Natural Language Processing). Dit was de aanleiding voor een vervolgproject, het beter leren, uit meerdere soorten data, van meerdere bedrijven, met behulp van meerdere AI-technieken. Deze Handreiking is het resultaat van dit project, genaamd ‘BLIC vooruit’.

Wat is BLIC vooruit?
De afkorting ‘BLIC vooruit’ staat voor ‘Beter Leren van Informatie in de Chemie door vooruit te kijken’. Deze woordkeuze is meer dan een afkorting, er is over nagedacht: De B staat voor Beter, hieronder vallen begrippen als anders, breder en gezamenlijk. De L staat voor Leren. De I staat voor Informatie, en niet voor Incidenten, vanuit onze overtuiging dat als de (chemische) industrie veiligheidsprestaties significant wil verbeteren, leren van incidenten alléén niet voldoende is. De C staat voor Chemie, omdat deze Handreiking in deze context is gemaakt en voor de (petro)chemische industrie is bedoeld. ‘Vooruit’ staat voor onze droom, dat wil zeggen het aan zien komen en zodoende voorkómen van ongewone voorvallen. Maar ook samenwerken om vooruit te komen, door opgedane inzichten, (verborgen) patronen en zwakke signalen te delen, waardoor we steeds beter worden in het vroeg herkennen van afwijkingen en daardoor proactief kunnen ingrijpen, vóórdat een ongewoon voorval zich ontwikkelt tot een incident.

Van elkaar leren in Community of Practice
Voor de uitvoering van deze Safety Deal is een samenwerkingsverband opgezet in de vorm van een praktijkgemeenschap oftewel ‘Community of Practice’ (CoP) op het chemisch cluster Chemelot in Limburg, de zogenaamde Early Warning Coalitie (EWC). Hierbij wordt opgemerkt dat geografische nabijheid geen voorwaarde is om een CoP op te zetten, dit is ook mogelijk tussen bedrijven die geografisch niet dicht bij elkaar gelegen zijn.

Het doel van de CoP op Chemelot is om beter zelf en van elkaar te leren. Om leerpotentieel met elkaar te delen en zodoende de eigen en de gezamenlijke veiligheidsprestaties te verbeteren. In een consortium met tien deelnemers hebben vier chemiebedrijven op Chemelot geëxperimenteerd met verschillende soorten data en verschillende soorten geavanceerde data-analysetechnieken om na te gaan óf en hoe je beter kunt leren. Samenwerking in een CoP kan het leerproces versnellen, omdat bedrijven direct van elkaar leren en niet ieder bedrijf elke stap en elk proces afzonderlijk hoeft te doorlopen.

6-stappenplan
Deze Handreiking bevat een stappenplan om zwakke signalen en leerpotentieel te identificeren in Big Data en hoe moderne analysetechnieken daarbij kunnen helpen. Denk aan beter en sneller inzicht in het ontstaan en het verloop van afwijkingen in (complexe) processen. Dit biedt kansen om eerder en effectiever in te grijpen in processen die fout dreigen te gaan, waardoor incidenten kunnen worden voorkomen. Het stappenplan begint met het opstellen en inrichten van een praktijkgemeenschap (stap 1), inclusief de voorwaarden en mogelijke blokkades. Daarna volgen de stappen die bedrijven individueel nemen (stap 2 t/m 5), zoals het inventariseren en analyseren van de eigen (vertrouwelijke) data. De daarmee opgedane inzichten en het leerpotentieel, bijvoorbeeld afwijkingen of zwakke signalen die vooraf zijn gegaan aan ongewone voorvallen, worden gedeeld in de CoP (stap 6). Hierdoor kunnen bedrijven ook leren van informatie/ data die niet binnen het eigen bedrijf voor handen is. Het opzetten van een CoP is geen voorwaarde – enkel van meerwaarde – voor de toepassing van geavanceerde data-analysetechnologie ter verbetering van de procesveiligheid. Ook individuele bedrijven kunnen aan de slag met de Handreiking (via stap 2 t/m 5).

Leeswijzer
De hoofdstukken in deze Handreiking behandelen elk een stap uit het stappenplan en zijn steeds op dezelfde manier opgebouwd. Eerst wordt uitgelegd ‘Waar gaat het om?’ (voorbereiding), vervolgens

[1] https://brightsitecenter.nl/procesveiligheid-verbeteren-met-innovatief-ai-model/

wordt ingegaan op ‘Hoe doe je aan?’ (uitvoering) en tot slot wordt het resultaat gedeeld ‘Hoe is het bij Chemelot gegaan?’

Wetenschappelijke onderbouwing
De wetenschappelijke verantwoording van diverse onderwerpen die onderdeel zijn van deze Handreiking is beschreven in een separaat achtergronddocument[2] met bronnen uit de literatuur en theorieën voor veiligheidsmanagement, organisatorisch leren en praktijkgemeenschappen en organisatorische leersystemen.

Over Safety Deal BLIC vooruit
De Handreiking is het resultaat van de Safety Deal ‘BLIC vooruit’ die in de periode 1 januari 2023 t/m 31 maart 2024 uitgevoerd is. Deze Safety Deal is een *cluster-samenwerkingsverband* en gerelateerd aan:

- **De thema’s**: veiligheidscultuur, ketenverantwoordelijkheid, transparante sector, veilige bedrijventerreinen en clusters, en hoogwaardige kennis
- **De speerpunten**: transparante samenwerking tussen bedrijven binnen een cluster en optimalisatie beste werkmethoden en technieken

De namen en rolverdeling van de partners[3] in ‘BLIC vooruit’ zijn in de tabel hieronder te vinden. Contactgegevens van de deelnemers per partner zijn bij de auteurs bekend.

Naam deelnemer	Rol in samenwerkingsverband
Sitech	Penvoerder en ketenpartner: expertise, regie & input handreiking
AnQore	Seveso bedrijf: expertise, leveren data, input handreiking
Envalior Stanyl (Envalior)	Seveso bedrijf: expertise, leveren data, input handreiking
SABIC	Seveso bedrijf: expertise, leveren data, input handreiking
Chemelot Site Permit (CSP)	Seveso bedrijf: expertise, leveren data, input handreiking
USG	Ketenpartner: expertise, review
TNO	Leerprincipes, effectiviteit AI-technieken, samenstellen handreiking
Safety Delta Nederland	Programmabureau: refelectie, disseminatie
Universiteit Maastricht	Onderzoeksinstelling: reflectie, review
Technische Universiteit Delft	Onderzoeksinstelling: reflectie, review

Disclaimer
Deze publicatie is opgebouwd uit feiten en kennis van 1 januari 2023 t/m 31 maart 2024. Hoewel wij onze uiterste best doen om alle informatie zo goed en foutloos mogelijk aan te bieden, kunnen wij niet verantwoordelijk of aansprakelijk gesteld worden voor eventuele fouten. Resultaten zijn gevoelig voor aannames en zijn geen voorspellingen, maar verschaffen inzicht. De besproken aanpak en resultaten in dit rapport komen niet noodzakelijkerwijs overeen met benaderingen van individuele bedrijven. Niets uit deze uitgave mag worden gekopieerd en/ of verspreid door derden zonder toestemming van Brightsite. In de bijlage staan de documenten om zelf mee aan de slag te gaan, deze mogen wel overgenomen worden.

[2] TNO Public TNO 2023 M11444 Samen met een BLIC vooruit, 15 december 2023
[3] Per 1 juni 2023 is de naam van Sitech Services gewijzigd in Sitech

Stappenplan

De activiteiten in deze Handreiking zijn in onderstaand stappenplan samengevat. Het stappenplan helpt om zwakke signalen en leerpotentieel te identificeren met behulp van moderne analysetechnieken. Dit biedt kansen om eerder en effectiever in te grijpen in processen die fout dreigen te gaan, waardoor incidenten kunnen worden voorkomen.

1	Opzetten en inrichten van een praktijkgemeenschap mbt Early Warning (EWC)	a. Bepaal doel, scope, voorwaarden en blokkades b. Identificeer coördinator en deelnemers c. Start, promoot en evalueer regelmatig
2	Selecteer databronnen met leerpotentieel	a. Bepaal doel b. Identificeer en classificeer databronnen c. Beoordeel leerpotentieel van databronnen
3	Selecteer geschikte en effectieve analyse-technieken	a. Bepaal doel b. Kies uit beschikbare analysetechnieken c. Beoordeel geschiktheid en effectiviteit
4	Identificeer zwakke signalen in Big Data	a. Verzamel en verwerk data b. Analyseer en interpreteer data c. Presenteer en visualiseer data
5	Stel leerpotentieel vast	a. Trek conclusies uit de analyse b. Formuleer concrete en meetbare acties c. Overleg met collega's, experts of partners
6	Deel en communiceer leerpotentieel binnen de praktijkgemeenschap	a. Bepaal doelgroep, boodschap en doel b. Kies geschikte platforms, kanalen en instrumenten c. Deel leerpotentieel en context

1 Opzetten en inrichten van een praktijkgemeenschap (CoP)

1.1 Voorbereiding: Waar gaat het om?

Praktijkgemeenschappen (Community of Practice, CoP) zijn groepen individuen of bedrijven die informeel met elkaar verbonden zijn door een gedeelde kennis en interesse in gemeenschappelijke vraagstukken en opgaven, die ze onderling met elkaar uitwisselen om hiervan te leren.

In dit hoofdstuk wordt uitgelegd hoe een praktijkgemeenschap kan worden opgezet, inclusief de eerste ervaring van een groep bedrijven op het chemiecluster Chemelot in Geleen. Dit CoP heeft als doel om gezamenlijk en beter te leren (individueel en van elkaar) om daarmee de eigen- en de gezamenlijke veiligheidsprestaties te verbeteren. Geografische nabijheid is geen voorwaarde om een CoP op te zetten, dit kan ook tussen bedrijven die geografisch niet dicht bij elkaar gelegen zijn. In een CoP werken bedrijven regelmatig samen om te leren en/ of hun werkpraktijk te bevorderen. Praktijkgemeenschappen zijn vaak gericht op het delen van goede praktijken en het creëren van nieuwe kennis om een domein van de beroepspraktijk vooruit te helpen.

1.1.1 Voorwaarden die het succes van een praktijkgemeenschap bepalen

1. **Gedeelde interesse, identiteit en besef van het belang**: Een gedeelde interesse en identiteit helpt bij duurzame onderlinge verbinding. Een gedeelde identiteit ontstaat vanuit een collectief van bedrijven die zich vervolgens positioneren, kennis delen, uitdagingen aanpakken en daarmee waarde toevoegen voor de eigen organisatie en het cluster als geheel. En er moet een zeker besef (awareness) aanwezig zijn voor het belang van samenwerking op gebied van veiligheid.

2. **Ondersteunende omgeving**: De leden streven hun belang na door middel van gezamenlijke activiteiten, discussies, mogelijkheden om problemen op te lossen en delen van informatie. Regelmatige interactie is hierbij belangrijk, zowel face-to-face als web-based ontmoetingen. De notie van een gemeenschap creëert het sociale netwerk om collectief leren mogelijk te maken. Een sterke gemeenschap bevordert interactie en stimuleert de bereidheid om ideeën te delen. De leden van de gemeenschap zijn daadwerkelijk beoefenaars in het gedeelde interessegebied en bouwen een gedeeld repertoire op van middelen en ideeën die zij weer mee terugnemen naar de eigen werkpraktijk en -omgeving.

3. **Continuïteit in deelname**: Om een praktijkgemeenschap te laten voortduren is continue steun en deelname van de leden uit de individuele organisaties nodig. Door deel te nemen aan een gemeenschap kunnen professionals op de hoogte blijven van de nieuwste trends en ontwikkelingen in de branche en hun veiligheidsprestaties verbeteren.

4. **Interne dynamiek en verwachtingen**: Veranderende interne dynamiek (drijfveren) en verwachtingen van de deelnemers hebben effect op resultaat en impact. De idee is dat verwachtingenmanagement leidt tot toenemende energie en met name tot vertrouwen, samenwerking, opbouw en delen van kennis en informatie en steun van de stakeholders.

5. **Nodig om de gemeenschap in stand te houden**: Inventariseer wat nodig is voor continu steun en deelname door leden vanuit de individuele organisaties. Denk aan voldoende capaciteit zoals tijd, kennis, kunde en (digitale) vaardigheden, maar ook aan commitment vanuit de managementteams van elk deelnemend bedrijf. Ga na of er (verborgen) weerstanden zijn, angst of onzekerheid om informatie te halen, te brengen of toe te passen. Ga na hoe deelnemers elkaar op de hoogte houden van actualiteiten, trends en ontwikkelingen op het cluster of in de sector. Ga na of er 'verschillen' zijn tussen bedrijven in beschikbare middelen en/ of kennis om in een CoP te halen of te brengen. Voor bedrijven met minder middelen/ kennis kan dit namelijk zorgen voor een ongelijke

onderhandelpositie bij het nemen van beslissingen. Belangrijk is dat hierover op voorhand goede afspraken worden gemaakt, zodat partijen gelijkwaardig in het CoP staan.

6. **Zorg voor een transparante cultuur**: Een cultuur waarin mensen zich vrij en veilig voelen om zaken bespreekbaar te maken, zonder angst voor sancties of represailles. Onderdeel hiervan is transparante communicatie over ongewone voorvallen, leerpotentieel en verbeteracties, inclusief uitwisseling van meningen, ervaringen, suggesties en constructieve feedback. Een cultuur waarin een hoge mate van onderling vertrouwen aanwezig is, zoals bij 'trusted communities'.

7. **Leren van anderen**: Het is belangrijk om eerst te leren van eigen informatie, voordat kan worden geleerd van anderen. Bedrijven in de chemische industrie leren voornamelijk van incidenten. Door eerst te leren van eigen incidenten kan gereflecteerd worden op het eigen handelen en kan begrip en compassie voor de eigen zwakke punten en die van anderen ontstaan. Door te leren van eigen informatie wordt een lerende grondhouding ontwikkeld, die helpt om open te staan voor feedback, perspectieven en alternatieven. Elke deelnemer kan nagaan wat al goed gaat en wat beter kan met betrekking tot het leren van incidenten, door gebruik te maken van de checklist in bijlage A.

1.1.2 Blokkades

Uit onderzoek[4] is gebleken is dat er verschillende blokkades zijn die opgelost moeten worden voor het aangaan en opzetten van een samenwerkingsverband zoals een CoP.

1. **Concurrentiegevoeligheid, ethiek en privacy**: Dit betekent dat er ethische of privacy kwesties zijn die het leren van informatie beïnvloeden. Er kunnen bijvoorbeeld zorgen zijn over herkomst, kwaliteit, nauwkeurigheid, relevantie, representativiteit of actualiteit van informatie. Er kunnen ook zorgen zijn over rechten, belangen, verwachtingen, toestemming of autonomie van informatiebronnen, informatiegebruikers of informatieontvangers.

2. **Juridisering**: Dit betekent dat er juridische beperkingen, risico's of verplichtingen zijn die het delen of gebruiken van informatie beïnvloeden. Er kunnen bijvoorbeeld:
   - Regels zijn over mededinging, aansprakelijkheid, geheimhouding, bescherming of naleving van de informatie
   - Contracten, overeenkomsten, vergunningen of vergoedingen zijn die het leren van informatie reguleren of beperken
   - Problemen zijn met betrekking tot intellectueel eigendom, privacy, ethiek of wetgeving van informatie

   Het gebruik van een (uniforme) NDA of andere overeenkomst kan helpen om deze blokkade weg te nemen.

3. **Gebrekkige vertrouwensrelatie**: Een vertrouwensrelatie tussen de partijen is een cruciaal punt in een praktijkgemeenschap, omdat het de basis vormt voor open communicatie en samenwerking. Wanneer er vertrouwen is tussen de partijen, zullen ze makkelijker informatie delen, feedback geven en ontvangen en samenwerken aan gemeenschappelijke doelen. Bovendien kan een vertrouwensrelatie tussen de partijen bijdragen aan een positieve (veiligheids)cultuur en een gevoel van verbondenheid en betrokkenheid bij de gemeenschap.

4. **Te geavanceerde (data-analyse) technologie**: Dit betekent dat de technologie die gebruikt wordt om informatie te genereren, verwerken, analyseren, presenteren of verspreiden niet begrijpelijk, betrouwbaar, veilig of compatibel is. Er kunnen ook technische storingen, fouten of beperkingen zijn die de toegang tot- of het gebruik van informatie bemoeilijken.

5. **Organisatorische blokkades**: Dit betekent dat de organisatie waarin het leren van informatie plaatsvindt niet over de nodige middelen, structuren, processen, culturen of strategieën beschikt om het leren van informatie te ondersteunen, stimuleren of belonen. Er kunnen ook conflicten, concurrentie, 'silo's' of hiërarchieën zijn die samenwerking, communicatie, feedback of innovatie belemmeren.

[4] TU Delft, van Nunen, Reniers, Swuste, Verkennende studie naar (petro)chemische clusters, veiligheid: Veiligheidsparameters binnen (petro)chemische clusters en losstaande (petro)chemische bedrijven, 2019 en van Nunen, Reniers, (Petro)chemische clusters en veiligheid: Drijfveren en hindernissen voor samenwerking, 2022. Crisislab, Ira Helsloot, Handreiking Beter leren van incidenten in de (petro)chemische industrie, 2020.

1.2 Uitvoering: Hoe doe je dat?

In deze sectie is samengevat met welke zaken rekening moet worden gehouden bij het opzetten en inrichten van een praktijkgemeenschap (CoP). Volg daartoe onderstaande checklist.

Checklist voor oprichten Community of Practise

Algemene voorwaarden

- ☐ Gedeelde interesse en besef van het belang: Wat gaat goed? Wat kan beter?
- ☐ Herkenbare identiteit op basis van (unieke) kennis en kunde
- ☐ Meerwaarde van de CoP voor de deelnemende organisaties
- ☐ Ondersteunende omgeving: Wat is nodig om te coördineren? Wie doet dat? Wie zijn deelnemers? Wat brengen en halen deelnemers?
- ☐ Transparant hebben/ maken van wat je kunt/ wilt/ mag delen
- ☐ Regelmatig (face-to-face) meetings, elkaar persoonlijk leren kennen
- ☐ Uniforme NDA (passend per partij) en juristen vroegtijdig betrekken
- ☐ IT (security) betrekken en support regelen

Specifieke voorwaarden

- ☐ Voldoende capaciteit: kennis, kunde, vaardigheden, competenties en tijd
- ☐ Delen van kennis voortvloeiend uit de lessen in afstemming met gebruikers
- ☐ Onderhouden van divers leeraanbod met meerdere leermiddelen
- ☐ Rekening houden met verschillende niveaus van digitale vaardigheden

Mogelijke blokkades

- ☐ Concurrentiegevoeligheid, ethiek, privacy
- ☐ Juridisering
- ☐ Vertrouwensrelatie
- ☐ Beschikbaarheid van capaciteit: kennis, kunde, vaardigheden en tijd
- ☐ Wantrouwen bij één of meerdere deelnemers
- ☐ Obstructies om data te delen
- ☐ Complexiteit en toepasbaarheid van (nieuwe, geavanceerde) technologie
- ☐ Beheer van dataopslag: Wie levert? Wie is eigenaar? Wie kan erbij? Wie beheert?
- ☐ Technologie voor dataopslag: Waar staat data (eigen server, systeem, web)?

1.3 Resultaat: Hoe is het bij Chemelot gegaan?

Chemelot is een chemiecluster gelegen in het zuiden van de provincie Limburg tussen de gemeentes Sittard-Geleen, Stein en Beek. Op Chemelot bevinden zich ca. 60 chemiebedrijven, van klein tot groot. Het is de ambitie van Chemelot om de meest veilige, concurrerende en duurzame chemie & materialensite in West-Europa te zijn. De partijen die in deze Safety Deal data leveren zijn allen gevestigd op Chemelot. Geografische nabijheid wil echter niet zeggen dat ze daardoor gelijk zijn in ideeën over voorwaarden en blokkades. Op het gebied van voorwaarden is er veel gelijkenis, bij blokkades zijn er verschillen.

