Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

TNO-rapport

TNO 2022 R10378

Herstelvermogen binnen OT infrastructuren

Datum 17 februari 2022

Auteur(s) Bart Gijsen, Yoram Meijaard, Bram Poppink

Aantal pagina's 33 (incl. bijlagen)
Aantal bijlagen 1
Opdrachtgever NCSC
Projectnaam -cy- NCSC 2021 Cyber Weerbaarheid - Herstelvermogen
Projectnummer 060.46708/01.02

Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

Voorwoord

Dit rapport is een direct resultaat van het onderzoek verricht in de meerjarige (2020-2022) onderzoekssamenwerking tussen het NCSC en TNO. Dit rapport is tot stand gekomen door inhoudelijke en richting gevende bijdrage van het NCSC (onder andere Jeroen van der Ham en Rik van Dijk), de bijdrage van domein experts van Nederlandse organisaties en het NCSC, en de inhoudelijke inbreng van het TNO projectteam (de auteurs van dit rapport, zie voorblad en management samenvatting). Wij danken alle betrokkenen voor hun bijdragen.

Dit rapport is op de NCSC website gepubliceerd, onder het thema onderzoek: www.ncsc.nl/onderzoek.

Tevens is dit rapport op de TNO website gepubliceerd onder het thema Cyber Security: het belang van een integrale oplossing.

Naast dit rapport zijn er ook andere aanverwante onderzoeksresultaten beschikbaar, of zijn nog in ontwikkeling, welke onderstaand zijn weergegeven.

Reeds beschikbaar:

- *Rapport 'Herstelvermogen binnen IT infrastructuren'.*

In ontwikkeling:

- *Herstelvermogen self-assessment;*
- *Herstelvermogen good-practices.*

Managementuittreksel

Titel :	Herstelvermogen binnen OT infrastructuren
Auteur(s) :	Bart Gijsen, Yoram Meijaard, Bram Poppink
Datum :	17 februari 2022
Rapportnr. :	TNO 2022 R10378

Inleiding. Herstelvermogen speelt een cruciale rol in de cyberweerbaarheid van organisaties, waaronder de doelgroep organisaties van het Nationaal Cyber Security Center (NCSC). In een meerjarige onderzoekssamenwerking tussen het NCSC en TNO is herstelvermogen daarom aangewezen als een belangrijk onderwerp voor kennisopbouw. In 2020 is een verkennend onderzoek uitgevoerd naar de status quo van herstelvermogen binnen Informatie Technologie (IT) infrastructuren bij Nederlandse organisaties[1]. In 2021 is dit onderzoek verbreed door ook de status quo van herstelvermogen binnen Operationele Technologie (OT) infrastructuren te inventariseren, en vast te stellen welke aspecten van belang zijn bij OT herstelvermogen. Dit rapport is het resultaat van het onderzoek naar OT herstelvermogen uitgevoerd in 2021.

In dit rapport worden de drie onderstaande onderzoeksvragen beantwoord:

a) Welke aspecten zijn van belang om herstelvermogen in te richten voor OT-infrastructuren bij de doelgroepen van het NCSC?
b) Wat is er anders ten opzichte van de situatie bij IT-infrastructuren?
c) Wat is de stand van zaken op het gebied van herstelvermogen bij OT doelgroep organisaties?

Methode. Om deze vragen te beantwoorden zijn drie onderzoeksfases uitgevoerd:
1) domeinverkenning, 2) interviews en 3) rapportage.

De *domeinverkenning* is uitgevoerd om tot een eerste beeld te komen van OT herstelvermogen in verschillende vitale sectoren waar OT wordt ingezet. Voor de domeinverkenning zijn (TNO-interne) domein experts bevraagt en is een literatuurscan uitgevoerd. Het eerste beeld is opgeschreven in een tussentijdse deliverable en gepresenteerd aan het IACS expert board[2] waar een korte discussie is gevoerd om dit voorlopige beeld te toetsen en aandachtspunten voor het vervolgonderzoek op te halen.

Daarna zijn er vier *interviews* afgenomen bij Nederlandse vitale infrastructuur organisaties. Deze organisaties beheren infrastructuur binnen verschillende OT domeinen. Op basis van deze gesprekken is het voorlopige beeld uitgebreid en aangescherpt. De interviews zijn in vertrouwelijkheid uitgevoerd en de resultaten zijn onherleidbaar gerapporteerd.

Tot slot, in de *rapportage* is het aangescherpte beeld opgeschreven in een concept versie van dit rapport. Dit rapport is door middel van een review geverifieerd bij een viertal van de organisaties aangesloten bij de IACS expert board en bij domeinexperts van het NCSC.

[1] De resultaten van dit onderzoek naar IT herstelvermogen zijn te vinden in deze publicatie: https://www.ncsc.nl/documenten/rapporten/2021/mei/10/index.

[2] Een wederkerende bijeenkomst, georganiseerd door het NCSC, waarin verschillende Nederlandse organisaties met zogenaamde Industrial Automated Control Systems (IACS), allemaal organisaties met een eigen OT infrastructuur, samenkomen om kennis en ervaringen te delen.

Aspecten OT herstelvermogen (onderzoeksvraag a). In dit onderzoek is OT herstelvermogen gedefinieerd als “de mate waarin een organisatie efficiënt en effectief in staat is om verstoord geraakte functionaliteit, die voorzien wordt door OT, weer beschikbaar te maken”. Voor OT herstelvermogen gelden verschillende aspecten opgedeeld in: 1) voorbereiden op herstel[3], 2) herstel-in-uitvoering, 3) leren van uitvoering en 4) overige aspecten.

Onder *voorbereiden op herstel* valt het opstellen van het dreigingsbeeld en voorbereiding van technische en organisatorische herstelmaatregelen. Hoewel de geïnterviewde organisaties de voorkeur geven aan preventiebeleid, geven alle geïnterviewde organisaties aan dat er ook protocollen klaarliggen voor het treffen van OT herstelmaatregelen.