Algemene voorwaarden

Partijen op Chemelot hebben als startpunt een gezamenlijke ambitie om de meest veilige site van West-Europa te zijn. Een aantal partijen op Chemelot heeft een gedeelde interesse om Big Data en AI

in te zetten in het veiligheidsdomein. Zij geloven in de inzet van AI-technieken voor de analyse van Big Data met als doel daarmee ongewone voorvallen te voorkomen. Zij zijn ervan overtuigd dat er zwakke signalen en patronen zijn die voorafgaan aan ongewone voorvallen. Deze 'believers' (AnQore, Envalior, CSP en SABIC) hebben zich voor de Safety Deal 'BLIC vooruit' verenigd in een Early Warning CoP (EWC) en nemen deel aan dit project.

Chemelot is een chemisch georiënteerd terrein van 800 hectare groot in Zuid Limburg en een belangrijke economische motor van Limburg en Nederland. Het terrein is uniek vanwege tal van elementen: de centrale ligging in West-Europa, de goede bereikbaarheid, de aanwezigheid van een groot aantal fabrieken die elkaar aanvullen en op unieke wijze samenwerken en de aanwezigheid van de Brightlands Chemelot Campus met research en pilot plants. Het terrein huisvest bijna honderdvijftig instellingen en bedrijven waaronder de bedrijven in deze Safety Deal, AnQore, Envalior, SABIC, Sitech, USG en CSP.

Binnen het EWC is AnQore de 'early adapter' van de combinatie AI en Big Data. Met Brightsite, het kenniscentrum voor de verduurzaming van de industrie, zijn eerdere projecten uitgevoerd, waardoor de spelers elkaar kennen, de manier van denken bekend is en er veel interessante ideeën zijn. Deze kennis heeft AnQore ingebracht in het EWC. SABIC heeft een corporate programma en interesse op gebied van AI en Big Data in een fabrieksomgeving. Envalior gelooft binnen alle lagen van de organisatie in Big Data en AI, zowel binnen de centrale staforganisatie als bij de betrokken fabriek (Stanyl) waarvan databronnen gebruikt zijn voor 'BLIC vooruit'. CSP[5] heeft diverse onderzoeken laten uitvoeren naar (gemeenschappelijke) oorzaken voor incidenten op Chemelot en vraagt zich af wat de combinatie Big Data en AI voor hen kan betekenen.

Om aan de slag te gaan met data is een Non-Disclosure Agreement (NDA) wenselijk. Binnen 'BLIC vooruit' is gekozen voor een uniforme opzet van de NDA (zie bijlage B).
Het tekenen van een NDA vergt tijd en goed contact met een jurist, waarbij de tijd nodig voor het getekend krijgen van de NDA varieerde tussen de 2 weken en 6 maanden.

Binnen 'BLIC vooruit' is een overlegstructuur opgezet, waarin naast de face-to-face kick-off en de afsluitende sessie, er maandelijkse digitale bijeenkomsten waren met alle partijen waarin de voortgang besproken werd. Figuur 1.1 toont de 'Terms of Reference' van het maandelijks digitale overleg.
Daarnaast waren er regelmatige bijeenkomsten tussen de afzonderlijke data-leverende partijen TNO en Sitech. De coördinatie van het geheel lag in handen van Sitech. De afstemming rond IT (security) is door iedere partij zelf georganiseerd.

Terms Of Reference : Voortgangsoverleg BLIC vooruit

<table>
<tr>
<td>Meeting: Voortgangsoverleg
Frequentie: Maandelijks op de 3e donderdag
Duur: 1 uur
Locatie: Teams</td>
<td>Deelnemers:
• Penvoerder (vz)
• Inhoudelijke contactpersonen</td>
<td>Doel van het overleg:
Monitor and discuss progress BLIC vooruit
• Status
• Bottlenecks
• Communication</td>
</tr>
<tr>
<td colspan="2">Input:
1. ppt former meeting
2. Topics...</td>
<td>Output:
1. ppt with main topics discussed including Actions & Decisions</td>
</tr>
<tr>
<td colspan="2">Agenda:
1. Action & decision list
2. ppt former meeting
3. Status
4. Bottlenecks
5. Communication
6. Recap actions & decisions
7. aob</td>
<td>Vergaderafspraken:
• Focus on the agenda
• No allocations of actions to non attendants</td>
</tr>
</table>

[5] Chemelot Site Permit – de beheerder van de koepelvergunning voor Chemelot

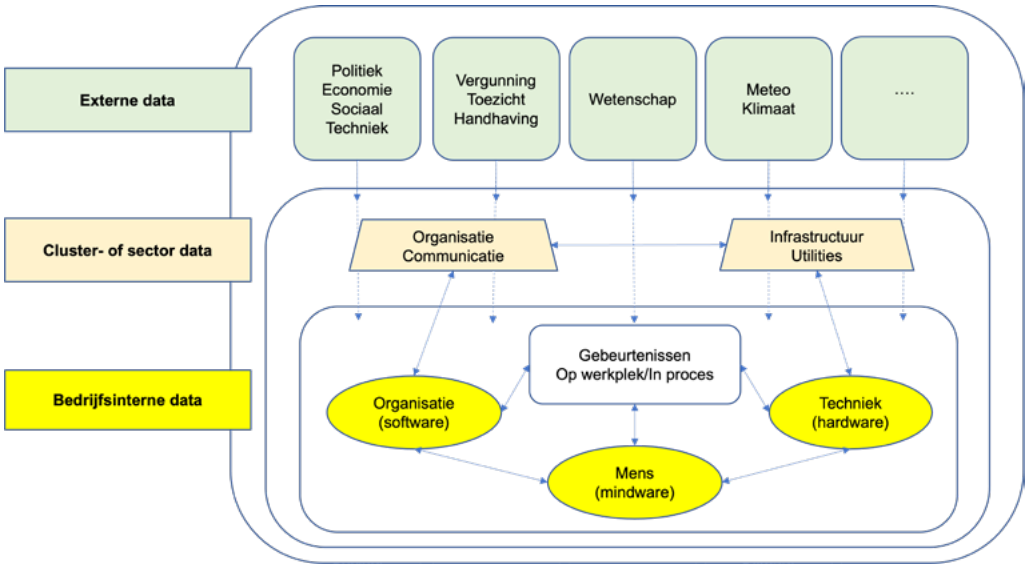
Specifieke voorwaarden
De chemische industrie leert tot nu toe vooral van incidenten. Dit is de basis waar we als EWC staan. Om erachter te komen hoe we daar ten opzichte van elkaar staan hebben de EWC-deelnemers de 'Leren van Incidenten' checklist uit bijlage A ingevuld. De deelnemers op Chemelot bleken op hetzelfde niveau te zitten, met ongeveer dezelfde aandachtspunten en verbetergebieden. Bij alle partijen zijn kennis, kunde en (digitale) vaardigheden aanwezig. Het vinden van voldoende prioriteit en tijd binnen een drukbezette organisatie bleek voor alle partijen een uitdaging. Flexibiliteit in denken en handelen is dan nodig.
Contactpersonen waren divers en mede afhankelijk van de gekozen databronnen en beoogde zwakke signalen. In deze Safety Deal waren onder andere betrokken: diverse engineers, een SHEQ manager, chefs van dienst, een plant- en productiechef en een maintenance supervisor. In sommige gevallen was het beoogd resultaat te groot. Het vinden van balans tussen een (toepasbaar) resultaat op korte termijn en een lange termijn doel is belangrijk ook om de interesse in het onderwerp van niet-deelnemende partijen vast te houden.

Mogelijke blokkades en succesfactoren
Verschillen tussen partijen zijn vooral bij mogelijke blokkades te vinden. SABIC heeft strenge IT-security eisen, het gebruik van de 'Cloud' en internet zijn gebonden aan restricties. Het productieproces van Envalior Stanyl is uniek, data in de 'Cloud' is niet toegestaan. Dit beperkt de inzet van vertaalprogramma's en daarmee, omdat de databronnen in het Nederlands zijn, de inzet van Engelstalige AI-tools. De manier van data-delen en data-opslag gaf daarentegen weinig discussie, wel enige uitdaging rondom cyber-security. De voorkeur had een werkwijze met data offline in files, bij voorkeur versturen via een safe-link, analyses met AI-tools op een server van TNO of van het eigen bedrijf. Persoonlijk contact met juristen/ IT- mensen bleek van cruciaal belang om blokkades weg te nemen, het sturen van mails is minder succesvol. Bij het opstellen van de NDA met CSP kwam de Wet Openbare Overheid (WOO) ter sprake. En in hoeverre valt TNO onder de WOO regels? Met andere woorden: kan het resultaat van een eventueel AI-experiment en/ of kan de onder NDA overgedragen data opgevraagd worden? Deze blokkade heeft tot de nodige vertraging geleid. Toelichting door een bestuursrechtjurist van TNO heeft helderheid in WOO gebracht en tot aanpassing in de NDA geleid (benadrukken van bedrijfsgevoeligheid van data).
De beelden bij succes verschillen door de ervaring die men al of niet heeft met Big Data. Daarnaast kan door een verschil in verwachtingen aan het resultaat de ene partij iets als een succes zien en de andere partij niet. In het algemeen kan gesteld worden dat het beter is om klein te beginnen, zodat de beschikbare tijd – die in de praktijk altijd minder is dan gedacht – ook echt tot een resultaat leidt.

2 Selectie van databronnen met leerpotentieel (zwakke signalen)

2.1 Voorbereiding: Waar gaat het om?

De eerste stap – nadat de CoP is opgericht – is dat elke deelnemer eerst voor zichzelf nagaat welke databronnen mogelijk leerpotentieel (zwakke signalen) bevatten. Daarna wordt dit met alle deelnemers gedeeld en wordt afgestemd wie welke data zal analyseren, hoe dat wordt gedaan (welke analysetechniek), wat mogelijk leerpotentieel is en de samenhang daarvan en hoe deze toegepast kunnen worden. Er zijn in principe drie soorten databronnen waaruit kan worden gekozen, ook wel het 'socio-technisch systeem' genaamd (zie Figuur 2.1): bedrijfsinterne data, sector- of clusterdata en externe data.



Figuur 2.1 Overzicht van soorten databronnen in een socio-technisch systeem

Bedrijfsinterne databronnen zijn bijvoorbeeld gegevens over de organisatie (zoals bedrijfsgrootte, omzet, inspectierapporten, meldingen), technische gegevens (zoals operationele gegevens, procesdata of storingsdata) en informatie over het personeel (zoals opleiding/ training, kennis, ervaring, ploegdata).

Sector- of clusterdata zijn bijvoorbeeld gegevens over het aantal en soort bedrijven of leden, wijze van samenwerking, onderlinge relaties, wederzijdse afhankelijkheden, ligging en omgeving, communicatie, logistiek en infrastructuur. Er kan ook worden gedacht aan databanken, waarin feiten en kennis wordt verzameld en beschikbaar gesteld, zoals interne (ongevallen) databases, externe (ongevallen) databases, Storybuilder, FACTS (Failure and Accidents Technical Information System), eMARS (Major Accident Reporting System) of Process Safety Incident Databases.

Externe databronnen zijn gegevens die afkomstig zijn 'van buiten', zoals inspectierapporten van toezichthouders, onderzoeksrapporten, wetenschappelijke publicaties of meteorologische data, maar ook wet- en regelgeving, normen en richtlijnen, 'citizen science', nieuwsberichten en social media.

2.2 Uitvoering: Hoe doe je dat?

In deze sectie de stappen voor het identificeren van databronnen met leerpotentieel (zwakke signalen). Het gaat daarbij met name om (soorten) databronnen met leerpotentieel op basis van (vermoedelijke) aanwezigheid van signalen. Dit kunnen zowel sterke signalen (zoals leren van incidenten) als zwakke signalen (zoals op basis van patronen of trends) zijn. Bij 'BLIC vooruit' ligt de nadruk op zwakke signalen.

1. **Inventariseer databronnen:**
   Elke deelnemer gaat eerst voor zichzelf na welke data-bronnen mogelijk leerpotentieel bevatten. Vervolgens wordt gezamenlijk besproken in de CoP:
   - De mogelijke databronnen en de afstemming wie welke databron gaat analyseren en hoe dat wordt gedaan (bijvoorbeeld welke analysetechniek kan worden gebruikt).
   - Het verwachte leerpotentieel en de samenhang

   Tabel 2.1 kan gebruikt worden om databronnen te selecteren.

2. **Beoordeel de databronnen op toepasbaarheid, bruikbaarheid en toegankelijkheid:**
   Welke soort data bevatten de databronnen, denkend aan tekst, getallen, 'time series', grafieken, tabellen, diagrammen, beelden of geluiden? Zijn de databronnen statisch of dynamisch? En hoe moeten de databronnen 'opgeschoond' of gefilterd worden om de data geschikt te maken voor analyse cq. analysetechniek?

3. **Beoordeel het verwachte leerpotentieel van de databron:**
   Kan de data worden omgezet naar bruikbare en overzichtelijke informatie? Hoe helpt deze informatie om leerdoelen te bereiken of om de veiligheid te verbeteren? Dit kun je doen door te kijken naar de aanwezigheid van sterke of zwakke signalen in de databronnen. Let daarbij op:
   1. Signalen die kunnen leiden tot (zeer) ernstige effecten
   2. Complexe situaties en/ of patronen
   3. Combinaties van verschillende (zwakke en sterke) signalen op hetzelfde moment

Onderstaand kader geeft nadere informatie omtrent sterke en zwakke signalen. Binnen de Safety Deal 'BLIC vooruit' lag de nadruk op zwakke signalen.

Sterke signalen zijn duidelijke, expliciete of directe indicatoren van relevante gebeurtenissen, situaties of problemen die je kunt leren. Typische kenmerken zijn:

a. Ze verwijzen naar duidelijke gebeurtenissen, situaties of problemen die gemakkelijk te identificeren en te begrijpen zijn. Deze gebeurtenissen, situaties of problemen hebben vaak directe en ernstige gevolgen voor mens, milieu, installatie of reputatie.
b. Ze zijn veelal voor de hand liggend en vereisen onmiddellijke aandacht.
c. Het leren van sterke signalen is relatief eenvoudig, omdat de oorzaak-gevolgrelaties meestal duidelijk zijn. Er is meestal geen twijfel over wat er moet worden verbeterd om herhaling te voorkomen.

Zwakke signalen zijn vage, impliciete of indirecte indicatoren van potentiële, toekomstige of latente gebeurtenissen, situaties of problemen die je kunt leren. Typische kenmerken zijn:

a. Ze zijn subtieler en moeilijker te herkennen. Ze zijn vaak verborgen in de dagelijkse gang van zaken en lijken op zichzelf niet ernstig. Ze kunnen wijzen op opkomende risico's of problemen die zich in de toekomst kunnen ontwikkelen.
b. Zwakke signalen worden vaak over het hoofd gezien of genegeerd, omdat ze geen directe en ernstige gevolgen hebben. Dit kunnen bijvoorbeeld herhaalde vervelende gebeurtenissen, ongewone trends, bepaalde afwijkingen of variaties of ongebruikelijke patronen zijn.
c. Het leren van zwakke signalen vereist een diepere analyse en het vermogen om verbanden te leggen tussen ogenschijnlijk onbelangrijke gebeurtenissen. Het is een proactieve aanpak om potentiële problemen te identificeren en te voorkomen voordat ze ernstig worden.

Tips voor het selecteren van databronnen:

- Relevant, beschikbaar en toegankelijk
- Kies niet te snel een databron
- Denk na of een databron voldoende dynamisch is. Hiermee wordt bedoeld variërend in de tijd en niet statisch
- Ga na of de databron gedeeld mag/ kan worden
- Ga na hoe of (hoe eenvoudig) de data op te halen is
- Ga na hoeveel capaciteit nodig is voor data 'opschonen'
- Ga na of en hoeveel capaciteit nodig is voor omzetten data naar 'leesbaar' bestand
- Realiseer je dat databronnen in de Nederlandse taal niet zomaar door Engelstalige AI-tools geanalyseerd kunnen en mogen worden

Soort	Databron	Typische elementen in deze databron waaruit mogelijk te leren is
Bedrijf	Openbaar	Adres, ligging, bedrijfstype, categorie, sector, volume, doorzet, soorten (gevaarlijke) stoffen, omzet, winst, personeel (aantal, verdeling, leeftijd, geslacht)
	Personeel	Geboortedatum, beroep, functie, taak of rol, certificaten, opleiding, ervaring, kennis, training, kwalificaties, senioriteit, verzuim, werktijden, contract, medische gegevens, keuringen
	Ploegen	Aantal, verdeling, werklocaties, werktijden, grootte, capaciteit, taken, werkbelasting, planning, storingen, spoedklussen, personeelsverloop, minimale grootte, kennis, ervaring, niveau verzuim, ongewone voorvallen
	Systeem	Beleid, RIE, veiligheidsstudies, procedures, assessments, meldingen, metingen, audits, inspecties, MOC, databases, actielijsten
	Operaties	Wachtdienstverslagen, dagverslagen, overleggen, afwijkingen, spoed acceptaties, werkvergunningen, ATEX
	Onderhoud	Assets, interval, reparaties, testen, duur, prioriteit, overdues, tipping points, interface, subcontractors, scope changes, rapporten
	Proces	Procesparameters, indicaties, alarmen, interlocks, overbruggingen, (open) notificaties, (duur van) overdues en prioriteiten
	Ongewone voorvallen	Tijd, dag, datum ongewoon voorval, type ongewoon voorval, soort schade/ leed, type/ geslacht/ leeftijd betrokkenen, directe oorzaak, achterliggende oorzaak, locatie, soort/ ernst letsel, type verzuim, hersteltijd, arbeidsomstandigheden, beschermingsmiddelen, status gereedschap, machine of procescondities
Cluster	Openbaar	Aantal bedrijven, mensen, soort, ligging, vergunning, regels, infrastructuur, faciliteiten, processen, (gevaarlijke) stoffen, onderlinge relaties, interfaces
	Systeem	Toegangsregels, poortintroductie, veiligheidsinformatie, afspraken, regels, onderlinge risico's, onderling leren, standaards, contractormanagement, communicatie
	Operaties	Observaties, inspecties, risico inventarisaties, audits, management reviews
	Incidenten	Ongevalsrapporten, analyses (zie ongewone voorvallen)
Extern	Toezichthouders	Grootte bedrijf, bevindingen, overtredingen, geslacht werknemers, type werknemers, aanleiding, gebeurtenissen, waarnemingen, bron verwondingen, onveilige handelingen, onveilige omstandigheden, soort ongeval, ongevalsinterval, arbeidsnationaliteit, sterftecijfers per 1.000 werknemers, verdeling naar ongevalstijden, ongevalsmaand of bronnen van letsel, aantal slachtoffers per ondernemingsgrootte
	Sector	Nieuws, artikelen, alerts, vakbladen, congressen, rapporten, peer reviews, benchmarks, normen, standaards, best practices, incidentdatabase
	Wetenschap	Onderzoek, publicaties, innovaties
	Meteo	Wind, temperatuur, relatieve vochtigheid, zon, neerslag, bewolking, bliksem

Tabel 2.1 Voorbeelden van databronnen

2.3 Resultaat: Hoe is het bij Chemelot gegaan?

Het startpunt bij de keuze van een (Big) databron waarin zich mogelijk zwakke signalen bevinden kan vanuit de databron of het mogelijk zwakke signaal starten. Op Chemelot zijn beide manieren voorgekomen: twee partijen hadden beelden bij een zwak signaal en zijn op zoek gegaan naar databronnen en twee partijen hadden databronnen waarvan zij wilden weten of die mogelijk zwakke signalen bevatten. Daarnaast is de keuze van een databron en mogelijk zwak signaal een iteratief proces. Het vergt tijd en denkwerk.

Een databron kan verschillende typen data bevatten. Het kan gaan om tekst, getallen, tabellen en time-series, maar ook om grafieken, diagrammen, beelden en geluiden.
Op Chemelot zijn drie partijen aan de slag gegaan met tekst en één partij met getallen.