Onder *herstel in uitvoering* valt, onder andere, de detectie, impactanalyse en besluitvorming benodigd voor herstel. De geïnterviewde organisaties geven aan de meeste activiteiten ten aanzien van herstel-in-uitvoering onder controle te hebben. Hierbij wordt opgemerkt dat de fysieke wereld waarin OT wordt toegepast de snelheid van herstel beperkt als er op locatie acties uitgevoerd moeten worden. Bovendien komt herstel vaak neer op herstel van een gedeelte van de infrastructuur en zelden op herstel van de gehele infrastructuur.

Onder *leren van uitvoering* valt de evaluatie van het incident en herstel. Dit wordt door alle geïnterviewde organisaties als zeer belangrijk beschouwd. Echter, onder andere door de heterogeniteit van OT systemen is de ruimte voor collectief leervermogen tussen verschillende organisaties beperkter dan voor meer algemeen gebruikte IT systemen.

Onder *overige aspecten* vallen herstelmaatregelen zoals: oefeningen, afstemming met ketenpartners en collectief herstelvermogen. Er wordt aangegeven dat de meest voorkomende herstelsituaties geoefend worden, maar oefeningen die een risico vormen voor de veiligheid of procescontinuïteit worden vermeden. Genoemde voorbeelden van collaboratieve oefeningen van OT herstelvermogen beperken zich tot directe betrokkenen bij een bedrijfsproces. De afstemming met ketenpartners verschilt per organisatie en is vooral gedreven door de mate van afhankelijkheid (bijvoorbeeld, het maken van afspraken over herstel als een organisatie gebruik maakt van onder-aannemende beheerders van infrastructuur).

Verschil met IT herstelvermogen (onderzoeksvraag b). Er zijn typische eigenschappen van OT infrastructuren die invloed hebben op OT herstelvermogen. Zo is er bij OT sprake van een *sterke koppeling tussen de gebruikte systemen en het onderliggende fysieke proces*. Verder blijft het onderliggende fysieke proces vaak voor langere gelijk (bijvoorbeeld de aansturing van een sluis, brug, of chemische fabriek), waardoor er bij OT infrastructuren vaak sprake is van een *lange levensloop en gemiddeld hoge leeftijd* van de gebruikte systemen. Bovendien bestaat veel OT uit *decentrale systemen*, waarbij het systeem zich vaak uitspreidt over een groot geografisch gebied. Eén van de gevolgen van deze verschillen tussen toepassing van OT en IT is een tragere hersteltijd voor lokale, fysieke OT componenten (zie ook de eerdere opmerking over *herstel-in-uitvoering*).

[3] Merk op dat preventiemaatregelen, ondanks grote relevantie voor OT security, niet binnen de scope van dit onderzoek vallen. Echter, sommige aspecten zijn zowel van belang voor preventie als voor herstel en zijn wel meegenomen als onderdeel van herstelvermogen. Voorbeelden van dergelijke aspecten zijn: het opstellen van een dreigingsbeeld, incidentdetectie en incidentevaluatie.

Een ander opmerkelijk verschil tussen IT en OT is de organisatiecultuur, want in de OT heerst een duidelijke *veiligheidscultuur*. Deze cultuur zorgt ervoor dat *safety* zeer prominent wordt meegenomen in eisen met betrekking tot herstelvermogen en afwegingen (*safety-first*). In tegenstelling tot in de IT, waar eisen voor herstelvermogen vaak beperkt zijn tot *confidentiality*, *integrity*, en *availability*.

De OT doelgroep organisaties van het NCSC, waaronder de geïnterviewde organisaties, beslaan een verscheidenheid aan sectoren en toepassingsdomeinen die elk hun eigen unieke kenmerken hebben. Deze sectorale kenmerken hebben in meer of mindere mate invloed op OT herstelvermogen. De sectorale verschillen, welke invloed hebben op OT herstelvermogen, die in dit onderzoek in kaart zijn gebracht zijn: *marktinrichting*, *innovatietempo*, *volwassenheid*, *toename/afname van gebruik infrastructuur*, *karakteristieken van het fysieke proces*, *gebruikte OT systemen*, en de *relevante cyberdreigingen*.

Status quo OT herstelvermogen (onderzoeksvraag c). Het algemene beeld dat uit dit onderzoek naar voren komt is dat OT organisaties hun verantwoordelijkheid nemen ten aanzien van herstelvermogen en vertrouwen hebben in hun herstelvermogen.

Vanwege de sectorale verschillen is het lastig om meer uniforme uitspraken te doen over de stand van zaken ten aanzien van OT herstelvermogen. De eisen die worden gesteld aan herstelvermogen zijn sector specifiek, evenals de regelgeving en toezicht op OT[4]. Enkele van de geïnterviewde organisaties geven aan dat de regelgeving over herstelvermogen verduidelijkt zou kunnen worden en dat, in vergelijking met andere landen, het toezicht redelijk vrijblijvend is ingericht. Daarnaast geven sommige organisaties aan dat ze, mede door de sectorale aanpak[5], nauwelijks tot geen ervaring hebben met (oefenen van) herstel na een grootschalig incident die meerdere sectoren raakt.

De toenemende invoering van IT componenten in OT infrastructuren, de zogeheten IT/OT convergentie, zorgt voor efficiënt beheer van de infrastructuur en vergaande optimalisatiemogelijkheden. Echter, IT/OT convergentie vergt aandacht om tot een weerbare inrichting te komen. De mate van IT/OT convergentie verschilt per sector en daarmee verschilt ook de relevantie van cybersecurity per sector. Een hoge mate van IT/OT convergentie maakt de implementatie van adequate OT herstelmaatregelen nog belangrijker en urgenter. In het licht van de IT/OT convergentie is er enige twijfel of (het tempo van) de getroffen maatregelen voldoende zijn.

Aanbevelingen. Op basis van dit onderzoek is aan te bevelen om duidelijke en uniforme kaders te stellen over het herstelvermogen van vitale OT infrastructuren en effectief toezicht daarop. Dit behelst ook het delen van meer informatie en cross-sectorale afstemming over herstelvermogen. Specifiek is er behoefte aan meer duidelijkheid over:

1. de verwachtingen richting vitale OT infrastructuur aanbieders ten aanzien van normen voor herstel van hun operationele processen;
2. de (periodieke) toetsing van de toepassing van deze normen;
3. aanscherping van de NIS Directive[6] door de scope duidelijker te verbreden van IT naar IT en OT; en

[4] Tot op zekere hoogte geldt dit ook voor IT. Echter, voor IT zien we dat sommige regelgeving, zoals AVG, generiek van toepassing zijn en dat regelgeving in verschillende sectoren vaak gebaseerd is op generieke informatiebeveiligingsstandaarden,
[5] Deze zin start bewust met de term “Mede”, omdat een tweede factor is dat een grootschalige, sector-overstijgend incident zich (tot dusver) niet heeft voorgedaan.
[6] https://www.enisa.europa.eu/topics/nis-directive

4. een richtlijn voor organisaties over een geschikte wijze van samenwerking tussen en/of integratie van het operational control center (OCC) en het security operation center (SOC).