AnQore
AnQore heeft als droom het ontwikkelen van een 'Early Warning systeem' op basis van meerdere, interne en externe databronnen. In eerdere projecten heeft AnQore wachtdienstverslagen en incidentrapportages als databron gebruikt om zwakke signalen te vinden. In 'BLIC vooruit' zijn twee databronnen gekozen, namelijk onderhoudsdata en meteodata. In een gemengd team, bestaande uit de Supervisor Maintenance, Reliability Engineer, SHEQ Manager, Risk Assessment Officer en Data Scientist, zijn de diverse onderhouds-databronnen en meteo-databronnen nagegaan. Kansrijke databronnen zijn data die voldoende dynamisch zijn (zijnde variërend in de tijd en niet statisch) in combinatie met voldoende ideeën over de mogelijk zwakke signalen in deze databronnen. AnQore is met twee soorten databronnen aan de slag gegaan, namelijk meteorologische data, zoals temperatuur, relatieve vochtigheid en windsnelheid, en onderhoudsdata, zoals 'notifications' (meldingen) in de diverse fabrieksonderdelen.

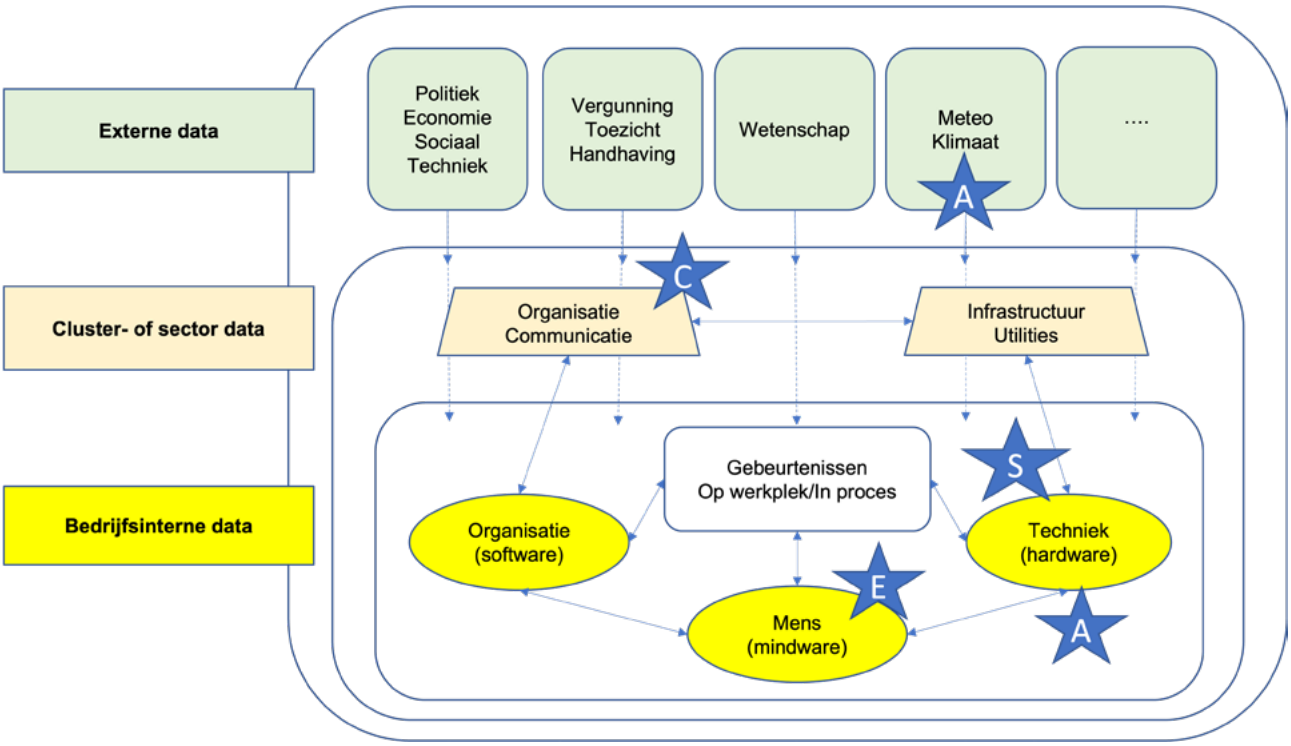
Envalior
Envalior is op zoek naar manieren om het 'begrip voor elkaar' tussen productie en staf te verbeteren. 'Begrip voor elkaar' (of het voorkomen van miscommunicatie) is hier een mogelijk zwak signaal. In een gemengd team, bestaande uit een Shift Supervisor, de Operations Manager en een Data Scientist, zijn diverse databronnen nagegaan. Uiteindelijk is het wachtdienstverslag als de meest kansrijke databron geselecteerd om mee aan de slag te gaan. Dit met als motivatie dat een wachtdienstverslag de verwoording van een ploeg over een dienst is, waaruit de staf vervolgens kan afleiden welke onderwerpen nadere aandacht verdienen en waar zorgen liggen. Het gaat hier niet om de sterke signalen zoals 'leiding verstopt', 'product off-spec'. Maar meer om zwakkere bewoordingen zoals 'weer te veel fines', 'doorstroming fluctueert'.

SABIC
SABIC werkt veel met Key Performance Indicators (KPI) met een relatie tot veiligheid. Als een individuele KPI 'rood' wordt, dan volgt er actie op die betreffende KPI. SABIC wil graag de afzonderlijke KPI's gaan combineren om zo een completer en daarmee beter beeld te krijgen van wat er speelt. De gedachte hierbij is dat het verloop van een KPI en combinaties van KPI's patronen kunnen geven. In een team, bestaande uit een Process Control Engineer, het Focal Point Digitalisering, de Senior Manager Polymer Process Engineering en een Data Scientist, zijn de mogelijke databronnen en features in scope besproken. Al snel werd duidelijk dat de diverse databronnen teveel variatie in format, opzet en analysemethode geven. Geconcludeerd werd dat alles oppakken teveel was en er moesten keuzes gemaakt worden. Besloten is om met informatie uit het DCS systeem aan de slag te gaan. De zwakke signalen die hierin zouden kunnen zitten, hebben betrekking op zaken als 'setpoint changes', 'echte trips', 'regelingen automatisch' of op 'hand en active/ acknowledged alarmen'.

CSP
Chemelot Site Permit (CSP) zou graag willen onderzoeken of er zwakke signalen te vinden zijn in haar archief in aanloop naar 2015/ 2016. In deze jaren is Chemelot namelijk getroffen door een serie incidenten. Het archief van CSP is beoordeeld op relevante documenten en de rapporten van reviews, inspecties en corporate audits uitgevoerd door CSP, de bedrijven of de overheid zijn als meest kansrijk bestempeld om te onderzoeken. De vraag om alle incidenten in 2015/ 2016 in scope te nemen bleek te groot en is versmald tot het analyseren van informatie in het CSP-archief voor één bedrijf.

Overall beeld gekozen databronnen
De uiteindelijk gekozen databronnen passen als volgt in het socio-technisch systeem op Chemelot (zie figuur 2.2):

- AnQore: onderhoudsmeldingen en meteo (temperatuur, relatieve vochtigheid, windsnelheid)
- Envalior: wachtverslagen (tekst)
- SABIC: DCS automation data (numeriek)
- CSP: CSP-inspecties, inspecties door Provincie Limburg, achteraf-rapportages en managementreviews (tekst)



Figuur 2.2 Plaats van de gekozen databronnen in 'BLIC vooruit' in het socio-technisch systeem (A =AnQore, E=Envalior, S=SABIC, C=CSP)

3 Selectie van geschikte en effectieve analysetechnieken

3.1 Voorbereiding: Waar gaat het om?

Geavanceerde technologie voor data-analyse kan organisaties helpen om beter, effectiever en sneller te leren van informatie. Er zijn verschillende digitale tools en analysetechnieken beschikbaar, zowel voor het ondersteunen van praktijkgemeenschappen, individuele bedrijven als voor specifieke doelen of doelgroepen. Voor geavanceerde technologie als analysevorm is het echter van belang te realiseren dat de inzet van AI niet direct leidt tot inzichten uit data waar zelfstandig opvolging aan kan worden geven.

In de toepassing van geavanceerde technologie zijn drie fasen te onderscheiden, namelijk:

1. **Descriptieve analyse**: identificeren en visualiseren van patronen met geavanceerde statistische algoritmen (beschrijvend)
2. **Voorspellende analyse**: wat kan er gebeuren en modelleren voor de huidige en toekomstige situaties
3. **Prescriptieve analyse**: wat moet ik doen door geanalyseerde procesgegevens om te zetten naar voorspelling c.q. handvatten voor preventie of verbetering van veiligheid

Binnen 'BLIC vooruit' wordt vooral descriptieve analyse toegepast. We kijken namelijk terug in beschikbare informatie om te leren of en welke zwakke signalen er zijn die vooraf gaan aan ongewone voorvallen.
Voor descriptieve data-analyse zijn veel verschillende soorten tools beschikbaar, zoals Excel, Python, R, Power BI, Minitab en SPSS. Excel heeft een gebruiksvriendelijke interface, waardoor het goed te gebruiken is voor eenvoudige data-analysetaken, zoals kleine datasets. Excel is ook krachtig voor het maken van rapporten en dashboards. R en Python zijn populaire programmeertalen voor gegevensanalyse en -verwerking en bieden een breed scala aan bibliotheken en frameworks voor meer complexe analyses en grotere datasets. AI vergelijken met Excel, R en Python is echter 'appels met peren' vergelijken: AI bestaat uit methodologieën, wiskundige modellen, enz., terwijl Python, R, enz. hulpmiddelen zijn om deze methodologieën te implementeren. In tegenstelling tot Excel, R en Python, die voornamelijk worden gebruikt voor het analyseren van gestructureerde gegevens, kan AI ook ongestructureerde gegevens zoals tekst, spraak en afbeeldingen analyseren. Dit maakt het mogelijk om inzichten te verkrijgen uit gegevens die anders moeilijk te interpreteren zouden zijn. Bovendien kan AI worden gebruikt om taken te automatiseren en de efficiëntie te verbeteren. AI is daarom een waardevolle aanvulling op Excel, R en Python, omdat het kan worden gebruikt om inzichten te verkrijgen uit ongestructureerde gegevens en om taken te automatiseren.

3.2 Uitvoering: Hoe doe je dat?

In deze stap gaat elke deelnemer aan de slag met zijn/ haar eigen data en kiest daarvoor in samenspraak met een Data Scientist een analysetechniek. De keuze van de analysetechniek hangt sterk af van zowel het type gegevens (databronnen) als de specifieke doelen van de analyse.

De stappen voor het selecteren van de meest geschikte en effectieve analysetechnieken zijn als volgt:

1. Bepaal de input: neem het overzicht van databronnen uit stap 2 met te analyseren data (input) en wat het leerpotentieel is
2. Bepaal de output: ga na wat nodig is om data op te schonen (filteren) om specifiek leerpotentieel uit de data te halen
3. Kies de analysetechniek (proces): er zijn verschillende data-analysetechnieken voor het identificeren van afwijkingen, patronen en/ of zwakke signalen in Big Data.

Elke techniek heeft zijn eigen sterke en zwakke punten. De keuze van de juiste techniek hangt af van de specifieke toepassing en het type data dat wordt geanalyseerd (zie kader)

4. Bepaal hoe de resultaten (kenmerken, leerpotentieel, patronen) gevisualiseerd kunnen worden. Denk bijvoorbeeld aan spreidingsdiagrammen, staafdiagrammen en boxplots voor numerieke analyse of word clouds voor tekstgegevens

Voorbeelden data-analysetechnieken:

1. **R en Python**: tools om data-analysetechnieken uit te voeren. R is een programmeertaal die speciaal is ontworpen voor statistische analyse en grafische weergave van gegevens. Het heeft een uitgebreide bibliotheek die handig is voor het werken met gestructureerde gegevens. Python wordt gebruikt voor een verscheidenheid aan toepassingen, waaronder data-analyse, en biedt verschillende tools om met ongestructureerde data te werken.
2. **Text mining en Natural Language Processing** (**NLP**): computers trainen om natuurlijke taal te begrijpen en te verwerken. Denk bijvoorbeeld aan het omzetten van tekst in ploegrapporten naar trends en afwijkingen door middel van technische sentimentanalyse.
3. **Anomaly detection**: voor het identificeren van afwijkingen, zoals afwijkingen in de frequentie van alarmsignalen of de responstijd op deze alarmen in sensorgegevens.
4. **Time series analyses**: om patronen in data te identificeren die in de loop van de tijd veranderen, bijvoorbeeld om patronen in seizoensgebonden data te identificeren.
5. **Machine Learning** (**ML**): een grote verscheidenheid aan modellen die zijn getraind om patronen in data te identificeren en voorspellingen te doen.
6. **Topic modelling**: een natuurlijke taalverwerkingsmethode om onderwerpen in tekst te identificeren.
7. **Zero-shot classification**: om tekstuele gegevens te classificeren zonder dat aanvullende training nodig is. Het is een vorm van natuurlijke taalverwerking waarbij gebruik wordt gemaakt van grote taalmodellen.

3.3 Resultaat: Hoe is het bij Chemelot gegaan?

De partijen op Chemelot hebben ieder voor zich verschillende databronnen geselecteerd en verwachtingen over inzichten c.q. leerpotentieel die uit deze databronnen verkregen zouden kunnen worden. Per soort databron zijn vervolgens verschillende soorten analysetechnieken geselecteerd.

AnQore
AnQore is met drie databronnen aan de slag gegaan:

1. Meteo data: uit IP21 (data verzamelsysteem van AspenTech) systeem als numerieke waarden in time series. De data is in de vorm van Excel files ter beschikking gesteld.
2. Onderhoudsmeldingen: uit SAP geëxporteerd en in de vorm van Excel files ter beschikking gesteld
3. Overzicht ongewone voorvallen

De volgende analysetechnieken zijn gebruikt:

- Visualisatie van weersomstandigheden versus ongewone voorvallen: het vergelijken van de trends in weergegevens en gegevens van ongewone voorvallen leverde inzicht over de invloed van weersomstandigheden op het vóórkomen van ongewone voorvallen. Met deze techniek is nagegaan of bepaalde weersomstandigheden kunnen leiden tot meer ongewone voorvallen.
- Logistic regression en negative binomial model: om de relatie tussen ongewone voorvallen en weersomstandigheden te onderzoeken.
- Visualisatie van meldingen (in de vorm van een online dashboard gemaakt via de R-Shiny applicatie) om data van verschillende fabriekslocaties en sublocaties te vergelijken, zoals het aantal openstaande onderhoudsmeldingen met verschillende prioriteitsniveaus als leerpotentieel (zwak signaal) voor hoogte van de werkbelasting van het onderhoudsteam. Trends en pieken en anomalieën in de visualisaties kunnen daarbij beschouwd worden als zwakke signalen voor onveilige situaties, zoals een toenemende trend in het aantal open meldingen, plotselinge pieken in het aantal meldingen en meldingen met hoge prioriteit.

Envalior
Om 'begrip voor elkaar' te verbeteren heeft Envalior wachtdienstverslagen als databron geselecteerd. Deze bevatten een schat aan leerpotentieel, maar zijn door hun lengte en type (ongestructureerde gegevens) vaak moeilijk te analyseren. De wachtdienstverslagen zijn in de vorm van tekstdocumenten uit de shiftreport applicatie geëxporteerd. Daarnaast zijn een aantal zaken handmatig bij elkaar gezocht en in de vorm van Word documenten aangeleverd, denk hierbij aan een overzicht van relevante ongewone voorvallen en stopstanden van de fabriek.

Verschillende soorten analyses zijn gedaan op ploegrapporten, waaronder:
- Technische Sentiment Analyse (TSA): hier hebben we een technisch lexicon gecreëerd (gebruikmakend van een lexicon dat eerder ontwikkeld is voor een ander bedrijf op Chemelot en ge-update is met typische Envalior-woorden) en gebruikt om te controleren op afwijkingen (anomalieën) in het sentiment van de ploegrapporten. Een zeer negatief sentiment of een afnemende trend in het sentiment van ploegrapporten kan een signaal zijn voor de ontwikkeling van een niet gewenste situatie.
- Topic modelling: waarmee onderwerpen uit ploegrapporten zijn geïdentificeerd waarover in een bepaalde periode veel is gesproken, zoals in de afgelopen week. Dit kan mogelijk een signaal zijn voor een aankomende niet-gewenste situatie. De plaatjes hieruit bleken echter dusdanig moeilijk interpreteerbaar dat deze als enkelvoudige toepassing niet is doorgezet.
- TF-IDF (term frequentie-inverse document frequentie): om specifieke woorden te identificeren die aan de lexicon voor de TSA moesten worden toegevoegd.
- Term Anomaly Detection: Gebruikers kunnen controleren op abnormale vermelding van bepaalde termen. Ze kunnen een lijst verstrekken en de visualisaties krijgen, evenals een csv-bestand dat afwijkingen (anomalieën) toont. Wanneer termen die geassocieerd zijn met niet-gewenste situaties te vaak worden vermeld, kan dit een signaal zijn voor een niet-gewenste situatie. (Deze mogelijkheid is gemaakt als een online tool ontwikkeld via Python Streamlit).

SABIC
SABIC is aan de slag gegaan met alarm en automation data uit het DCS (Distributed Control System), zoals alarmgegevens en gegevens over instellingen van de fabriek. Deze informatie is in de vorm van time series in Excel overgedragen.
Voor de alarmgegevens is met name gekeken naar de tijd tussen de verschillende statussen in de alarmgegevens, dat wil zeggen de tijd tussen het optreden van een alarm, de bevestiging van het alarm en het terugkeren naar normaal. Tevens zijn de frequentie en tijdsduur van setpoint wijzigingen en modewijzigingen (tussen automatisch en handmatig) gevisualiseerd.

Bij SABIC zijn de volgende analysetechnieken toegepast:
- Visualisatie-technieken
- Statistische (descriptieve) analyse voor frequentie per shift, per uur, per tag
- Anomaliedetectie

CSP
CSP heeft gekozen voor analyse van informatie van een bedrijf op Chemelot, zoals CSP-inspecties, inspecties door Provincie Limburg, achterafrapportages en managementreviews. Deze zijn aangeleverd in tekstformaat in PDF, Word, Powerpoint en Excel. Diverse aangeleverde pdfs bleken onleesbaar te zijn voor de AI-tools. Dit bleek een leerpunt: ingescande documenten moeten of opgeslagen worden in een format dat leesbaar is voor AI-tools of er moet een techniek (zoals OCR) ingezet worden om de tekst (opgeslagen als afbeelding) leesbaar te maken.

De volgende technieken zijn gebruikt om de gegevens te analyseren:
- OCR (optische tekenherkenning) om gescande tekstbestanden om te zetten in machinaal leesbare tekst
- Zero-shot classification: deze werd uitgevoerd met behulp termen in relatie tot 'negatief', 'zorg', 'urgent', 'incident', 'falen', 'risico' en 'gevaar'. Er zijn scores berekend voor elke combinatie van deze termen met verschillende documenten uit verschillende jaren, met als doel trends te visualiseren.

4 Identificeren van zwakke signalen in Big Data

4.1 Voorbereiding: Waar gaat het om?

In deze stap wordt bepaald hoe zwakke signalen in databronnen kunnen worden geïdentificeerd en geduid. Het doel van deze stap is het toepassen van de in de vorige stap geselecteerde technieken: het identificeren van 'zwakke signalen' in Big Data.

Door de aldus verkregen informatie in de context van de werkomgeving te plaatsen, wordt dieper inzicht verkregen en beter begrepen waaróm iets of niets is gebeurd. Het lerende effect gaat daardoor de grenzen van een specifieke gebeurtenis voorbij, want leren wordt ook toegepast op andere gebeurtenissen (= 'beter leren') én dat van de eigen organisatie door het delen van informatie met andere deelnemers in de CoP.

4.2 Uitvoering: Hoe doe je dat?

De stappen voor het identificeren van zwakke signalen in Big Data zijn in essentie niet anders dan die voor het leren van incidenten en worden in industriële omgevingen ook wel onderdelen van 'Weak signal management' genoemd.

1. Pas de in de stap 3 gekozen analyse- en visualisatietechnieken toe.
2. Maak een eerste, globale (brede) beoordeling van resultaten, zoals patronen, staafdiagrammen, boxplots of word clouds en probeer de eerste stap naar mogelijke verbanden en leerpotentieel te maken.
3. Zoek specifieke patronen of trends die wijzen op zwakke signalen, bijvoorbeeld een toename (of de ernst) van ongewone voorvallen.
4. Benoem specifiek geconstateerde afwijkingen en/ of patronen. Beschrijf ook voor elk signaal (voor zover bekend) eventuele opvallende zaken en/ of context. Deze aanvullende informatie kan namelijk belangrijk zijn om zwakke signalen beter/ sneller te kunnen begrijpen en duiden.
5. Verdieping en begrijpen ('sense-making'): probeer afwijkingen en patronen daadwerkelijk te begrijpen. Zet zwakke signalen daarna om naar leerpotentieel: Welk inzicht is verkregen? Doen we de goede dingen?
6. Interpretatie en actie: Hoe nu verder? Bepaal hoe belangrijk de gevonden zwakke signalen en het leerpotentieel zijn. Ga na welke acties of maatregelen genomen kunnen worden en hoe effectiviteit die (kunnen) zijn.

4.3 Resultaat: Hoe is het bij Chemelot gegaan?

Het proces om informatie uit plantdata met behulp van AI te halen bestaat uit meerdere stappen. Terugkijkend naar de ervaringen van de bedrijven op Chemelot is duidelijk geworden dat het begint met visualisatie, dat stappen overslaan niet werkt en dat klein houden de sleutel tot succes is.

Het denkproces kan zowel vanuit een databron als vanuit een mogelijk zwak signaal 'feature' beginnen. Welke bron zou zinvolle informatie kunnen bevatten, dan wel aan wat voor soort features denk je? Probeer te denken in termen van databron, 'feature' en het (veiligheids)risico dat daarmee te maken heeft.

AnQore
Bij AnQore zijn eerdere experimenten met data en AI uitgevoerd. Een aantal mensen in de organisatie heeft de werkwijze inmiddels in de vingers. Vanuit de Supervisor Maintenance kwam de vraag om aan de slag te gaan met 'te hoge temperaturen' als risicobron. Na discussie is besloten om een soort van weersentiment op te zetten, samengesteld uit diverse weerscondities. In tabel 4.1 zijn weerscondities en de daarbij horende denklijn naar risico uitgewerkt vanuit het perspectief van onderhoud en productie:

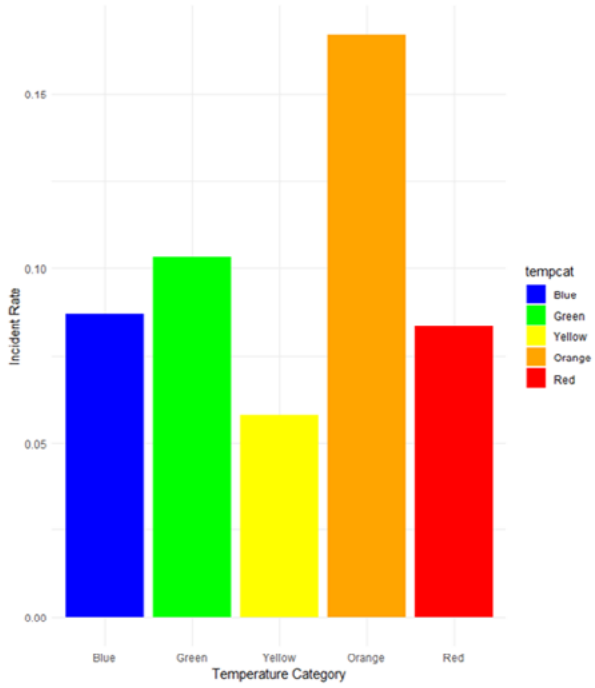
Tabel: Risico per weerelement	
Weersconditie	**Risico**
Hitte	Hittestress, overmatig zweten, zweetdruppels in ogen waardoor verminderd zicht, ...
Koude	Onderkoeling/bevriezing, stijve spieren
Windkracht	Flapperende kleding, leidt af van het werk, risico hijsen en takelen en werken op hoogte
Windrichting	Niet van toepassing?
Windstoten	Risico hijsen en takelen en werken op hoogte
Onweersbuien	Dreiging van onweer kan leiden tot haast, electrocutie door bliksem
Regen	Hevige regen geeft slecht zicht op werkzaamheden en haastwerk vanwege onaangename omstandigheden, of op het vermijden van (noodzakelijke) werkzaamheden buiten, of ongewenste onderbreking van werkzaamheden
Hagel/sneeuw	Hagel/sneeuw geeft slecht zicht op werkzaamheden en haastwerk vanwege onaangename omstandigheden, of op het vermijden van (noodzakelijke) werkzaamheden buiten, of ongewenste onderbreking van werkzaamheden
Gladheid	Uitglijden op bevroren water (is vaker als incident voorgekomen bij AnQore)
Bevriezing installatie	Metalen delen bevroren, (spoel)water bevriest, aflsuiters/kleppen, ijspegel-vorming
Mist (beperkt zicht)	Beperkt zicht kan leiden tot het niet opmerken van lekkages e.d.

Tabel 4.1 Mogelijke onderdelen in een weersentiment

In 'BLIC vooruit' is ingezoomd op een aantal van deze weerscondities, zoals temperatuur en relatieve vochtigheid. Uit analyse van temperatuurgegevens blijkt dat temperatuur van invloed kan zijn op het optreden van ongewone voorvallen. In figuur 4.1 vertegenwoordigt elke kleur een temperatuurcategorie:

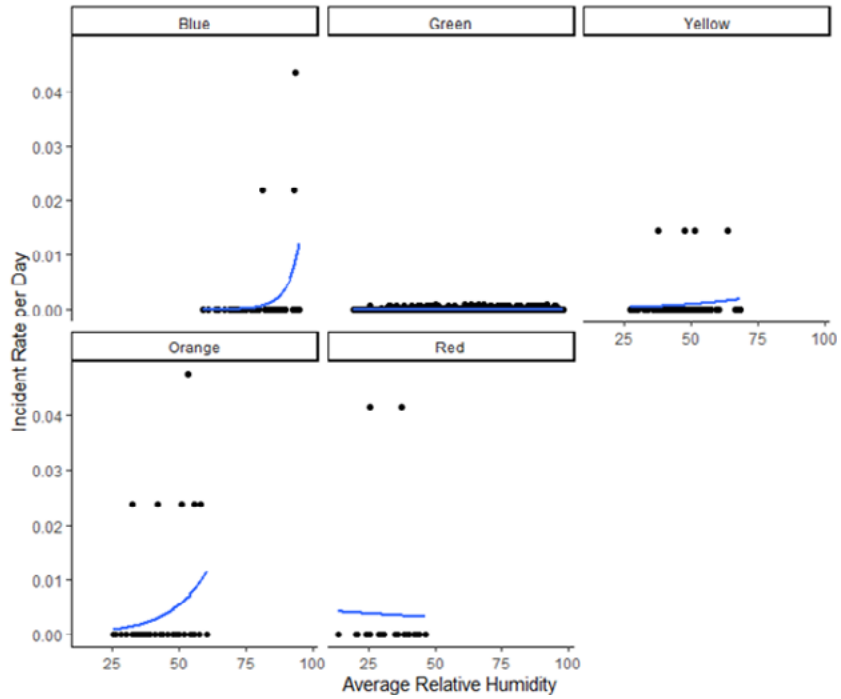
- Blauw: Temperatuur <= 0
- Groen: Temperatuur > 0 & Temperatuur <= 25.599
- Geel: Temperatuur >= 25.6 & Temperatuur <= 27.699
- Oranje: Temperatuur >= 27.7 & Temperatuur <= 31.099
- Rood: Temperatuur >= 31.1

Het aantal punten (ieder punt is een werkploeg) voor de temperatuurcategorieën blauw, groen, geel, oranje en rood bedraagt respectievelijk 46, 3107, 69, 42 en 24. De figuur toont het percentage ongewone voorvallen per temperatuurcategorie (aantal ongewone voorvallen gedeeld door het aantal datapunten binnen elke bijbehorende temperatuurcategorie).
Zoals blijkt uit de figuur, hangt het hoogste percentage ongewone voorvallen samen met de temperatuurcategorie oranje (tussen 27,7 en 31.1 graden Celsius). De temperatuurcategorie rood heeft een lager percentage ongewone voorvallen. In deze temperatuurcategorie is bij AnQore het 'Hitteprotocol Maintenance voor werken bij warme weers- of werkomstandigheden' van kracht.



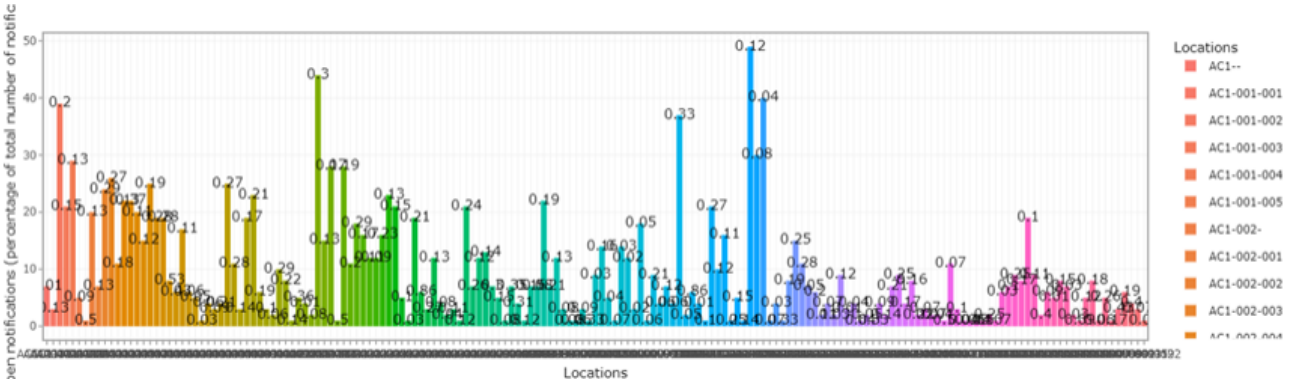
Figuur 4.1 Temperatuurcategorieën versus ongewone voorvallen

Daarnaast is voor de verschillende temperatuurcategorieën het aandeel ongewone voorvallen in relatie tot de relatieve vochtigheid gevisualiseerd. Zie figuur 4.2. Het betreft indicatieve resultaten, er is nog geen statistische validatie aangezien het weinig incidenten betreft. In deze indicatieve resultaten is het mogelijk zwakke signaal zichtbaar dat bij een hogere relatieve vochtigheid in combinatie met temperatuurcategorie blauw (< 0°C) het aantal ongewone voorvallen toeneemt. Een verklaring hiervoor kan gezocht worden in moeilijkere werkomstandigheden door ijsafzetting en aanvriezen van vocht uit de lucht.



Figuur 4.2 Aandeel ongewone voorvallen in relatie tot
de relatieve vochtigheid voor de verschillende temperatuurcategorieën

Bij de databron onderhoudsmeldingen is gestart met het visualiseren van meldingen in de tijd. De analyse van onderhoudsmeldingen laat een grote variabiliteit zien tussen verschillende jaren, verschillende fabrieken en binnen fabrieken (zie Figuur 4.3).



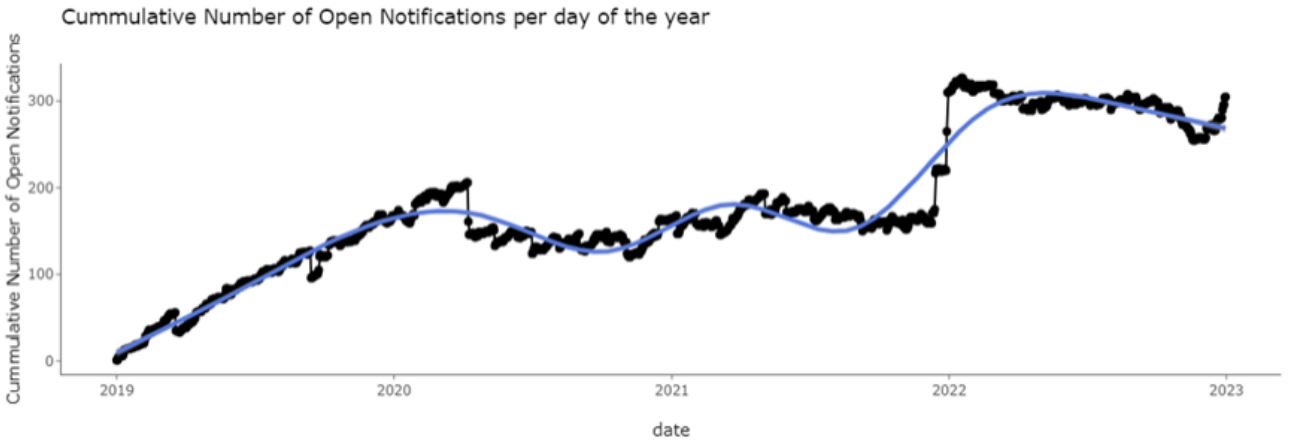
Figuur 4.3 Onderhoudsmeldingen in verschillende locaties binnen 1 fabriek over 1 jaar

Figuur 4.3 geeft het aantal 'open onderhoudsmeldingen' weer voor verschillende locaties binnen één fabriek, in één jaar. De kleuren corresponderen met secties in de fabriek. Het getal bovenaan de balk geeft aan hoeveel 'open onderhoudsmeldingen' er zijn ten opzichte van het totaal aantal onderhoudsmeldingen voor die locatie. Uit een dergelijke figuur kan ook worden afgeleid waar (op welke plaatsen) in de fabriek de meeste meldingen zijn. Om dat gegeven nader te kunnen duiden of verklaren is een aanvullende analyse of nader onderzoek nodig.

Bij de discussie over het risico dat 'open onderhoudsmeldingen' met zich meebrengen kwam het perspectief van onderhoud en van productie op tafel. Veel 'open onderhoudsmeldingen' in een fabriek betekent dat productie in een fabriek aan het werk is met mogelijk zwakke plekken. Voor onderhoud betekenen veel 'open onderhoudsmeldingen' een mogelijk hoge werkdruk. Het perspectief van productie is meer vanuit procesveiligheid, vanuit onderhoud meer vanuit arbeidsveiligheid.

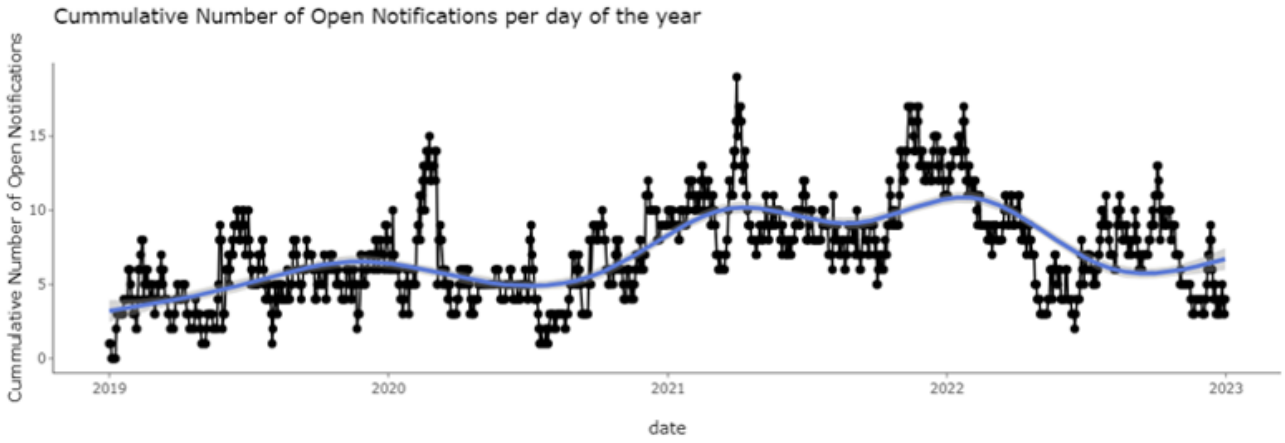
Daarnaast is gekeken naar het aantal openstaande onderhoudsmeldingen. Figuur 4.4 illustreert dat het aantal openstaande onderhoudsmeldingen tot begin 2020 een stijgende trend vertoonde. Hierna gingen de gegevens een periode van stabiliteit in, met tussen de 150 en 170 openstaande onderhoudsmeldingen tot begin 2022. Begin 2022 deed zich een aanzienlijke stijging voor, het verhogen van het aantal open onderhoudsmeldingen, dat vervolgens op ongeveer 300 bleef steken.

Nadere analyse is nodig om te onderzoeken of hier sprake is van een mogelijk zwak signaal. Gedacht kan worden aan een zwak signaal met relatie tot een fabriek op leeftijd, toenemende werkdruk voor onderhoud toeneemt of meer zwakke plekken in de plant. Het kan ook zijn dat er geen zwak signaal is en dat de oorzaak voor het patroon administratief van aard is (bijvoorbeeld als geplande werkzaamheden ver van tevoren in het systeem ingebracht zijn).



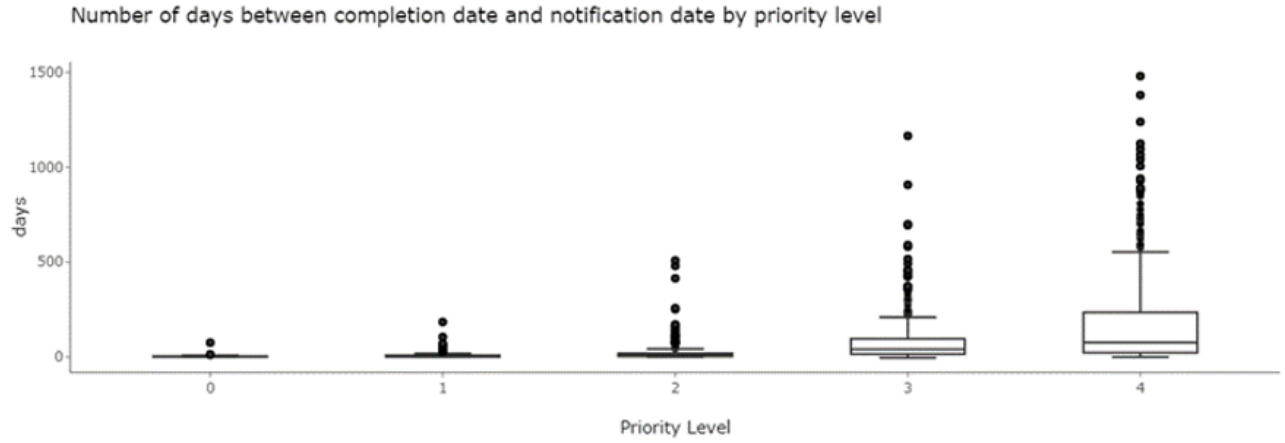
Figuur 4.4 Cumulatieve aantal 'open onderhoudsmeldingen' over een periode van 4 jaar tussen januari 2019 en december 2022

Zoals blijkt uit figuur 4.5 vertoont het aantal openstaande onderhoudsmeldingen met hoge prioriteit (prioriteitsniveaus 0, 1 en 2) een variatie in de tijd. Vanuit het aantal openstaande onderhoudsmeldingen gezien leken de jaren 2021 en 2022 een verhoogde druk te geven op het onderhoudsteam.



Figuur 4.5 Cumulatieve aantal 'open onderhoudsmeldingen' met prioriteit niveau 0, 1 en 2, over een periode van 4 jaar tussen januari 2019 en december 2022

Figuur 4.6 toont de tijdsduur tussen de registratie- en voltooiingsdatum van onderhoudsmeldingen. Hieruit blijkt dat meldingen met lagere prioriteiten, zoals niveau 3, 4 en 5, vaak gedurende langere perioden open blijven staan, soms meerdere jaren. Omgekeerd hebben meldingen met hogere prioriteiten, niveaus 0 en 1, doorgaans kortere voltooiingstijden. Er zijn echter gevallen waarin zelfs deze meldingen met hoge prioriteit gedurende langere perioden onopgelost bleven, waarbij de langste duur 75 dagen was voor niveau 0 en 184 dagen voor niveau 1. Dit kan een administratieve oorzaak hebben, bijvoorbeeld geen tijd om af te sluiten of vergeten af te sluiten. Het kan ook een technische oorzaak hebben, bijvoorbeeld beschikbaarheid reserveonderdelen. Meer onderzoek en relateren aan ongewone voorvallen is nodig om te beoordelen of hier een zinvol zwak signaal uit te halen is, denk aan 'tijd tot reparatie'.