Uit het onderzoek blijkt dat er ten aanzien van OT herstelvermogen een rol voor het NCSC voorzien wordt. Een verdere inventarisatie van de behoefte van doelgroep organisaties zou een grondslag kunnen bieden voor de positionering van het NCSC.

Inhoudsopgave

1 Inleiding

In de afgelopen jaren heeft er een paradigmaverschuiving plaatsgevonden in het cybersecuritylandschap: het is niet langer de vraag óf een organisatie kwetsbaar is voor toekomstige incidenten, maar een betere vraag is wannéér een organisatie getroffen zal worden door een volgend incident. Dit betekent dat men in de praktijk de nadruk van maatregelen zal moeten verleggen van preventiegerichte maatregelen naar weerbaarheidgerichte maatregelen. *Herstelvermogen* is één van de belangrijke componenten van weerbaarheid, want op het moment dat een organisatie getroffen wordt door een incident is het herstelvermogen van deze organisatie van cruciaal belang.

Herstelvermogen is daarom binnen de NCSC onderzoeksagenda[7] voor de periode 2019-2022 aangewezen als een belangrijk onderwerp voor onderzoek, gegeven de cruciale rol die herstelvermogen speelt in de cyberweerbaarheid van haar doelgroep organisaties. Ook degelijk ingericht herstelvermogen draagt bij aan het voorkomen dat een incident bij één (doelgroep)organisatie kan leiden tot significante negatieve maatschappelijke impact, of zelfs tot een cascade effect van verstoring in een gehele (vitale) dienstketen.

Met deze aanleiding zijn het NCSC en TNO in 2020 gestart met verkennend onderzoek naar herstelvermogen binnen het IT-domein. Er is kwalitatief onderzocht wat de status-quo is van *IT herstelvermogen* bij Nederlandse organisaties, waarvan de resultaten begin 2021 zijn opgeleverd[8]. In vervolgonderzoek is de scope verbreed naar *OT herstelvermogen*.

Namelijk, voor veel van de doelgroep organisaties van het NCSC, vooral vitale infrastructuur organisaties, is toepassing en beheer van OT onderdeel van het primaire proces. Daarmee is Nederland sterk afhankelijk van OT voor het normaal functioneren van de maatschappij. Daarom is de verbreding van dit onderzoek naar het OT domein relevant voor zowel het NCSC als (een deel van) haar doelgroepen.

Door technologische ontwikkelingen convergeren van oudsher geïsoleerde OT infrastructuren meer en meer met Informatie Technologie (IT) infrastructuren zoals bedrijfsnetwerken of zelfs het internet. Vaak ten behoeve van verhoogde efficiëntie en het op afstand kunnen aansturen van fysieke processen. Dit resulteert in een veranderend dreigingslandschap[9] voor OT infrastructuren, en daarmee dus ook voor de vitale infrastructuur van Nederland. In dit rapport wordt besproken wat de stand van zaken is en welke mogelijke verbeteringen worden gezien ten aanzien van herstelvermogen voor onze vitale OT infrastructuren.

Er is bewust gekozen om de scope van het onderzoek naar herstelvermogen niet te beperken tot cyberdreigingen. Ook het herstel na niet-intentionele verstoringen is relevant voor dit onderzoek. Een belangrijke reden hiervoor is de veronderstelling dat ervaringen en kennis van herstel naar aanleiding van verstoringen ook relevant kunnen zijn voor herstel naar aanleiding van cyberincidenten.

[7] https://www.ncsc.nl/documenten/publicaties/2019/september/26-9-2019/ncsc-onderzoeksagenda-2019-2020.
[8] De resultaten van dit onderzoek naar IT herstelvermogen, voorafgaand aan dit onderzoek, zijn te vinden in deze publicatie: https://www.ncsc.nl/documenten/rapporten/2021/mei/10/index.
[9] https://www.nctv.nl/documenten/publicaties/2021/02/03/dreigingsbeeld-statelijke-actoren-3-februari-2021

In dit onderzoek gaan we uit van de volgende definitie van OT herstelvermogen:

> *OT herstelvermogen is de mate waarin een organisatie efficiënt en effectief in staat is om verstoord geraakte functionaliteit, die voorzien wordt door OT, weer beschikbaar te maken.*

Deze definitie is breed geformuleerd aangezien herstelvermogen een heel scala aan maatregelen raakt: van redundantie tot data-back-ups, van tijdelijk herstel tot duurzame vernieuwing, en van herstelprocedures tot crisis management. Overige relevante definities zullen worden behandeld in sectie 1.1.

Naast een definitie is het ook van belang om te bepalen welke aspecten van belang worden geacht voor OT herstelvermogen. Voor IT herstelvermogen is in het onderzoek uitgevoerd in 2020, naast een vergelijkbare definitie als bovenstaande definitie van OT herstelvermogen, ook een opdeling gemaakt van de belangrijkste hoofd- en deelaspecten waarin IT herstelvermogen kan worden onderverdeeld. Voorbeelden van deze hoofd- en deelaspecten zijn: *voorbereiden op herstel* (hoofdaspect) en *dreigingsbeeld opstellen* (bijbehorend deelaspect), *herstel-in-uitvoering* (hoofdaspect) en *incident detectie* (bijbehorend deelaspect), en *leren van uitvoering* (hoofdaspect) en *evaluatie* (bijbehorende deelaspect). In dit onderzoek worden dezelfde aspecten als relevant beschouwd voor OT herstelvermogen. Deze aspecten worden genoemd in hoofdstuk 2, echter niet opnieuw uitgebreid toegelicht. Ook worden de hoofdaspecten gebruikt als leidraad voor het toelichten van de status-quo van OT herstelvermogen in hoofdstuk 3.3. Voor een toelichting op deze aspecten verwijzen wij u naar de publicatie van het voorafgaande onderzoek[10]. Ook zal in hoofdstuk 3 verder worden ingegaan op aspecten welke specifiek relevant zijn voor OT herstelvermogen (e.g. typische eigenschappen van OT infrastructuren).

Binnen bovenstaand kader heeft TNO, in samenwerking met het NCSC, een onderzoek verricht onder Nederlandse organisaties met OT infrastructuren in beheer. Via interviews is onderzocht wat de status is van OT herstelvermogen, maar ook de invloed die IT/OT convergentie hierop heeft. De resultaten hiervan leest u in dit rapport. Deze resultaten kunnen inzicht verschaffen aan organisaties die gebruik maken van OT infrastructuren voor de (primaire) bedrijfsvoering, onder andere om de inrichting van herstelvermogen aan te scherpen. Ook verschaffen deze resultaten inzicht aan het NCSC om haar rol met betrekking tot OT herstelvermogen verder vorm te geven.

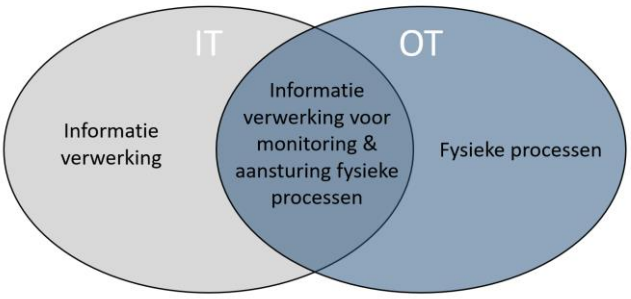
Dit document beschrijft achtereenvolgens
- aanpak van het onderzoek, in hoofdstuk 2;
- OT en herstelvermogen, in hoofdstuk 3;
- effect van digitalisering op OT herstelvermogen, in hoofdstuk 4;
- conclusies en toekomstig onderzoek, in hoofdstuk 5.

1.1 Definities en begrippen

In deze sectie zal worden toegelicht wat er wordt bedoeld met de belangrijkste termen in dit rapport. De toelichting is in sommige gevallen vertaald of grotendeels overgenomen van de documenten waar onderstaand aan gerefereerd wordt.

[10] Publicatie, zie ook voetnoot 1 en 8.

- *Operationele technologie* (*OT*) is hardware en software die een verandering detecteert of veroorzaakt door directe monitoring en/of controle van industriële apparatuur, activa, processen en gebeurtenissen[11].
- *Informatie technologie* (*IT*) is een spectrum aan hardware, software en communicatie technologie voor informatie verwerking[12]. Uitgaande van deze definities bestaat er een overlap tussen OT en IT, afgebeeld in Figuur 1.
- *OT infrastructuren* is het geheel van operationele en informatie technologie voor de monitoring en besturing van fysieke processen.
- *Vitale processen* zijn processen die zo essentieel zijn voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid[13].



Figuur 1: Overlap tussen OT en IT.

[11] https://www.gartner.com/en/information-technology/glossary/operational-technology-ot
[12] https://www.gartner.com/en/information-technology/glossary/it-information-technology
[13] https://www.nctv.nl/onderwerpen/vitale-infrastructuur

2 Aanpak en methodiek

Dit rapport is een vervolg op het eerdere onderzoek *Herstelvermogen binnen IT infrastructuren*[14]. Zoals gedefinieerd in het rapport van dit eerdere onderzoek omvat herstelvermogen een veelvoud aan aspecten, opgedeeld in:

- *voorbereiden op herstel:* opstellen van dreigingsbeeld en voorbereiding van technische en organisatorische herstelmaatregelen,
- *herstel-in-uitvoering:* incident detectie, impactanalyse, escalatie, besluitvorming, acuut en duurzaam herstel, gebruik van draaiboeken in de praktijk en improvisatie, verslaglegging tijdens incidenten en verhoogde dijkbewaking na herstel,
- *leren van uitvoering:* evaluatie van incident en herstel[15].
- *overige aspecten:* oefeningen & opleiding, afstemming met ketenpartners, en collectief herstelvermogen.

In dit rapport zullen de drie onderstaande onderzoeksvragen worden beantwoord:

a) Welke aspecten zijn er van belang om herstelvermogen in te richten voor OT-infrastructuren bij de doelgroepen van het NCSC?
b) Wat is er anders ten opzichte van de situatie bij IT-infrastructuren?
c) Wat is de stand van zaken op het gebied van herstelvermogen bij OT doelgroep organisaties, met betrekking tot het bovenstaande?

Om antwoord te geven op deze onderzoeksvragen is een viertal activiteiten uitgevoerd, welke onderstaand worden omschreven.

Eerst is er een domeinverkenning uitgevoerd voor de verschillende vitale processen[16] waar OT wordt ingezet. Door het interviewen van domein experts, veelal TNO onderzoekers die in de betreffende domeinen werkzaam zijn, en het raadplegen van relevante literatuur is een beeld gevormd van de toepassingen van OT, de typen OT systemen, de staat van IT/OT convergentie en de staat van herstelvermogen, binnen de vitale sectoren. Dit is uitgevoerd voor de volgende vitale sectoren: spoorwegen, elektriciteit, gas, drinkwater, water keren en beheren, en chemische processen. Daarnaast zijn ook radarsystemen onderzocht als een specifiek type OT dat in meerdere vitale sectoren wordt toegepast. De opgehaalde inzichten zijn tussentijds gedeeld met het NCSC.

Vervolgens zijn de tussentijdse conclusies gepresenteerd aan de *IACS expert board*. Dit is een wederkerende bijeenkomst, georganiseerd door het NCSC, waarin verschillende Nederlandse organisaties met zogenaamde Industrial Automated Control Systems (IACS), allemaal organisaties met een eigen OT infrastructuur, samenkomen om kennis en ervaringen te delen. Naast de presentatie is er ook een korte discussie gevoerd om deze voorlopige conclusies te toetsen en aandachtspunten voor het vervolgonderzoek te krijgen.