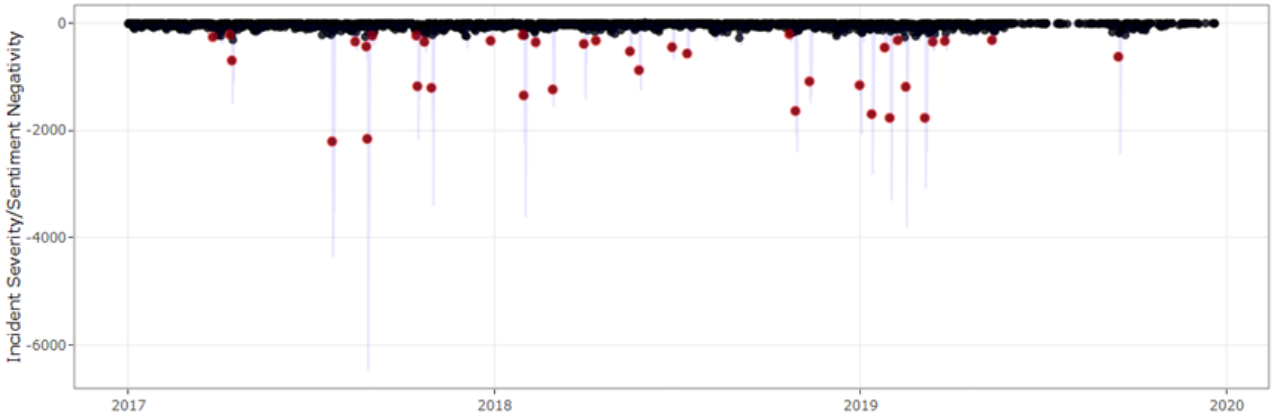


Figuur 4.6 Tijdsduur tussen inleggen en klaarmelden van onderhoudsnotificaties

Bij de databron onderhoudsmeldingen zijn in de discussie vele mogelijke zwakke signalen/ features de revue gepasseerd. Een aantal voorbeelden: 'open onderhoudsmeldingen' irt werkdruk, verdeling in prioriteit van onderhoudsmeldingen, # 'open onderhoudsmeldingen' per fabrieksonderdeel, tijd tot reparatie, # partijen dat aan een klus gaat werken en nog veel meer.

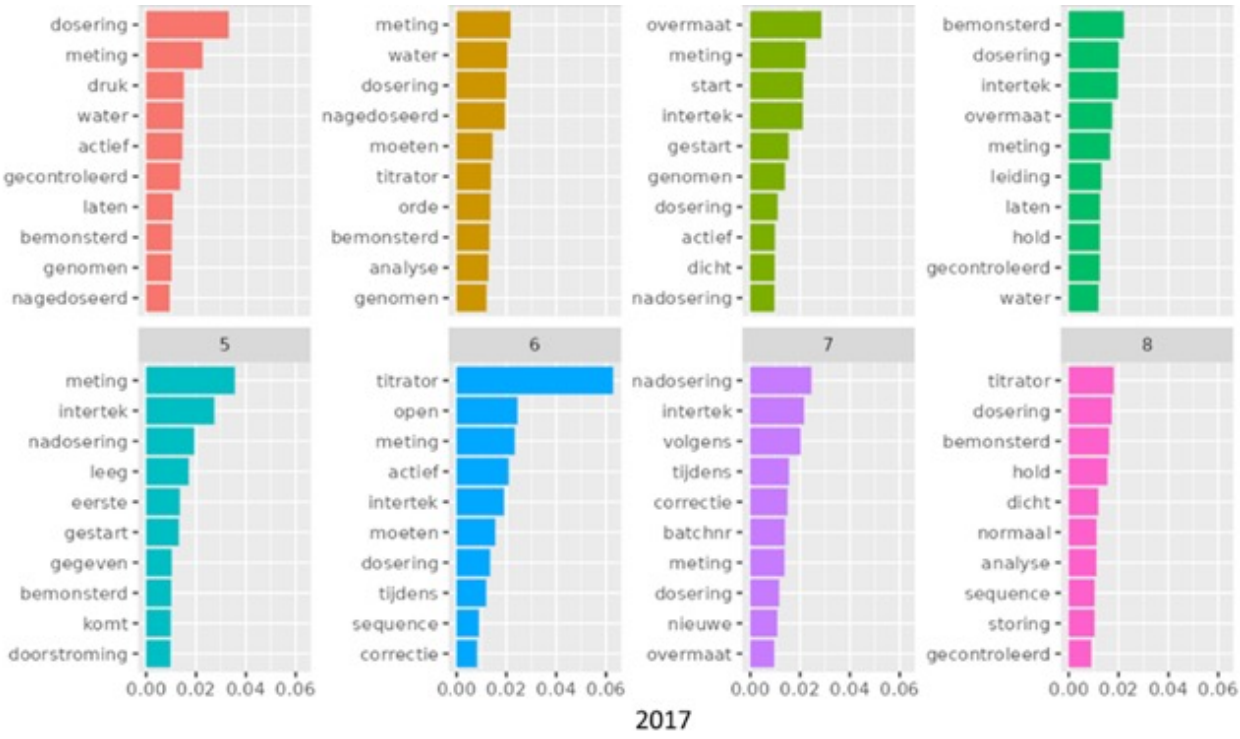
Envalior
Envalior is op zoek naar features die 'begrip voor elkaar' onderbouwen. Een eerder ontwikkelde feature (Technische Sentiment Analyse) bleek ook voor Envalior van toegevoegde waarde, waarmee aangetoond is dat een feature voor één bedrijf ontwikkeld ook bij een ander bedrijf kan werken. De binnen kenniscentrum Brightsite ontwikkelde 'Safety Stethoscope' is door Envalior toegepast als advanced analytics tool voor tekstbestanden.

In figuur 4.7 is het negatieve sentiment gevisualiseerd voor Envalior in de periode januari 2017 tot december 2019. Significante afwijkingen zijn weergegeven door rode punten. De verticale lijnen visualiseren het geaggregeerde sentiment van de voorgaande twee dagen.

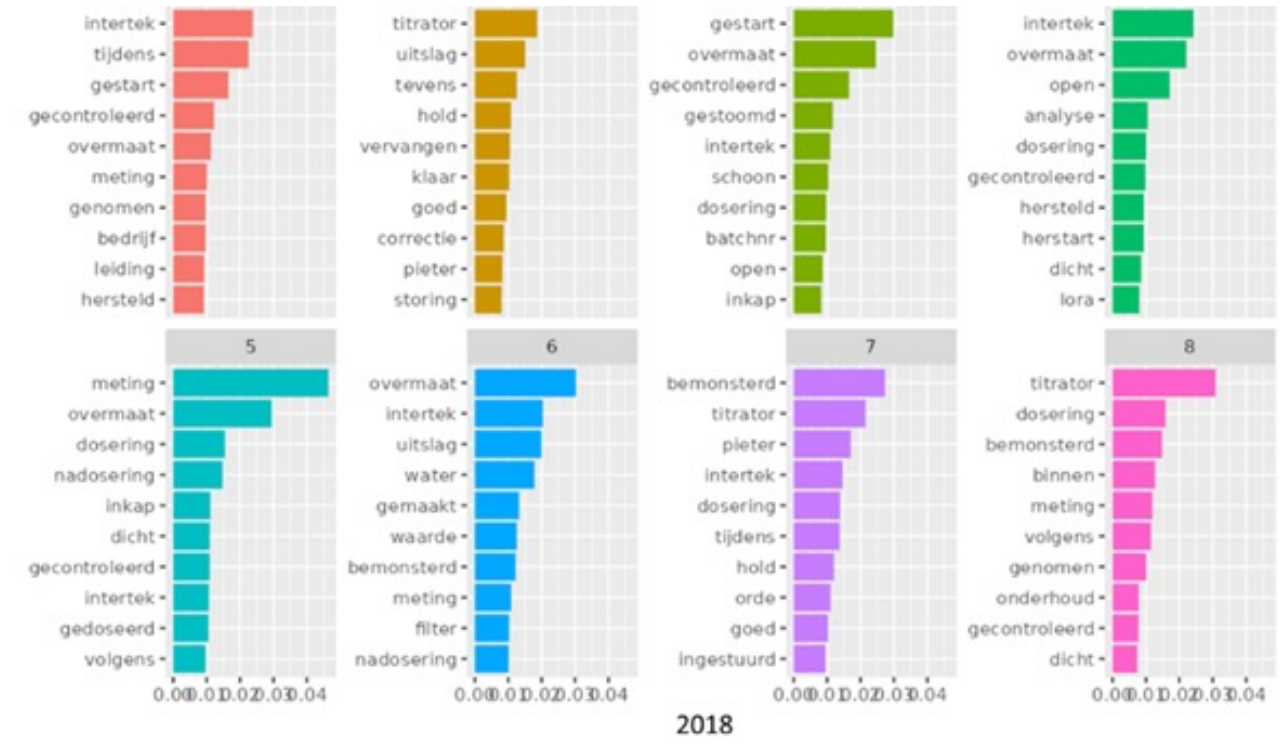


Figuur 4.7 Technisch Sentiment

Bij Envalior is ook 'topic modelling' toegepast op wachtdienstverslagen voor verschillende fabrieken en tijdperiodes. In de figuren 4.8 en 4.9 wordt de top 8 voor 2017 en 2018 weergegeven voor één fabrieksonderdeel.

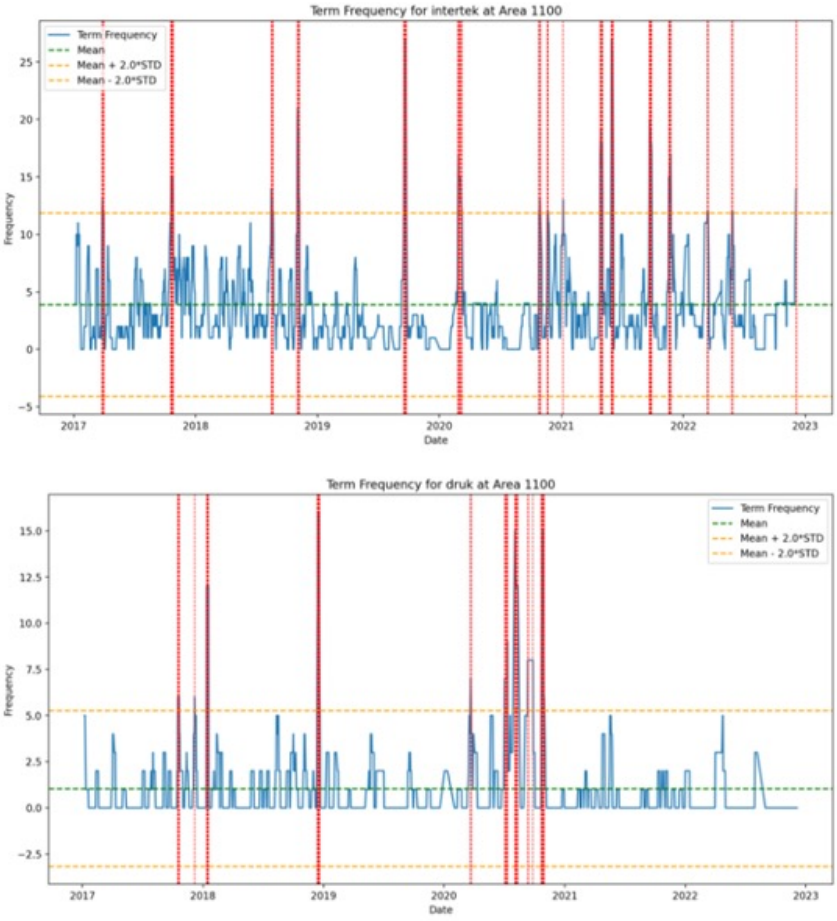


Figuur 4.8 Topic modelling: top 8 van één fabrieksonderdeel in 2017



Figuur 4.9 Topic modelling: top 8 van één fabrieksonderdeel in 2018

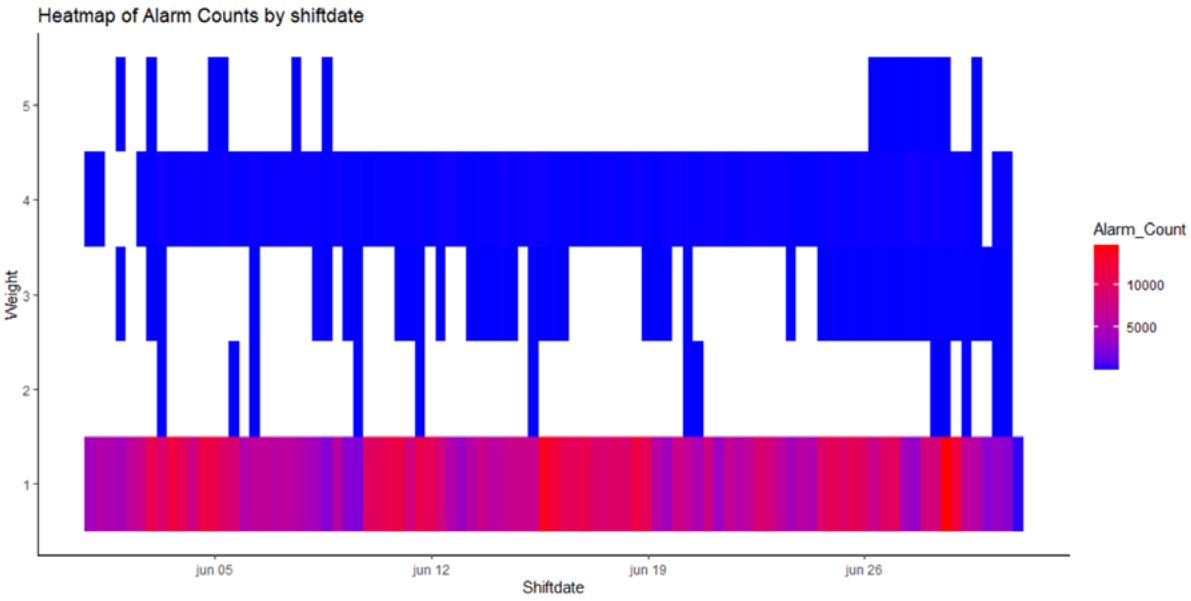
De interpretatie van de resultaten voor 'topic modelling' bleek te complex, waarna de overstap gemaakt is naar de term 'frequency benadering'. Figuur 4.10 is een voorbeeld hoe afwijkingen kunnen worden gevisualiseerd op basis van frequentie. Afwijkingen kunnen worden weergegeven voor elk gegeven woord en resultaten kunnen worden samengevat in tabellen.



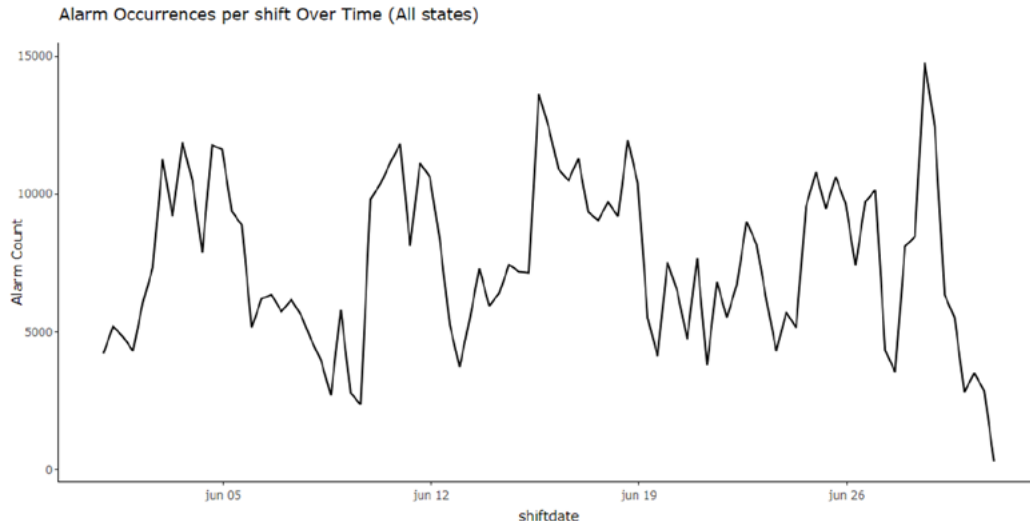
Figuur 4.10 Term frequency afwijkingen

SABIC
SABIC is aan de slag gegaan met DCS data. De beoogde scope was erg groot en is teruggebracht naar data die druk op de operator kunnen geven. Meer specifiek: alarmen, mode changes en grade changes. De eerste stap – de visualisaties (zie de figuren 4.11 en 4.12) – heeft veel discussie en daarmee meer inzicht gegeven voor de medewerkers van SABIC in hun eigen data, systemen en werkwijze. De keuze is gemaakt/ het is beter om deze discussies intern af te ronden en daarna gericht op zoek te gaan naar features.

De DCS data is nu in de systemen namelijk op een dusdanige manier gebouwd, verwerkt en gevisualiseerd voor de meetkamer en operators dat zij er voor het daadwerkelijke bedrijven van de fabriek mee kunnen werken. Het over een langere termijn beschouwen van trends/ druk in de aangeboden data, vergt een geheel andere presentatie en was complexer dan vooraf gedacht. De signalen die wij zoeken zijn namelijk zwakke signalen en die zijn meestal niet eenvoudig te vinden. De denklijn vooraf moet helder zijn.