[14] Publicatie, zie ook voetnoot 1 en 8.
[15] Merk op dat preventiemaatregelen, ondanks grote relevantie voor OT security, niet binnen de scope van dit onderzoek vallen. Echter, sommige aspecten zijn zowel van belang voor preventie als voor herstel en zijn wel meegenomen als onderdeel van herstelvermogen. Voorbeelden van dergelijke aspecten zijn: het opstellen van een dreigingsbeeld, incident detectie en incident evaluatie.
[16] https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

Daarna zijn er vier externe interviews afgenomen bij Nederlandse vitale infrastructuur organisaties, allen binnen verschillende domeinen, en dus met verschillende infrastructuren in beheer. Hierbij is gebruik gemaakt van een vaste interviewvragenlijst, zie de appendix in hoofdstuk 6.1. Op basis van deze gesprekken zijn de voorlopige conclusies uitgebreid en aangescherpt. De interviews zijn in vertrouwelijkheid uitgevoerd en de resultaten zijn onherleidbaar gerapporteerd.

Als laatste stap zijn de conclusies opgeschreven in een conceptversie van dit rapport, en vervolgens door middel van review geverifieerd bij een viertal van de organisaties aangesloten bij de IACS expert board, en bij domeinexperts van het NCSC.

Dit rapport is het eindresultaat van de hierboven beschreven activiteiten.

3 OT en herstelvermogen

In dit hoofdstuk worden de bevindingen ten aanzien van de drie onderzoeksvragen beschreven die zijn vastgesteld middels de interviews met organisaties en de reviews en gesprekken met domeinexperts.

Ten aanzien van de eerste twee onderzoeksvragen wordt eerst besproken wat typische eigenschappen zijn van OT infrastructuren. Ook zullen deze eigenschappen ter verduidelijking regelmatig worden vergeleken met de typische eigenschappen van IT infrastructuren. Dit zal besproken worden in sectie 3.1. Vervolgens zullen sectorale kenmerken welke van belang zijn bij de discussie over OT herstelvermogen worden besproken in sectie 3.2. Ten slotte wordt de status quo van herstelvermogen in OT infrastructuren in Nederland besproken in sectie 3.3.

3.1 Typische eigenschappen van OT infrastructuren

Zoals in sectie 1.1 gedefinieerd, doelen we met OT op hardware en software die een verandering detecteert of veroorzaakt door directe monitoring en/of controle van industriële apparatuur, activa, processen en gebeurtenissen.

Bij OT is er daarom sprake van een *sterke koppeling tussen de gebruikte systemen en het onderliggende fysieke proces*. Dit leidt tot twee belangrijke observaties. Ten eerste zijn de OT systemen vaak maatwerkoplossingen voor één specifieke toepassing, waardoor grote technologische heterogeniteit ontstaat. Ter illustratie, een brugbedieningssysteem bestaat uit substantieel andere onderdelen en processen dan een chemische fabriek waarin een continu proces gemonitord en gestuurd moet worden. Ten tweede blijft het fysieke proces vaak (redelijk) constant, en daardoor blijven ook de functionaliteitseisen van het systeem constant, waardoor OT systemen minder veranderlijk zijn dan IT systemen.

In de OT is er daardoor ook vaak sprake van een *lange levensloop en gemiddeld hoge leeftijd* van de gebruikte systemen. IT systemen hebben typisch een levensduur van enkele jaren, terwijl in de OT het niet ongebruikelijk is dat systemen 15 tot 30 jaar in gebruik zijn. Dit heeft tot gevolg dat de snelheid waarmee technologie wordt vervangen voor OT systemen veel trager is dan voor IT systemen. Bovendien kan het vervangen van OT systemen veel werk en hinder opleveren. Bijvoorbeeld, het vervangen van een brug is een omvangrijke logistieke operatie, waarvoor een spoor of snelwegtraject vaak langere tijd moet worden afgesloten. Hierdoor wordt in het ontwerp vaak gestreefd naar een zo laag mogelijke faalkans. Hierdoor ligt er voor OT systemen, in vergelijking met IT systemen, relatief meer nadruk op preventie dan op herstel.

Het verschil in levensloop van IT en OT heeft ook gevolgen voor de beveiliging. In de interviews wordt genoemd dat de beveiliging van gebruikte communicatie protocollen, zoals *fieldbuses* en industrieel ethernet, vaak verouderd is en kwetsbaarheden bevat. Daarnaast is gebruikte IT als onderdeel van OT systemen soms dermate oud dat er geen security patches meer voor ontwikkeld worden. Door deze security kwetsbaarheden van oudere OT systemen is het van belang om voldoende aandacht te geven aan herstelvermogen (in aanvulling op de van nature zwaardere nadruk op preventie).

Bovendien bestaat veel OT uit *decentrale systemen*, waarbij het systeem zich vaak uitspreid over een groot geografisch gebied. Hierdoor krijgen OT systemen voordelen die voortkomen uit een decentraal geïmplementeerd systeem. Het belangrijkste gevolg hiervan is dat in veel gevallen een natuurlijke mate van segmentering en robuustheid is aangebracht, waarbij delen van het systeem uit kunnen vallen zonder dat dit effect heeft op andere delen van het systeem.

Een opmerkelijk verschil tussen IT en OT is de organisatie cultuur. In de OT heerst een duidelijke *veiligheidscultuur*. Alle geïnterviewden hebben aangegeven dat veiligheid van mens, proces en milieu voorop staat. Met betrekking tot cybersecurity eigenschappen werd in één van de interviews aangegeven dat in plaats van CIA de acroniem SAIC gebruikt wordt, die de onderlinge prioriteit weergeeft van Safety, Availability, Integrity en Confidentiality[17]. Vanuit een andere organisatie werd gechargeerd naar voren gebracht: "OT richt zich op safety en IT op security." Ook werd opgemerkt dat de nadruk op veiligheid van OT, in combinatie met de langere levensloop ervan, leidt tot een behoedzame houding t.a.v. het doorvoeren van veranderingen in OT. Dit staat in contrast met het hoge verandertempo van IT toepassingen. Elk van deze constateringen maken duidelijk dat er een verschil bestaat tussen de organisatiecultuur van IT en OT.

3.2 Sectorale kenmerken van belang bij OT herstelvermogen

De OT doelgroep organisaties van het NCSC, waar onder de geïnterviewde organisaties, beslaan een verscheidenheid van toepassingsdomeinen die elk hun eigen unieke kenmerken hebben. Deze sectorale kenmerken hebben in meer of mindere mate invloed op OT herstelvermogen, zoals beschreven in sectie 3.3. In dit onderzoek zijn specifiek de volgende sectorale kenmerken naar voren gekomen:

- Marktinrichting: de wijze waarop een sector is ingericht heeft invloed op de betrokken organisaties bij herstelvermogen, bijvoorbeeld op hun autonomie ten aanzien van herstelmaatregelen en het belang van communicatie en samenwerking. Als voorbeeld kenmerkt de energiesector zich door een grote mate van marktwerking en relatief veel partijen, terwijl de drinkwaterdistributie vanuit een absolute monopoliepositie gewerkt wordt.
- Innovatietempo: De verschillende sectoren innoveren op verschillende tempi. Er zijn verscheidene redenen waarom deze verschillen bestaan. Typisch ontstaat deze verscheidenheid door het verschil in noodzaak voor innovatie of concurrentiepositie. Sectoren met een hoger innovatietempo gebruiken uiteindelijk, logischerwijs, ook modernere technieken.
- Volwassenheid: Er is een verschil in de volwassenheid tussen de verschillende sectoren, zowel in de gebruikte OT besturingstechnologie, als op organisatieniveau. Bijvoorbeeld het elektriciteitsnetwerk is zeer ver in de adaptatie van nieuwe technieken. In tegenstelling, het gasdistributienetwerk berust op handwerk en heeft veel ruimte voor technologische innovatie. Deze twee sectoren lijken de uitersten van het volwassenheidsspectrum te vertegenwoordigen, met alle andere sectoren ergens ertussen.
- Toename/afname gebruik infrastructuur: In sommige sectoren wordt het gebruik van de infrastructuur uitgebreid, bijvoorbeeld in de spoorwegen, terwijl in andere sectoren het gebruik van de infrastructuur juist krimpt, bijvoorbeeld in de gasdistributie.

[17] Een ander acroniem genoemd tijdens de interviews is RAMS(SHEEP). Dit staat voor Reliability, Availability, Maintainability, Safety (plus Security, Health, Environment, Economics, Politics). De inhoud van de tekst hierboven is ook op deze acroniem van toepassing.

- Karakteristieken van proces: Processen zijn verschillend te typeren. Een proces kan discreet zijn, bijvoorbeeld in de productie van individuele producten, of continu, zoals in de elektriciteitsdistributie. Een proces kan enkel incidenteel ingezet hoeven te worden, zoals bij het sluiten van een waterkering, of een proces staat altijd aan en is slechts incidenteel buiten bedrijf, bijvoorbeeld het leveren van kraanwater in de waterdistributie.
- Gebruikte OT systemen: De verschillende gebruikte OT is grotendeels sectorspecifiek en beslaat een breed spectrum aan technologieën. Voor dit onderzoek voegt meer detailniveau dan Figuur 2, het Purdue referentie model voor OT systemen weergegeven in sectie 4.1, niet veel toe. Wel moet er rekening gehouden worden met dat de onderliggende technologie niet overeenkomstig hoeft te zijn in vergelijkingen tussen de sectoren.
- Actieve cyberdreigingen: De dreigingen vanuit verschillende actoren verschillen per sector. Het dreigingsbeeld statelijke actoren van de NCTV geeft hier inzicht in. Het is niet het doel van dit onderzoek om het dreigingsbeeld[18] verder uit te werken.

De bovenstaande sectorale kenmerken verschillen tussen de sectoren en zijn de reden waarom het niet zinnig is om het OT herstelvermogen van de verschillende geïnterviewde organisaties te scoren en met elkaar te vergelijken, zoals wel is gedaan in het onderzoek naar IT herstelvermogen in 2020. Toch wordt er getracht in de volgende sectie, 3.3, en in hoofdstuk 4, algemene conclusies te trekken over de status-quo van OT herstelvermogen. Daar waar noodzakelijk zullen sector specifieke aspecten expliciet benoemd worden.

3.3 Status-quo OT herstelvermogen

In het voorgaande onderzoek naar herstelvermogen in IT infrastructuren[19] is een definitie van herstelvermogen geïntroduceerd. Hierop voortbouwend wordt OT herstelvermogen als volgt gedefinieerd:

OT herstelvermogen is de mate waarin een organisatie efficiënt en effectief in staat is om verstoord geraakte functionaliteit, die voorzien wordt door OT, weer beschikbaar te maken.

In dit onderzoek is OT herstelvermogen onderverdeeld in de volgende aspecten:

1. Voorbereiden op herstel
2. Herstel-in-uitvoering
3. Leren van uitvoering
4. Overige aspecten

Voordat deze aspecten worden besproken zal er eerst worden ingegaan op de drijfveren voor een goede inrichting van herstelvermogen.

[18] https://www.nctv.nl/documenten/publicaties/2021/02/03/dreigingsbeeld-statelijke-actoren-3-februari-2021
[19] https://publications.tno.nl/publication/34638040/15Frgu/TNO-2020-R12064.pdf

3.3.1 Drijfveren voor herstel

De drijfveren voor, en de eisen die worden gesteld aan, herstelvermogen verschillen per sector. In de spoorwegensector wordt de norm ten aanzien van de maximale hersteltijd van een OT object in belangrijke mate bepaald door het verstorende effect dat het heeft op het regionale of landelijke dienstrooster. Terwijl in de chemiesector bij het normeren van incidenten - en daarmee gepaard gaande herstelmaatregelen - in belangrijke mate meeweegt of het kan leiden tot verspreiding van giftige stoffen in de omgeving.

Uit de interviews komt naar voren dat deze drijfveren voor herstel ingebakken zit in het DNA van de ondervraagde organisaties. Dit komt onder andere tot uiting in de *veiligheidscultuur* die zo kenmerkend is voor OT organisaties, zoals eerder besproken in sectie 3.1. Specifieke voorbeelden hiervan zijn *veiligheid* voor de samenleving, in de chemische sector. Ook komt dit tot uiting in de eisen die worden gesteld aan de *business continuity* van de geleverde dienst (e.g. in de water- en elektriciteitssector).