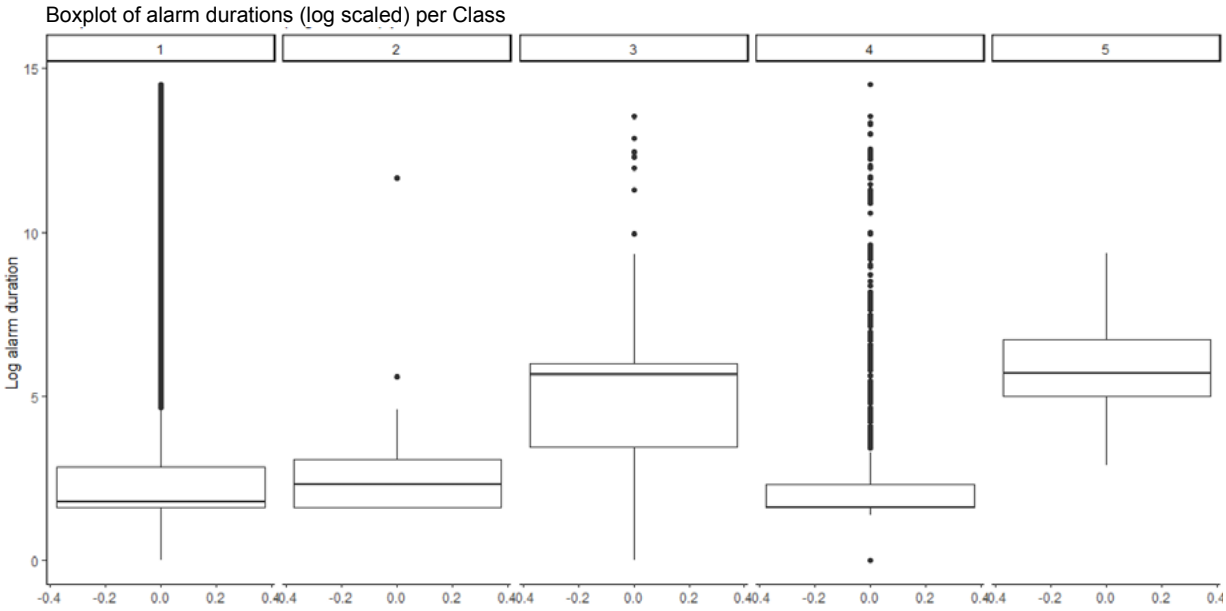
Figuur 4.11 Heatmap van het aantal alarmen binnen een wachtdienst in een periode van een maand



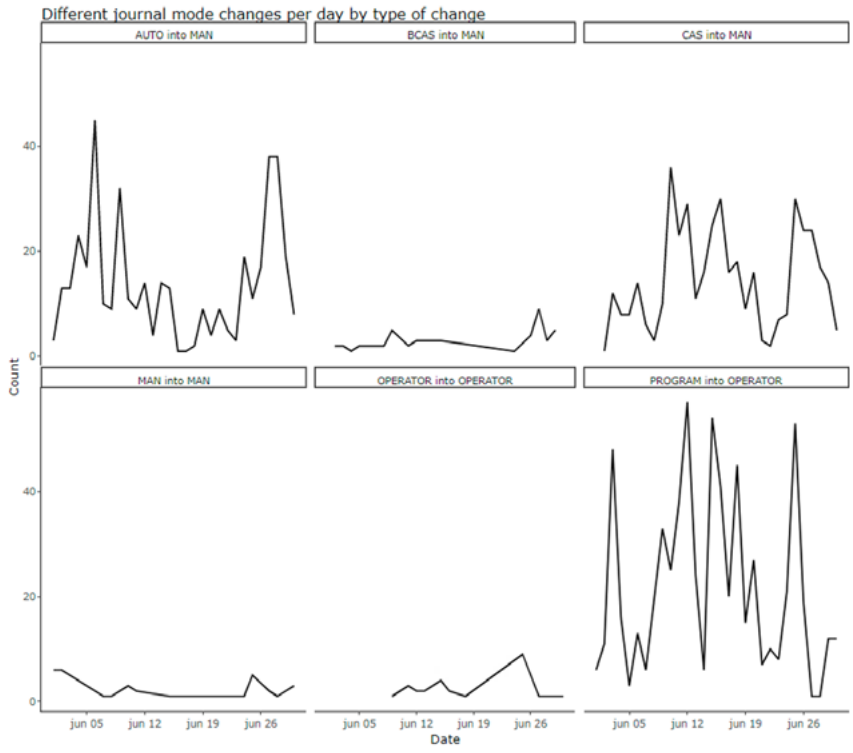
Figuur 4.12 Visualisatie van het aantal alarmen per wachtdienst in een periode van een maand

Bovenstaande twee figuren gaan over ‘alarm’, wat in deze context omvat alle systeemmeldingen en dus veel meer is dan bijvoorbeeld een ‘operator alarm’. Een groot aantal ‘alarmen’ vindt plaats op de achtergrond en is daardoor niet zichtbaar voor een operator en niet direct bekend bij de verschillende disciplines/ afdelingen, het zijn zaken die je alleen bij bouw en ontwerp van een systeem beschouwd. Daarom bleek ook in beide grafieken dat het aantal meldingen en trends in de tijd een compleet

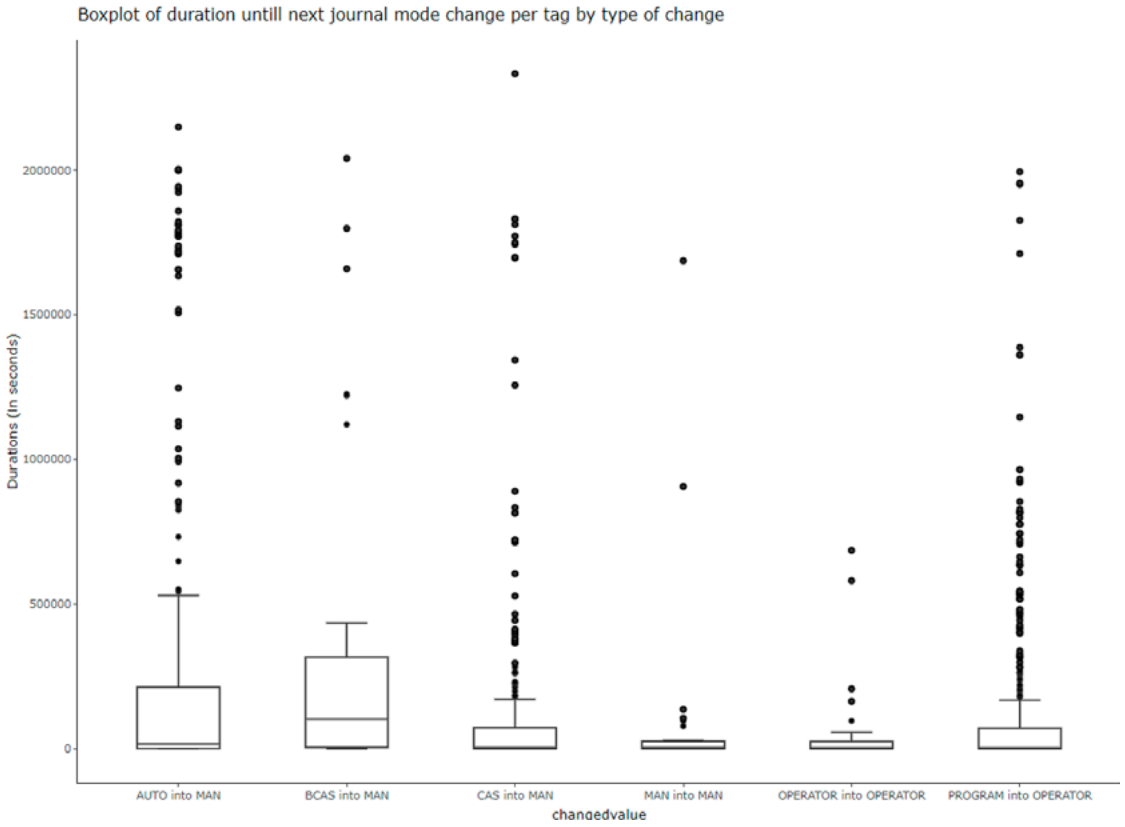
vertekend beeld gaf en dat er veel meer inhoudelijke slagen gemaakt moesten worden om de dataset een bepaalde weegfactor mee te gaan geven, wat complexer was dan gedacht.
Een aantal verwachte trends waren zichtbaar, zoals een stijging tijdens stopstanden en bepaalde ingrijpende handelingen in de fabriek, maar bij 'rustige' periodes waren ook intensieve/ hoge aantallen van systeemmeldingen/ handelingen te zien, welke stuk voor stuk beoordeeld moesten worden.
Hetzelfde werd zichtbaar in onderstaande figuren, 4.13 tot en met 4.16, over de tijdsduur van bepaalde systeemmeldingen, mode-instellingen, enz., en ook daar geldt dat veel meer benodigde tijd voor correcte interpretatie nodig is om tot een eindresultaat te kunnen komen.
Wel zichtbaar is dat er schijnbaar geen directe relatie is tussen de ploegendiensten zelf (ochtend-, middag- en nachtdienst) en de 'drukte' in de systemen. Uiteraard kan dat inzicht wijzigen zodra het bovenstaande (het correct interpreteren en meegeven van weegfactoren) is uitgevoerd.



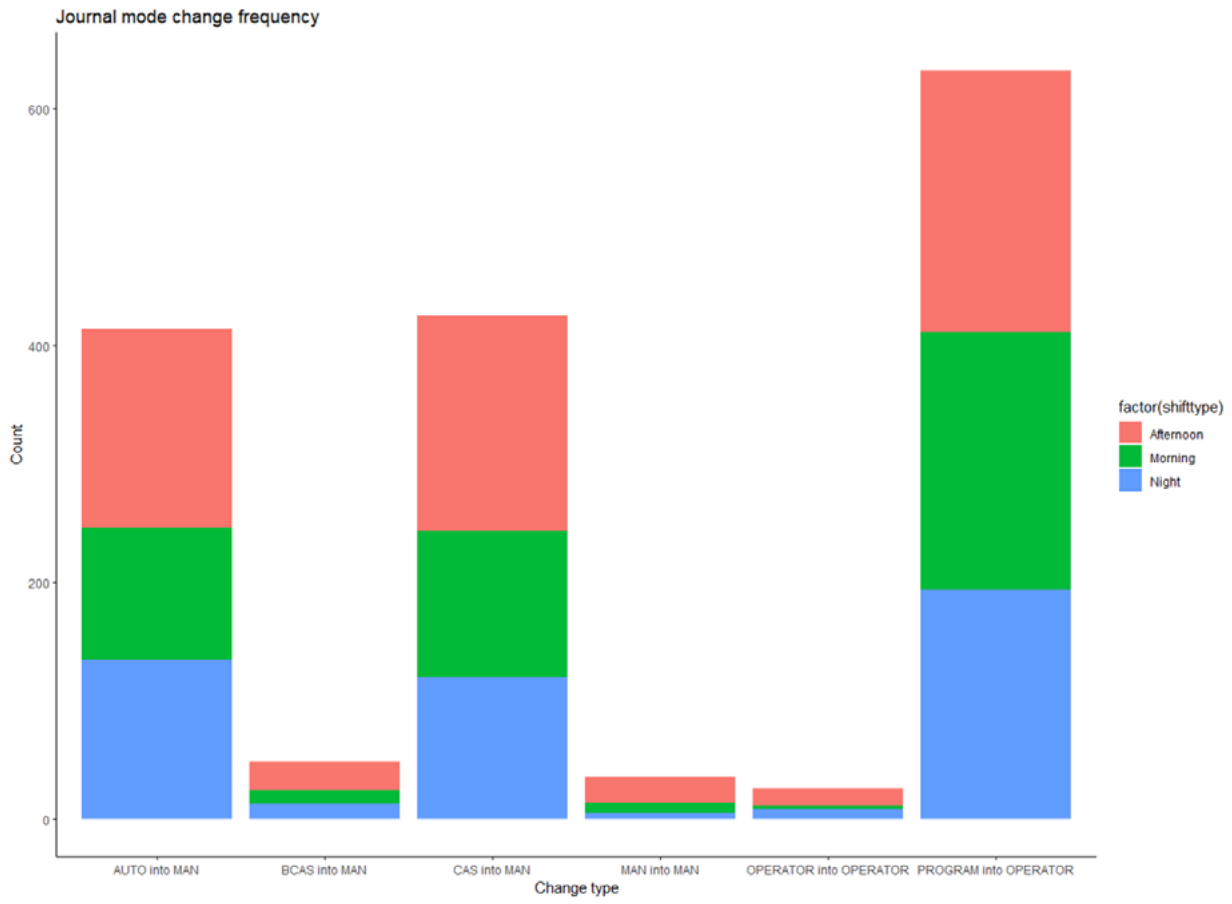
Figuur 4.13 Visualisatie door middel van een boxplot met alarm/ system setting tijdsduren (Log schaal)



Figuur 4.14 Visualisatie aantal mode-wijzigingen per dag



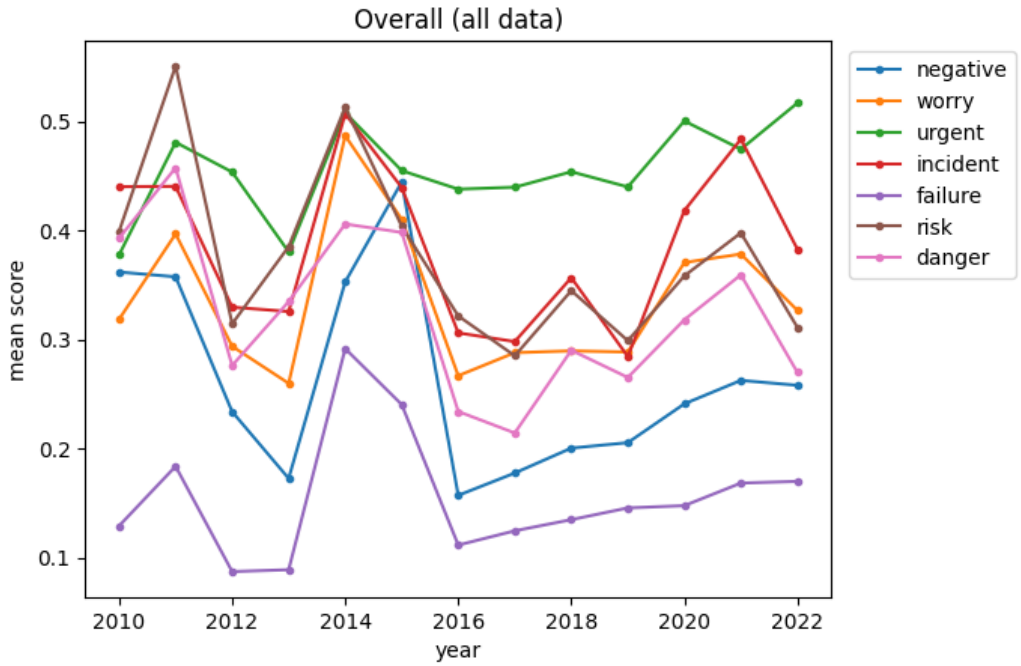
Figuur 4.15 Visualisatie door middel van een boxplot van de tijdsduur tot een mode-wijziging



Figuur 4.16 Visualisatie door middel van een staafdiagram voor mode-wijzigingen

CSP

CSP vraagt zich af of er zwakke signalen vooraf zijn gegaan aan een tweetal incidenten in 2015 voor één van de bedrijven op de chemiesite. Nadere bestudering van de twee incidenten maakte duidelijk dat het incidenten zijn met een verschillend karakter. Het ene incident is een soort van 'zwarte zwaan' voor Chemelot (een gebeurtenis die niemand van tevoren heeft zien aankomen of voorspeld), het tweede is toe te schrijven aan de eigen organisatie van het betreffende bedrijf. De data in scope van 'BLIC vooruit' past vooral bij het tweede incident. De analyse van de documenten uit het CSP-archief met behulp van zero shot-classification in de tijd gaf het volgende resultaat (figuur 4.17):



Figuur 4.17 Trend in documentatie in CSP-archief voor een aantal begrippen

Naast een duidelijke piek voor 2016 ziet het betreffende bedrijf nog 2 pieken (2018 en 2021), kort daarna hebben eveneens incidenten plaatsgevonden. In deze overall analyse zijn de tekstdocumenten van diverse soorten audits, inspecties en reviews meegenomen. Nadere analyse is nodig, vooralsnog lijkt hier sprake van een mogelijk nieuwe feature.
De analyse is uitgevoerd aan de hand van documenten uit het CSP-archief. Het betrof voornamelijk ingescande documenten, de wijze van inscannen (leesbaar opslaan, niet als plaatje) bleek een factor bij de analyse met digitale technieken. Leesbaar opslaan vergemakkelijkt het proces. Wel is hiermee aangetoond dat ook niet digitale informatie een databron kan zijn.

5 Vaststellen van leerpotentieel

5.1 Voorbereiding: Waar gaat het om?

In de voorgaande stappen heeft elke deelnemer voor zichzelf databronnen geïnventariseerd, geanalyseerd en patronen/ zwakke punten (inclusief context) samengevat (1e orde leren). Dit hoofdstuk gaat over het interpreteren van de eigen (gedetailleerde) resultaten en het omzetten daarvan naar specifiek leerpotentieel (2e orde leren). In deze stap wordt het leerpotentieel van elk bedrijf verzameld en gedeeld met alle deelnemers in de CoP.

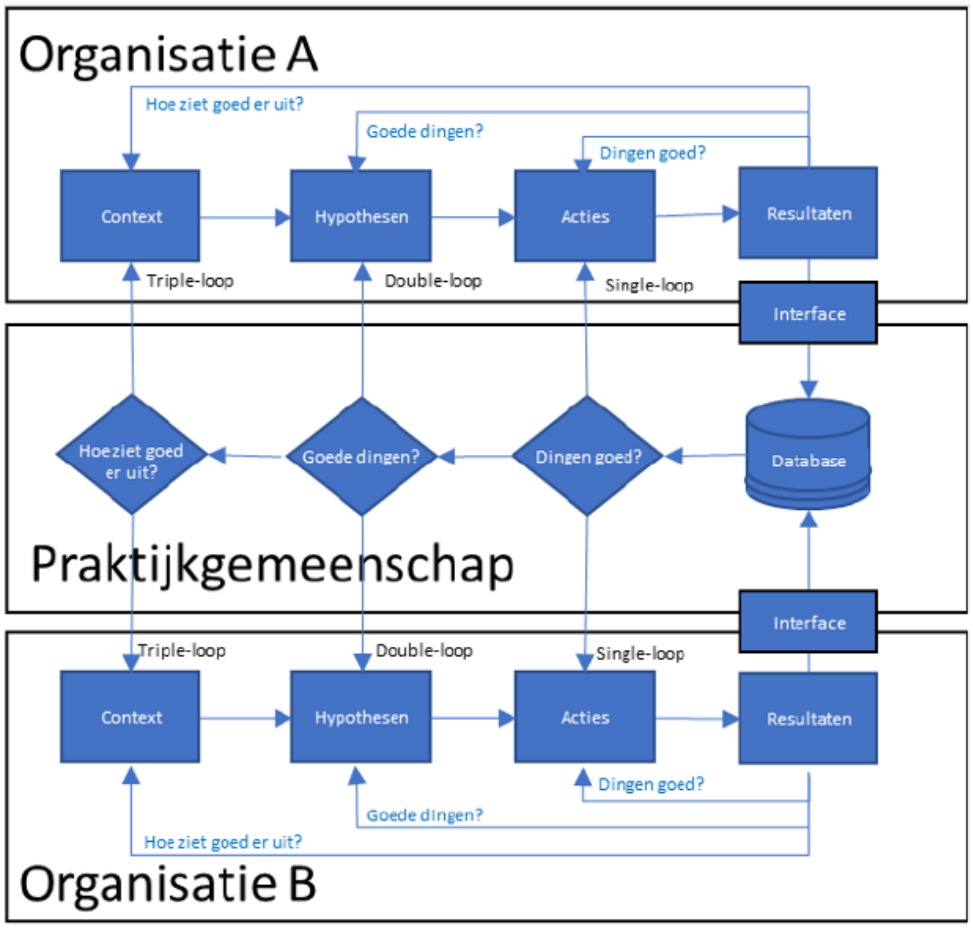
Uit dat overzicht kan gezamenlijk bepaald worden wat het individuele én gemeenschappelijke leerpotentieel is, of/ wat onderlinge relaties zijn, de eventuele samenhang en hoe (gemeenschappelijk) leerpotentieel toegepast kan worden in de praktijkgemeenschap. Het doel van dat laatste is ook om inzicht te krijgen in de context, condities of de omgeving waarin gebeurtenissen hebben plaatsgevonden in een bepaald systeem (3e orde leren). Zie voor toelichting het blok hieronder.

1e orde leren (Doen we de dingen goed?):
Het eerste en meest eenvoudige niveau is het identificeren van leerpotentieel op basis van gemaakte fouten, zoals bijvoorbeeld een probleem, storing of ongewoon voorval. De aanleiding om een incidentonderzoek uit te voeren is vaak een 'sterk signaal', zoals een ernstig incident. Incidentonderzoek is vaak beperkt tot 'hindsight bias' en tot 'single-loop-leren' in plaats van het waardevollere 'double-loop-leren'. Single-loop-leren is het resultaat van de analyse van het incident, waarbij vaak alleen de specifieke situatie of het falen wordt aangepakt en gecorrigeerd binnen het organisatiesysteem zoals het in zijn huidige vorm bestaat. Over het algemeen is dit leerpotentieel relatief snel en eenvoudig te vinden zonder tussenkomst van complexe leersystemen: mensen lossen het probleem op en (eenvoudige, 'quick fix') maatregelen zijn vaak al genomen.

2e orde leren (Doen we de goede dingen?):
Het tweede niveau is identificatie van leerpotentieel op basis van systemische oorzaken in processen, systemen of op basis van achterliggende oorzaken, 'root causes' or 'causal learnings'. Het is strikt genomen niet noodzakelijk om in een (bestaand) veiligheidsmanagementsysteem te doen, want ook in overleggen kunnen discussies plaatsvinden die de vraag beantwoorden en op basis waarvan besluiten worden genomen.