De *juridische kaders* waarin de organisaties bewegen komen in de interviews ook regelmatig naar voren als belangrijke drijfveer voor herstel. Uit de interviews komt tevens het beeld naar voren dat organisaties waarin het hoger management het belang van herstel erkent, hier vervolgens ook voldoende budgetten voor worden gealloceerd, wat weer ten gunste komt aan het herstelvermogen van de organisatie.

De mate waarin de drijfveren kunnen worden omgezet in implementatie is, naast het besef bij hoger management, ook voor een groot deel afhankelijk van de mate van eigenaarschap over de te beheren infrastructuur. De geïnterviewde organisaties van het spoorwegennetwerk en de elektriciteitsdistributie hebben de infrastructuur volledig in eigen beheer. Hierdoor kunnen deze organisaties in grote mate bepalen welke systemen gebruikt worden en welke maatregelen er getroffen moeten worden ten aanzien van herstelvermogen.

Een vergelijkbare, maar andere, situatie speelt bij een organisatie uit de watersector. Deze organisatie werkt veel met onderaannemers waardoor ze meer optreden als regievoerder. Effectief herstel is in deze laatste situatie sterk gestuurd via contractmanagement, waarin strakke eisen gesteld zijn aan de onderaannemers met betrekking tot cybersecurity en herstelvermogen.

Een partij uit de chemische industrie gaf aan zich in mindere mate in controle te voelen. Deze organisatie is voor het herstelvermogen van hun proces in grote mate afhankelijk van andere partijen, waarmee vergelijkbare contractuele verplichtingen niet bestaan. In deze situatie heeft de organisatie in mindere mate controle over de technische inrichting van de OT en het bijbehorende herstelvermogen.

3.3.2 Voorbereiden op herstel

De geïnterviewde OT organisaties geven allemaal aan de voorkeur te geven aan een *preventiebeleid,* i.e., voorkomen dat een systeem verstoord wordt. Er zijn verschillende maatstaven gehanteerd (e.g. six sigma) waaraan de organisatie moet voldoen. Hiertoe worden ook maatregelen geïmplementeerd, echter zijn niet alle maatregelen relevant omdat in dit onderzoek specifiek wordt gefocust op herstelvermogen. In de onderstaande paragrafen zullen de voorbereidende maatregelen, welke genoemd zijn tijdens de interviews, en bovendien direct relevant zijn voor herstel, worden besproken.

Eén van deze maatregelen is *redundantie*. In de interviews gaf een bedrijf uit de energiesector het voorbeeld dat er een 2-redundante infrastructuur wordt gehanteerd voor zowel OT als IT. Hierdoor bestaat er altijd een terugvalmogelijkheid indien een systeem verstoord raakt.

Bovendien geven alle geïnterviewde organisaties aan dat er protocollen klaarliggen voor het treffen van herstelmaatregelen. De mate waarin het *incident response plan* ook daadwerkelijk bijgehouden wordt als onderdeel van een *plan-do-check-act cyclus* verschilt per organisatie.

3.3.3 *Herstel-in-uitvoering*

Bij de geïnterviewde OT organisaties komen de aspecten bij herstel-in-uitvoering[20] in grote mate overeen met het opgehaalde beeld in IT infrastructuren. Dit wil zeggen dat voor de geïnterviewde OT organisaties geldt dat ze zelf aangeven de meeste activiteiten ten aanzien van herstel-in-uitvoering onder controle te hebben. De opvallende afwijkingen met betrekking tot herstelacties is tweeledig.

Ten eerste beperkt de fysieke wereld de snelheid van herstel als er op locatie acties uitgevoerd moeten worden. Ter illustratie, de uit te voeren acties kunnen een simpele inspectie zijn waarna het OT systeem na een incidentmelding weer vrijgegeven wordt. De acties kunnen ook neerkomen op het (voorzichtig) afbreken van de beschadigde infrastructuur, om deze daarna vanaf de fundering weer terug op te bouwen.

Ten tweede, herstel van een OT systeem komt in de praktijk vaak neer op gedeeltelijk herstel. Dit heeft te maken met het decentrale karakter van OT systemen. Lokale kleine incidenten worden beschouwd als *business-as-usual* en de organisaties zijn goed in staat om hiermee om te gaan. Grotere, lokale, incidenten komen niet vaak voor, echter wanneer deze desondanks optreden wordt de gehele crisismanagement keten opgestart, al dan niet op basis van het draaiboek. De geïnterviewde organisaties lijken echter nauwelijks, tot geen, ervaring te hebben met herstel na een grootschalige verstoring van de gehele eigen infrastructuur, noch na een grootschalige organisatie-overstijgende verstoring.

3.3.4 *Leren van uitvoering*

Alle geïnterviewde OT organisaties geven aan dat *leren van uitvoering* zeer belangrijk is, wat overeenkomt bij het opgehaalde beeld bij het onderzoek naar herstelvermogen bij IT organisaties. Alle organisaties geven aan incidenten achteraf te evalueren en eventueel technische of organisatorische maatregelen te treffen. Een organisatie uit de chemische sector geeft aan evaluatie als ‘absoluut noodzakelijk’ te zien.

Ook het delen van ervaringen op conceptueel niveau binnen een Information *Sharing and Analysis Center* (ISAC)[21] wordt als waardevol gezien. Echter, onder andere door de heterogeniteit van OT systemen is de ruimte voor collectief[22] leervermogen tussen verschillende organisaties beperkter dan voor meer algemeen gebruikte IT systemen.

3.3.5 *Overige aspecten*

Overige aspecten omvatten het uitvoeren van *oefeningen & opleiding van personeel*, *afstemming met ketenpartners*, en *collectief herstelvermogen*.

---

[20] Met herstel-in-uitvoering wordt bedoeld de manier waarop herstelwerkzaamheden worden uitgevoerd, zodra er een incident is opgetreden (zie ook de eerste opsomming in sectie 2).
[21] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/start-een-isac
[22] Collectief refereert hier aan de mate waarin organisaties gezamenlijk optrekken richting herstel.