3e orde leren (Hoe ziet goed eruit?):
Het derde niveau is identificeren van leerpotentieel op basis van structurele, fundamentele oorzaken in (primaire) businessprocessen of systemen. Op dit niveau gaat het om fundamentele aannames en over 'waarom' dingen gaan zoals ze gaan en hoe die hebben bijgedragen aan het ontstaan van een gebeurtenis, waardoor beter leren plaatsvindt. Dit niveau vraagt veel van een organisatie, want er moet ruimte en tijd zijn om na te denken over de vraag 'Hoe beslissen we dat dingen goed zijn?' Denk bijvoorbeeld aan het anders inrichten van een proces, voor het fabriceren van andere producten, inzet van andere (nieuwe) soorten technologie of het invoeren van een digitale leeromgeving voor ontwikkeling van predictive-based safety. Besluitvorming kan losstaand zijn, maar vaak volgt het uit managementsystemen die laten zien dat bepaalde processen keer op keer aangepast worden.

Een blauwdruk voor het leerproces in een praktijkgemeenschap (CoP) is weergegeven in figuur 5.1. Dit is een opzet voor een praktijkgemeenschap die deelnemers ondersteunt om gezamenlijk te leren van data waar mogelijk zwakke signalen in zijn verborgen. Naar gelang van de wensen van de deelnemende partijen kan de praktijkgemeenschap op verschillende manieren ingevuld worden.



Figuur 5.1 Blauwdruk voor het leerproces in de praktijkgemeenschap (CoP)

Toelichting op de blauwdruk:

- Centraal staat de praktijkgemeenschap, die informatie van deelnemers (in de figuur: organisatie A en organisatie B) verzameld en opslaat in een (centrale) database (kennisbank). Vanuit de kennisbank worden deelnemers ondersteund bij respectievelijk de single-loop-leren (1e orde leren: “Doen we de dingen goed?”) zoals voor verbeteracties of anders doen, de double-loop-leren (2e orde leren: “Doen we de goede dingen?”) zoals anders denken, vernieuwen of werken met hypotheses, en de triple-loop-leren (3e orde leren: ”Hoe ziet goed er uit?”) waarin de context belangrijk is en verwijst naar de omgeving waarin het leerproces plaatsvindt, inclusief de fysieke, sociale en culturele omgeving.
- De praktijkgemeenschap wordt geflankeerd door deelnemende organisaties, die zowel individueel leren als leren door samenwerking in de praktijkgemeenschap.

5.2 Uitvoering: Hoe doe je dat?

De stappen voor het vaststellen en toepassen van leerpotentieel op basis van de ‘Plan-Do-Check-Act’ (PDCA) benadering zijn als volgt:

1. Benoem geconstateerde afwijkingen en/ of patronen: beschrijf aanvullend (voor elk signaal, voor zover bekend) eventuele opvallende zaken en/ of de context waarin een gebeurtenis heeft plaatsgevonden. Deze aanvullende informatie kan namelijk belangrijk zijn om zwakke signalen te kunnen begrijpen en te duiden.

2. Begrijpen (‘sense-making’): probeer afwijkingen en patronen echt te begrijpen door analyse van de zwakke signalen. Gebruik de resultaten van de analyse om de belangrijkste inzichten, lessen of leerpotentieel te formuleren. Reflecteer op betekenis, relevantie, validiteit en betrouwbaarheid van de gevonden patronen, relaties of zwakke signalen. Vergelijk bevindingen met doelstellingen, verwachtingen, aannames of normen.

3. Interpretatie: ga na hoe belangrijk de zwakke signalen zijn en wat de leerpotentieel kunnen betekenen. Gebruik dit – samen met de conclusies uit de vorige stap - om concrete, haalbare en meetbare acties te formuleren. Gebruik de ‘SMART’-methode om acties te formuleren: Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden.

4. Overleg met collega’s, experts en/ of deelnemers van de CoP bij het vaststellen van leerpotentieel en acties. Vraag om hun mening, feedback, suggesties of ondersteuning. Zorg voor draagvlak en zorg ervoor dat iedereen het eens is met leerpotentieel en acties, en dat iedereen zich verantwoordelijk en gemotiveerd voelt om deze uit te voeren.

5. Implementeer leerpotentieel en acties: voer de acties uit die uit de leerpotentieel voortvloeien en monitor voortgang, resultaten en effecten. Gebruik een actieplan, logboek, agenda of ander hulpmiddel om acties te plannen, uit te voeren en te documenteren.

6. Monitor voortgang en controleer of de maatregelen effectief zijn geweest, ook na verloop van tijd. Gebruik feedback, evaluaties of audits om te controleren of de acties leiden tot de gewenste verandering of verbetering. Verzamel en analyseer daartoe data over het leerproces, zoals leerprestaties, ervaringen en behoeften, voor, tijdens en na het uitvoeren van de acties.

7. Sluit de leerkring: maak ‘weak signal management’ een vast onderdeel van het veiligheidsmanagementsysteem. Reflecteer op leerproces en leerpotentieel, en deel ervaringen, inzichten en aanbevelingen met anderen. Integreer leerpotentieel en acties in de dagelijkse praktijk, routines, procedures of systemen. Zorg ervoor dat het leerproces regelmatig wordt geëvalueerd en bijgesteld op basis van nieuwe data, feedback of veranderingen.

5.3 Resultaat: Hoe is het bij Chemelot gegaan?

De in 5.2 beschreven werkwijze voor het vaststellen en toepassen van leerpotentieel op basis van de PDCA-benadering is herkenbaar voor het verloop op Chemelot. In de praktijk zijn vooral de eerste vier stappen door de individuele deelnemers en in het CoP doorlopen: ‘benoemen, begrijpen, interpreteren en overleggen’.

In 4.3 is beschreven welke zwakke signalen deelnemende partijen op Chemelot op het spoor zijn gekomen. Het benoemen van zwakke signalen vond plaats aan de hand van visualisatie van patronen. In de stappen ‘begrijpen en interpreteren’ kon in sommige gevallen aangetoond worden dat een zwak signaal een relatie met ongewone voorvallen heeft. Of er werd een denklijn opgezet waarmee beredeneerd is wat de relatie van een mogelijk zwak signaal met ongewone voorvallen zou kunnen zijn en in welke context dat het geval zou kunnen zijn. In een beperkt aantal gevallen is een begin met stap 5 gemaakt in de vorm van mogelijke acties. Overigens is het niet zo dat ieder zwak signaal tot een leerpotentieel en bijbehorende actie hoeft te leiden. Het bundelen van meerdere zwakke signalen in een ‘early warning system’ is ook een optie.

AnQore
Bij AnQore zijn zwakke signalen die met weerscondities te maken hebben aangetoond die daadwerkelijk een relatie met ongewone voorvallen hebben, namelijk:
Bij temperaturen tussen 27,7 en 31,1 °C, bij temperaturen onder nul in combinatie met een hoge relatieve vochtigheid en bij windsnelheden in de range 10,6-11,8 m/ s lijkt er meer kans op ongewone voorvallen.
Opvallend is dat hitte (hoge temperatuur en hoge relatieve vochtigheid) en wind boven 11,8 m/ s daarentegen geen grotere kans op ongewone voorvallen geven. Een verklaring hiervoor kan zijn dat er protocollen zijn om bij hitte en harde wind vereisen de werkzaamheden aan te passen dan wel te stoppen. Voor andere weerscondities bestaan die niet protocollen. AnQore overweegt of met deze

resultaten additionele protocollen kunnen worden opgesteld, die gaan bijdragen aan een betere veiligheidsprestatie.
AnQore droomt van een ‘early warning systeem’ (EWS). In kleine experimenten met Big plant Data en AI zijn de afgelopen jaren inmiddels 3 zwakke signalen geïdentificeerd. En er zijn voldoende aanknopingspunten voor nog meer zwakke signalen. Hiermee is voor AnQore herbevestigd dat er zwakke signalen zijn en dat zwakke signalen daadwerkelijk te vinden zijn.

Envalior
De toepassing van de ‘Safety Stethoscope’ op de wachtdienstverslagen, met zijn diverse technieken en presentatie van diverse variabelen, op diverse manieren, geeft Envalior de mogelijkheid om sneller en beter het grote plaatje te zien (helicopterview).
De analyseresultaten van wachtdienstverslagen op de feature sentiment hebben Envalior gesterkt in de overtuiging dat het sentiment een zwak signaal is om ‘begrip voor elkaar’ inzichtelijk te maken.
Er is nog geen online en realtime app beschikbaar om dit dagelijks te gaan toepassen. Als (niet digitale) tussenoplossing wordt sinds medio 2023 aan de ploegen gevraagd om iedere dienst een waarde (in de kleur rood/ geel/ groen) te geven aan het sentiment van de wachtdienst en aan te geven waarom de betreffende score gegeven is. De resultaten hiervan worden regelmatig besproken. Het verzamelen van deze scores is overigens een nieuwe databron, die weer gebruikt kan worden om de sentiment app verder te ontwikkelen.
Om te kunnen vaststellen of het actief volgen van het sentiment tot verbetering leidt is tevens een enquête opgesteld (zie bijlage C) en uitgezet onder de medewerkers in productie en staf om inzicht te krijgen in ‘begrip voor elkaar’.

SABIC
De eerste analyseresultaten van de beschikbare en geselecteerde informatie uit de DCS systemen, hebben verhelderend inzicht gegeven in de complexiteit van dit systeem. Deze data is gebouwd en opgezet voor een visualisatie voor de Operator om een fabriek op korte termijn veilig en goed te kunnen bedrijven, wat iets heel anders is dan het doel wat dit projectteam voor ogen had, namelijk visualisatie van een ‘sentiment-monitor’ voor Supervisors/ Management/ Staf.
Het belang voor juiste interpretatie (veel systeemmeldingen, alarmen en modes bleken voorwaardelijk gekoppeld of hadden bepaalde onderlinge verbanden) en een goed beoordeelde weging (objectief en deels subjectief meegeven van een prioriteit) bleek duidelijk aanwezig. Dit was complexer dan gedacht en vergde meer tijd dan vooraf beschikbaar was gemaakt.
Wel was vanuit de data-analyses en hun visualisatie tot nu toe te zien dat er trends en beoordelingscriteria beschikbaar zijn, waar stuk voor stuk in detail naar gekeken moet worden met meerdere disciplines/ afdelingen. Het geloof dat het gewenste eindresultaat uit de data gehaald kan worden, is nog steeds aanwezig, maar zoals gezegd, vraagt veel meer tijd en inspanning dan voor SABIC beschikbaar was binnen ‘BLIC vooruit’.

CSP
Met name de rapportages van de CSP-inspecties en managementreviews lijken zwakke signalen te bevatten voorafgaand aan incidenten. Nader onderzoek zal nodig zijn om aan te tonen of dit een feature voor een ‘early warning system” (EWS) van een bedrijf kan zijn dan wel een tool kan worden.
Voor CSP zou een dergelijke analyse zich mogelijk kunnen ontwikkelen tot een hulpmiddel om het aantal en de inhoud van inspecties te optimaliseren.

CoP overall
Het samen optrekken in een CoP als de ‘Early Warning Coalitie’ geeft inspiratie. Deelnemers hebben van elkaar geleerd, ervaringen uitgewisseld en elkaar geadviseerd over uiteenlopende zaken.
Algemene voorwaarden zoals een NDA en de wijze van data delen zijn uniform ingevuld. Wel vergt het meedraaien in een CoP in combinatie met het bedrijven van een fabriek flexibiliteit.
Het thema van deze Safety Deal ‘zwakke signalen halen uit Big plant Data met behulp van AI’ heeft ons geleerd dat dit een complex proces is. Visualisatie om patronen te herkennen is de eerste stap. Klein beginnen met een lange termijn beeld is de route naar succes.

6 Delen en communiceren van leerpotentieel binnen een CoP

6.1 Voorbereiding: Waar gaat het om?

In deze stap is beschreven hoe leerpotentieel effectief kan worden gedeeld en gecommuniceerd binnen de praktijkgemeenschap (CoP) met als doel om 'beter leren' te bevorderen. Tevens is aangeven welke instrumenten zoal beschikbaar zijn in een praktijkgemeenschap om te communiceren over veiligheid en zodoende de veiligheidsprestaties van het hele cluster te verbeteren.

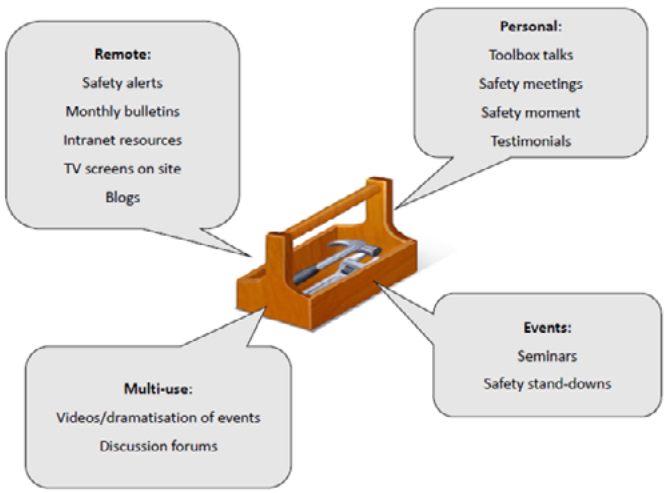
Het doel van de deelnemers in een praktijkgemeenschap is kennis beschikbaar te stellen en leerpotentieel te delen om zodoende 'beter leren' te bevorderen. 'Beter leren' omvat daarbij zowel het bereiken van meer bedrijven die mogelijk met dezelfde problemen kampen, het beïnvloeden van mensen op de langere termijn, ook lang na de herinnering aan bepaalde gebeurtenissen, het toepassen van leerpotentieel op een breder scala aan gebeurtenissen, als het bereiken en beïnvloeden van mensen buiten de praktijkgemeenschap.

Dit leidt tot wederzijdse kennisontwikkeling, innovatie en samenwerking op het gebied van veiligheid. Door informatie te delen, kunnen bedrijven van elkaar leren over best practices, risico's, ongewone voorvallen, maatregelen en verbeterpunten die relevant zijn voor hun processen, producten en diensten. Dit kan hen helpen om hun eigen veiligheidsniveau te verhogen, maar ook om bij te dragen aan de veiligheid van andere deelnemers in de praktijkgemeenschap. Door informatie te delen kunnen bedrijven ook profiteren van synergie, feedback, ondersteuning en de expertise die beschikbaar is in de praktijkgemeenschap. Dit kan hen helpen om sneller en effectiever te reageren op veranderingen, uitdagingen of kansen die zich voordoen in de omgeving.

6.2 Uitvoering: Hoe doe je dat?

De stappen voor het delen en communiceren van leerpotentieel op een CoP zijn als volgt:

- Identificeer leerpotentieel: kijk dan zowel naar leerpotentieel op het gebied van techniek, organisatie, human factors en omgeving (context). Dit onderscheid kan helpen bij het identificeren van relevante lessen en potentiële risicobeperkende maatregelen.
- Identificeer stakeholders: kijk zowel naar interne als externe stakeholders. Stel voor elk van hen vast wat hun belangen of behoeften zijn en de eventuele kernboodschap.
- Kies methode en communicatietechniek: er zijn diverse technieken beschikbaar om leerpotentieel over te brengen. In de gereedschapskist in Figuur 6.1 staan verschillende instrumenten, zoals persoonlijke (face-to-face) en multifunctionele methodes, zoals gebruik van speciale evenementen.



Figuur 6.1 Toolbox met communicatietechnieken [Energy Institute, 2016)

Er zijn nog ander soorten instrumenten om in een praktijkgemeenschap te communiceren over veiligheid, zoals:

- Platforms en kanalen om informatie te delen, zoals publicaties, evenementen, webinars, blogs, nieuwsbrieven en sociale media. Deze instrumenten kunnen gebruikt worden om kennis, ervaringen, inzichten en aanbevelingen te verspreiden en te ontvangen over veiligheidsthema's, zoals wet- en regelgeving, normen en richtlijnen, onderzoeksrapporten, nieuwsberichten, goede voorbeelden of best practices.
- Netwerken en discussies om informatie uit te wisselen, zoals bijeenkomsten, workshops, forums, chats, webcasts of video's. Deze instrumenten kunnen gebruikt worden om meningen, feedback, suggesties of vragen te delen en te bespreken over veiligheidskwesties, zoals oplossingen, verbeterpunten, leerpotentieel of actiepunten.
- Enquêtes, polls, observaties of tests om informatie te verzamelen, zoals cijfers, grafieken, tabellen, diagrammen, teksten, beelden of geluiden. Deze instrumenten kunnen gebruikt worden om gegevens, feiten, resultaten of effecten te meten en te analyseren over veiligheidsaspecten, zoals prestaties, ervaringen, behoeften, risico's, ongewone voorvallen, maatregelen of verbeteringen.

6.3 Resultaat: Hoe is het bij Chemelot gegaan?

Gezamenlijk aan de slag in een CoP betekent dat de deelnemers successen, teleurstellingen en leerpotentieel met elkaar kunnen delen. De handreiking die u nu aan het lezen bent en bijbehorende audiovisuele presentatie/ video zijn eveneens manieren om leerpotentieel te delen en te communiceren.

De uitdaging is hoe bereik je anderen die niet aan het CoP deelgenomen hebben. Dit kan zijn in de eigen organisatie van de deelnemer, zoals de eigen afdeling (onderhoud, SHE, operations), de eigen fabriek (het management team) of (indien relevant) het hele bedrijf. Voorbeelden hiervan: Envalior heeft tijdens wereldwijde Envalior-bijeenkomsten over 'BLIC vooruit' bericht. En bij kenniscentrum Brightsite is een digitaal colloquium aan Big plant Data en AI gewijd. Bij de EWC zijn als tools in het algemeen face-to-face-gesprekken en (digitale) presentaties toegepast.

Op Chemelot zijn diverse themagerichte overlegstructuren. Het EWC gaat deze overlegstructuren gebruiken om de leerpotentieel van 'BLIC vooruit' uit te dragen, zoals bij het 'Leren van Incidenten' platform en bij een 'Samen Bewust Veilig' themabijeenkomst.

Bijlage A:
Waar staan we met betrekking tot leren van eigen informatie?

Voorbereiding: Waar gaat het om?

Het is belangrijk om eerst te kúnnen leren van eigen informatie (zoals incidenten), voordat kan worden geleerd van anderen. De reden is (onder andere) beter kunnen reflecteren op eigen handelen, begrip en compassie voor eigen zwakke punten en kunnen inschatten van risico's en mogelijkheden in vergelijkbare situaties. Door te leren van eigen informatie wordt inzicht verkregen in eigen sterke en zwakke punten, en door te leren van eigen informatie wordt een lerende grondhouding ontwikkeld, die helpt om open te staan voor feedback, perspectieven en alternatieven.

Leren van incidenten (als informatiebron) is de standaard binnen de chemische industrie. Vandaar dat leren van incidenten hier het onderwerp is. In deze bijlage is daarvoor een checklist (Learning From Incidents, LFI) toegevoegd. Door toepassing daarvan kan een bedrijf voor zichzelf nagaan wat al goed gaat en wat beter zou kunnen. En het totaal beeld geeft inzicht in de verschillen en overeenkomsten tussen de partijen in een praktijkgemeenschap (CoP).

Uitvoering: Hoe doe je dat?

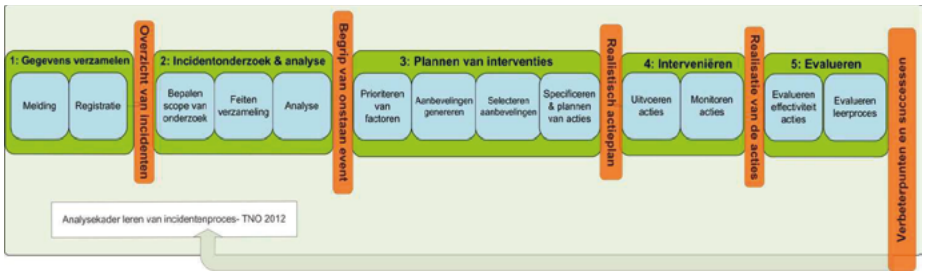
De stappen voor 'beter te leren van eigen incidenten' zijn als volgt:

1. Voorbereiden van de enquête: dit is de fase waarin de doelstelling, scope, doelgroep en methode van de enquête wordt bepaald. Er kan een online of papieren vragenlijst worden gebruikt om de perceptie van de betrokkenen over het incident te meten. En deze kan afgenomen worden bij een steekproef, of bij een hele populatie.

2. Invullen van de enquête (LFI-vragenlijst): de LFI-vragenlijst is een gestandaardiseerd instrument om de leercultuur en leereffectiviteit van een organisatie te meten. De LFI-vragenlijst bestaat uit 34 vragen die vier dimensies van leren van incidenten omvatten: rapportage, analyse, actie en evaluatie. De vragenlijst kan worden aangepast aan de context en/ of behoeften van de organisatie.

3. Analyseren: er kan gebruik worden gemaakt van statistische methoden om de betrouwbaarheid, validiteit, gemiddelden, standaarddeviaties, correlaties en verschillen tussen groepen te meten en/of berekenen. Er kan ook gebruik worden gemaakt van kwalitatieve methoden om open vragen, opmerkingen en feedback van respondenten te coderen en categoriseren. Ook kunnen sterktes, zwaktes, kansen en bedreigingen voor het leren van incidenten in de organisatie worden geïdentificeerd.

4. Terugkoppelen resultaten: dit is de fase waarin resultaten worden gerapporteerd en gepresenteerd aan belanghebbenden. Er kan gebruik worden gemaakt van grafieken, tabellen, diagrammen en tekst om belangrijkste bevindingen, conclusies en aanbevelingen te communiceren. Ook kunnen resultaten worden vergeleken met de doelstellingen, benchmarks of best practices van het leren van incidenten. Verzamel en verwerk de feedback en suggesties van belanghebbenden.



Formele procedures
Geef aan welke van de volgende stappen in uw organisatie formeel zijn geregeld. Denk hierbij aan procedures, documenten en systemen.
Kruis aan als deze stap apart geregeld is. Indien de stap samenvalt met een andere stap, dan alleen de eerste aankruisen.

Melden van incidenten	☐
Registreren van incidenten	☐
Bepalen scope van het onderzoek naar het incident	☐
Feiten verzameling	☐
Analyse	☐
Prioriteren van factoren en oorzaken	☐
Aanbevelingen genereren	☐
Selecteren aanbevelingen	☐
Specificeren en plannen van acties	☐
Uitvoeren van acties	☐
Monitoren van acties	☐
Evalueren effectiviteit acties	☐
Evalueren leerproces, om te zien of het doorlopen van de hier genoemde stappen verbeterd kan worden	☐

Uitvoering

Welke van deze stappen wordt volgens u goed uitgevoerd in uw organisatie?

Melden van incidenten	☐
Registreren van incidenten	☐
Bepalen scope van het onderzoek naar het incident	☐
Feiten verzameling	☐
Analyse	☐
Prioriteren van factoren en oorzaken	☐
Aanbevelingen genereren	☐
Selecteren aanbevelingen	☐
Specificeren en plannen van acties	☐
Uitvoeren van acties	☐
Monitoren van acties	☐
Evalueren effectiviteit acties	☐
Evalueren leerproces, om te zien of het doorlopen van de hier genoemde stappen verbeterd kan worden	☐

	zeer slecht	slecht	neutral	goed	zeer goed
Hoe beoordeelt u in het algemeen het overzicht van incidenten die plaats hebben gevonden binnen uw afdeling? (Fase 1)	☐	☐	☐	☐	☐
Hoe beoordeelt u in het algemeen het inzicht in oorzaken van incidenten op uw afdeling? (Fase 2)	☐	☐	☐	☐	☐
Hoe beoordeelt u de kwaliteit van de actieplannen? (Fase 3)	☐	☐	☐	☐	☐
Hoe beoordeelt u in het algemeen de kwaliteit van de uitvoering van de acties? (Fase 4)	☐	☐	☐	☐	☐
Hoe goed worden uitgevoerde acties geëvalueerd? (Fase 5)	☐	☐	☐	☐	☐
Hoe goed wordt volgens u het leren van incidenten proces geëvalueerd? (Fase 5)	☐	☐	☐	☐	☐

Bron: Drupsteen vragenlijst LFI in drie talen, via TNO

Bijlage B:
Geanonimiseerd NDA format ‘BLIC vooruit’

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

THE UNDERSIGNED:

1. ……, a limited partnership incorporated under the laws of the Netherlands, whose registered office is at ……, listed in the Commercial Register of the Chamber of Commerce under file number ……, duly represented by ……., hereinafter referred to as ‘….’,
2. ….., a legal entity governed by public law of the Netherlands whose registered office is at …., listed in the Commercial Register of the Chamber of Commerce under file number, duly represented in this matter by ……., hereinafter referred to as: ‘…’,
   and
3. ….., a private limited liability company under the laws of the Netherlands, whose registered office is at ……., listed in the Commercial Register of the Chamber of Commerce under file number ….., duly represented in this matter by ……, hereinafter referred to as ‘…..’,
   …, … and … are hereinafter collectively referred to as ‘**Parties**’ and each individual as ‘**Party**’,

WHEREAS

1. Parties desire to engage in and/or wish to carry on confidential discussions and negotiations regarding the Safety Deal “BLIC vooruit”;
2. ….. is located at Chemelot and is active in the field of …….;
3. Parties expect that during said discussions, negotiations and/or activities it may be necessary for each Party to disclose information, data, technologies, studies, findings, ideas, plans, results, knowledge and/or experience to the other Party that it regards as confidential;
4. Parties wish to reciprocally protect and safeguard the confidentiality of such information, data, technologies, knowledge and/or experience and desire to define their respective rights and obligations in relation thereto in this Agreement;

PARTIES AGREE ON THE FOLLOWING:

1. Definition and interpretation
Each of the Parties hereto is a disclosing party (the “**Discloser**”) and a receiving party (the “**Recipient**”) of Confidential Information. **Confidential Information means** …., …. and/or ….
information as the context of this Agreement requires, disclosed by a Discloser to a Recipient in connection with the **Purpose**, as defined in clause 2, regardless of such information being disclosed in oral, written, graphic, machine recognizable, electronical and/or sample form and that is identified as “Confidential” or “Proprietary” with an appropriate, conspicuous marking; or in case of oral or visual disclosures, that is identified by the Discloser at the time of disclosure as being disclosed in confidence or marked as confidential or proprietary. Information that was not marked or identified as confidential or proprietary shall be treated as Confidential Information upon a written notice to the Recipient within 30 days from disclosure;

…. **Confidential Information** means information relating to means information relating to knowledge Sitech brings in on the historic and actual ways to prevent and predict incidents by means of the so-called Integrated Management System Plants &Sitech - used for managing EHS,

maintenance and operations -, including work processes and underlying documents, practices, procedures, instructions, tools, formats, checklists, criteria, sequences, data, and on challenge of the results of the analysis on big data, predictive modelling techniques, Artificial Intelligence and Machine Learning and on managerial aspects related to the Purpose.

.... Confidential Information means information relating to knowledge TNO brings in on processing and analysis of big data, predictive modelling techniques, Artificial Intelligence and Machine Learning, as well as particular expertise and know-how on industrial Health, Safety and Environment (HSE) in the chemical industry .

..... Confidential Information means information relating to knowledge ..... brings in on, historic and actual plant data of various sources and challenge of the results of the analysis on big data, predictive modelling techniques, Artificial Intelligence and Machine Learning, including data from shift reports, operational meeting reports, management reports, incident reports, environmental reports and permits, HSE reports, safety studies, maintenance notifications, maintenance repairs, maintenance inspections, maintenance plans, technological studies, plant modifications and investments, measurements and analyses, plant operation systems and process control systems

Affiliate shall mean any company or other entity, whether or not a legal person, which directly or indirectly controls, is controlled by or is under joint control with a Party. For this purpose, a Party is deemed to control a company or entity if it (i) owns, directly or indirectly, more than 50 percent of the capital of the other company, or (ii) in the absence of such ownership interest, substantially has the power to direct or cause the direction of the management and set the policies of such company or entity.

Effective Date shall mean .....

2. Purpose of disclosure
Confidential Information is disclosed solely for the purpose of an exchange of information between the Parties for the Safety Deal “BLIC vooruit” (“Purpose”).
In this respect Parties will exchange information on (i) available data sources in the plant, (ii) potential features hidden in these datasources, and (iii) the interpretation of the results of experiments with the datasources and AI techniques.
This Agreement does not obligate a Party to disclose any Confidential Information to (one or more of) the other Parties or to enter into any other agreement or arrangement, nor shall it be construed as granting any rights by license or otherwise in any such information, including but not limited to, software or inventions.

3. Standard of care
The Recipient agrees to receive and maintain Confidential Information in the strictest confidence and to safeguard the Confidential Information with the same degree of care as is used by the Recipient to protect its own confidential information, but in no event less than reasonable care. The Recipient agrees further not to use Confidential Information received from the Discloser for its own benefit or for a purpose other than as expressly set forth in this Agreement; or to disclose such information to third parties, including but not limited, to Affiliates and subsidiaries of the Recipient, without the prior written permission of the Discloser.

The Recipient shall handle, test, use and keep the Confidential Information from the Discloser in conformity with all applicable legal requirements. Except as provided otherwise, the Recipient shall not disclose, publish, disseminate or make accessible any part of the Confidential Information, in any way or form, to anyone. No photographs, compositional or structural analysis shall be made of any part of the Confidential Information for a purpose other than expressly set forth in this Agreement. The Recipient shall not reverse-engineer, disassemble, re-assemble or decompile any Confidential Information.

4. Disclosure to Affiliates and employees
The Recipient further agrees to disclose the Confidential Information only to its Affiliates, directors, officers, employees and/or other representatives who have a need to have access to and knowledge of the Confidential Information solely for the Purpose. Prior to disclosure of any Confidential Information to such persons, the Recipient shall inform each such person of the confidential nature of the Confidential Information and shall require that the person expressly agrees to treat the Confidential Information as is provided in this Agreement, by countersigning this Agreement or signing a Non-Disclosure Agreement with the Recipient that contains terms and conditions that are no less restrictive than those herein or has similar confidentiality obligations in its labor agreement. Notwithstanding due observance of these requirements, the Recipient shall be liable for any breach of this Agreement by such person.

5. Exceptions
The Recipient is not obligated to keep as confidential any Confidential Information that the Recipient can demonstrate by evidence (i) was lawfully known to the Recipient or in its possession before the disclosure hereunder free of any obligation to keep it confidential at the time it was received or obtained by the Recipient; (ii) was publicly available at the time it was received or obtained by Recipient through no wrongful act of default of the Recipient; (iii) is received or obtained by Recipient without restriction from a third party having the legal right to do so other than Discloser or any of its Affiliates; (iv) has been developed by the Recipient independently of the Confidential Information; or (v) is approved for disclosure or release by written authorization of the Discloser.

6. Legal obligation to disclose
Should the Recipient be obligated to disclose Confidential Information received hereunder pursuant to a statutory obligation, the order of a court of competent jurisdiction, arbitrator or the requirement of a competent regulatory body, the Recipient shall, to the extent permitted by law, before such disclosure is made immediately notify the Discloser so that Discloser may oppose the requirement and/or seek a protective order and/or other action, and upon the request of the latter, shall reasonably cooperate with the Discloser in contesting such a disclosure and/or seeking such protective order and/or other action. If disclosure is ultimately required, then the Recipient shall restrict any disclosure to only such information that is legally required to be provided and will use reasonable endeavors to assure confidential treatment is accorded such Confidential Information.

7. Copies
The Recipient agrees that it will immediately cease use of and, within ten (10) days after written request by the Discloser, return or, at the Discloser's sole discretion destroy, all documents and tangible materials in its possession which contain any Confidential Information and permanently erase from its systems and data carriers any Confidential Information held by it in intangible form. The return requirement pursuant to this section does not apply to (a) copies of Confidential Information not reasonably capable of being readily located and segregated (such as, for example, routinely made backup copies of electronically-exchanged confidential and other information), or (b) each Recipient's legal department or its outside legal counsel may retain one archival copy of Discloser's Confidential Information for (i) copies that parties are bound to keep a copy of under the applicable law (for purposes of regulatory compliance, compliance with the terms and conditions of this agreement or otherwise), (ii) for evidentiary purposes (for example for use in case of a dispute concerning this agreement). For the avoidance of doubt, all confidentiality obligations and restrictions will continue to apply to all such copies until the deletion thereof. Upon request of the Discloser, the Recipient shall certify in writing that the Recipient has complied with the obligation set forth in this Clause.

8. Intellectual property rights
Nothing in this Agreement shall be construed as granting any Party any rights under any patents

and/or any other intellectual or industrial property rights be they presently owned or subsequently owned by another Party or by its Affiliates and/or to Confidential Information of another Party or of its Affiliates and shall not claim any legal right thereto, whether by means of patent application or otherwise. All intellectual property rights arising out of the Purpose as described in this Agreement shall remain with and be vested in the Party from which they originate. No Party is in any way obligated to provide or accept Confidential Information.

9. Effective Date and term
This Agreement commences on the Effective Date and shall continue for a period of 1 year. Any Party may by written notice to another Party terminate this Agreement at any time by giving thirty (30) days prior written notice.

The Recipient's obligations under this Agreement shall survive the termination or expiration of this Agreement, regardless of the manner of such termination, for a period of three (3) years from the date of last disclosure under this Agreement.

10. Severability
All rights and restrictions contained herein may be exercised and shall be applicable and binding only to the extent that they do not violate any applicable laws and are intended to be limited to the extent necessary so that they will not render this Agreement illegal, invalid of unenforceable. In the event of the invalidity or unenforceability of any provision of this Agreement under applicable law, Parties agree that such invalidity or unenforceability shall not affect the validity or enforceability of the remaining portions of this Agreement.

11. Assignment
Neither this Agreement nor any right hereunder, shall be assignable by any Party without the prior written consent of the other Parties, and any purported assignment and/or amendment without such written consent shall be void.

12. No warranties
The Discloser shall not have any liability or responsibility for errors or omissions in, or any decisions made by the Recipient in reliance upon, any Confidential Information disclosed or acquired pursuant to this Agreement. The Recipient assumes all risk, known or unknown, arising from its use of Confidential Information, and the Discloser assumes no responsibilities whatsoever for the completeness, utility, quality, or accuracy of any Confidential Information and shall have no liability of any kind to the Recipient or any third party arising out of such use. The parties expressly recognize that the Confidential Information is provided "as is" and that the Discloser makes no warranties, express, implied, statutory or otherwise (including without limitation, warranties of merchantability, fitness for purpose or of non-infringement of third party rights) in respect of the Confidential information.

13. Whole agreement
This Agreement shall be binding upon and insure to the benefit of the Parties' successors in interest. This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof, and shall supersede all previous or contemporaneous communications, representations, understandings, and agreements, either oral or written, between the Parties or any officials or representatives thereof. This Agreement may not be changed or modified except by a written agreement signed by the Parties hereto or by their successors in interest. Nothing contained in this Agreement shall be deemed to grant to any Party the right to make commitments of any kind for, on behalf of, or for the account of another Party without the other Party's prior written consent.

14. Counterparts and signature pages
This Agreement may be executed and delivered in multiple counterparts, each of which will be

deemed an original, and all of which together will constitute one and the same instrument. This Agreement may be executed and delivered by facsimile and with separate signature pages with the same effect as though all parties had executed and delivered the same original signature page.

15. Governing law and jurisdiction
This Agreement shall be construed in accordance with and governed by the law of the Netherlands. Any and all disputes between the Parties arising out of or in connection with this Agreement and/or any agreement, arrangement or undertaking arising out of this Agreement shall be finally and exclusively resolved by arbitration under the Rules of Arbitration of Nederlands Arbitrage Instituut (NAI) by one or more arbitrators to be appointed in accordance with said Rules. The place of arbitration shall be Maastricht, The Netherlands. The arbitral procedure shall be conducted in the Dutch language.

THUS, AGREED AND EXECUTED

Meer informatie over NDA op te vragen bij auteurs

Bijlage C:
Enquête ‘begrip voor elkaar’

Intro

internal use only

We zijn continu op zoek naar mogelijkheden om onze veiligheidsprestatie te verbeteren.

Sinds dit jaar zijn we aan de slag met het (technisch) sentiment van de shift, als een soort van graadmeter hoe de shift verlopen is en of we dezelfde beelden bij een shift hebben. Hoe doen we dat? Met behulp van een AI tool wordt het technisch sentiment van de shift reports bepaald en iedere shift geeft zelf aan het einde van de dienst een score aan het sentiment.

Wij willen nu (aan het begin) en eind van het jaar/begin volgend jaar bij jullie ophalen wat jullie ervan vinden en of we hiermee op de goede weg zijn. Het zou fijn zijn als jullie de volgende vragen willen beantwoorden.

Alvast dank en het spreekt voor zich dat we de resultaten (anoniem) zullen delen.

Aankruisen

Ik behoor tot

- ☐ Continudienst
- ☐ Dagdienst

Bij het verloop van de shift hebben de continu- en dagdienst hetzelfde beeld

Helemaal niet eens	Niet eens	Neutraal	Eens	Helemaal eens

Niet van toepassing / Ik weet het niet

Continu- en dagdienst begrijpen elkaar als het om veiligheid gaat

Helemaal niet eens	Niet eens	Neutraal	Eens	Helemaal eens

Niet van toepassing / Ik weet het niet

Continu- en dagdienst hebben goede gesprekken met elkaar over veiligheid

Helemaal niet eens	Niet eens	Neutraal	Eens	Helemaal eens

Niet van toepassing / Ik weet het niet

Korte toelichting

internal use only

Ik behoor tot

- ☐ Continudienst
- ☐ Dagdienst

Denk je dat meer inzicht in het (technisch) sentiment ons gaat helpen?
(Aankruisen wat van toepassing is en aanvullen met tekst)

- ☐ Zo ja, waarom?

.....

- ☐ Zo nee, waarom niet?

.....

- ☐ Ik weet niet wat met (technisch) sentiment bedoeld wordt
- ☐ Ik heb nog niet meegekeregen dat we hiermee bezig zijn
- ☐ Anders:

.....

Bijlage D:
Lijst met afkortingen

AI	Artificial Intelligence
BLIC	Beter Leren van Informatie in de Chemie
CoP	Community of Practice
CSP	Chemelot Site permit
DCS	Distributed Control System
EWC	Early Warning CoP of Early Warning Coalitie
FtF	Face to face
IT	Informatie technologie
IP21	Aspen InfoPlus.21
LFI	Learning From Incidents
ML	Machine Learning
NDA	Non Disclosure Agreement
NLP	Natural Language Processing
BI	Business Intelligence
R	Programmeertaal
SPSS	Statistical Package for the Social Sciences
TNO	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek
TSA	Technische Sentiment Analyse
USG	Utility Support Group
WOO	Wet Openbare Overheid

Transformatie naar een duurzame industrie

Brightsite levert een belangrijke bijdrage aan de overgang van de chemische industrie naar hernieuwbare energie en grondstoffen, met als doel deze sector klimaatneutraal te maken en oplossingen te bieden voor andere sectoren. Wij stimuleren de ontwikkeling en commerciële toepassing van technologieën die de chemische industrie in staat stellen haar doelstellingen op het gebied van duurzaamheid, veiligheid en menselijk kapitaal te bereiken, in overeenstemming met de klimaatuitdaging en de energietransitie.

Wilt u meer weten over de inhoud van deze Handreiking? Neem dan contact op met de auteurs:

Esta de Goede
esta.goede-de@sitech.nl

Johan van Middelaar
johan.vanmiddelaar@tno.nl

Wilt u meer weten over hoe wij aankijken tegen de transitie in de chemie of wilt u met ons samenwerken? Neem dan contact met ons op via **www.brightsitecenter.com**