In het onderzoek naar IT herstelvermogen zagen we dat er vaak wel, in meer of mindere mate, geoefend wordt met herstellen na incidenten, maar dat risicovolle oefeningen niet of nauwelijks worden uitgevoerd (bijvoorbeeld het uitschakelen van de stroomvoorziening in een datacenter om te oefenen met *fail-over* naar een ander datacenter). Ook worden grootschalige, collectieve IT oefeningen weinig uitgevoerd. Ten aanzien van OT herstelvermogen zien we hetzelfde. Er wordt aangegeven dat de meeste voorkomende herstelsituaties veel geoefend worden, maar ook hier worden oefeningen die een risico vormen voor de veiligheid of procescontinuïteit vermeden. Wel wordt in sommige interviews aangegeven dat er mogelijkheden komen om simulaties in de live omgeving uit te voeren[23], maar deze worden al snel als 'te duur' gezien. Collectieve OT crisisoefeningen (vooral gericht op de veiligheid) worden uitgevoerd door partijen die regelmatig gezamenlijk herstelwerkzaamheden uitvoeren. Een voorbeeld hiervan zijn oefeningen door de brandweer en alle fabrieken gevestigd op een chemisch industriecomplex.

Samenwerking tussen directe betrokkenen rond OT in een vitaal proces beperkt zich niet tot oefeningen. Bijvoorbeeld, in één van de interviews met een organisatie die veel gebruikmaakt van onderaannemers is aangegeven dat samenwerking ook wordt ingeregeld via contractmanagement. Deze organisatie heeft een doorvertaling gemaakt van OT (preventie- en) hersteleisen voor het proces naar de te stellen eisen aan de producten en diensten van vele (regionale) onderaannemers. Hiertoe heeft deze organisatie OT 'bouwblokken' gestandaardiseerd. In het kader van de verwachte afnemende heterogeniteit, toegenomen koppeling en uitbesteedbaarheid biedt deze aanpak een middel om controle te behouden. Ook ten aanzien van cybersecurity worden hierbij specifieke afspraken gemaakt.

De genoemde voorbeelden van collaboratieve oefeningen en OT herstelvermogen beperken zich wel tot directe betrokkenen bij een bedrijfsproces. Bijvoorbeeld, tussen OT operator en hun leveranciers, of tussen operators die gezamenlijk gebruik maken van gedeelde (transport)faciliteiten. Dergelijk collaboratief herstelvermogen is effectief voor incidenten die hersteld kunnen worden door directe betrokkenen. Voor grootschaliger incidenten kan herstelcoördinatie nodig zijn tussen meer partijen. Een voorbeeld betreft het herstellen van elektriciteitsdistributie na een grootschalige storing. Zodra de verstoring verholpen is, is coördinatie nodig tussen distributienetwerken en hun afnemers. Dit om te voorkomen dat het opschakelen van de distributie weer direct leidt tot onbalans in het stroomnetwerk. Voor dergelijke herstelcoördinatie bestaan er momenteel geen plannen of concrete afspraken en de coördinatie zal improvisatie vergen als zo'n incident optreedt. Uit de interviews volgt dat de grens van collaboratief herstelvermogen ligt tussen de directe procesbetrokkenen en de overige groep van indirecte procesbetrokkenen, waaronder de afnemers van hun diensten en producten.

[23] In OT omgevingen bestaat het concept van separate Ontwikkel-, Test-, Acceptatie- en Productie omgevingen niet zoals dat voor IT gebruikelijk is, maar door toenemende toepassing van digital twinning neemt de train- en testbaarheid van OT wel toe.

4 Effect digitalisering op OT herstelvermogen

In sectie 4.1 zal worden ingegaan op de trend van IT/OT convergentie, en in sectie 4.2 op de invloed ervan op herstelvermogen. Afsluitend wordt in sectie 4.3 aangegeven welke herstelmaatregelen in de praktijk getroffen worden ten aanzien van gedigitaliseerde OT infrastructuren.

4.1 IT / OT convergentie

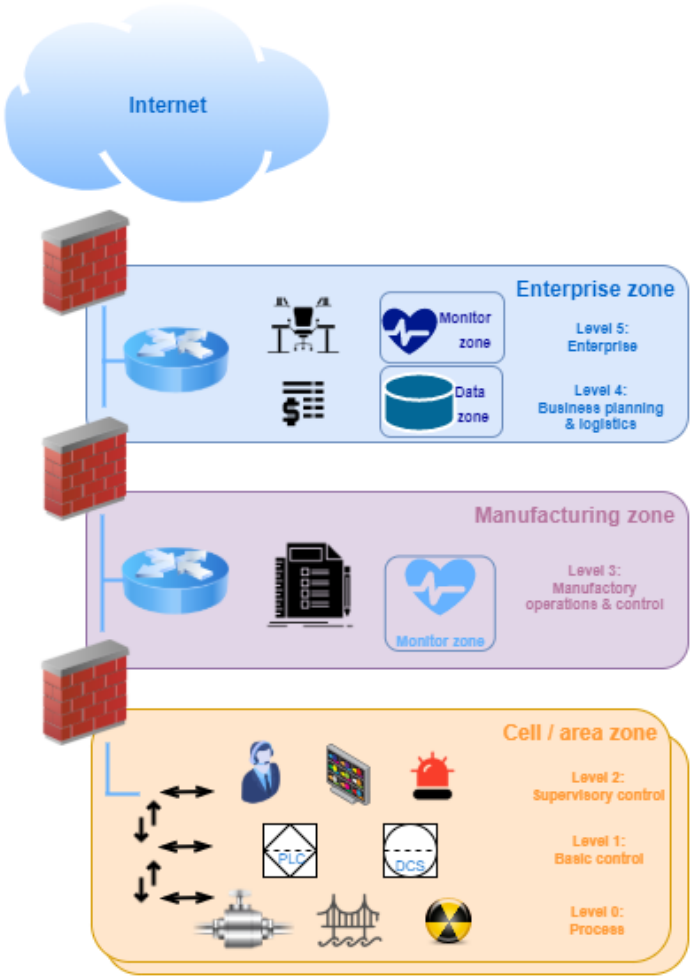
De oorspronkelijke reden voor de toepassing van OT is voornamelijk gericht op automatisering van (vitale) fysieke processen, ten behoeve van procesoptimalisatie en beheerefficiëntie. In eerste instantie heeft dit geresulteerd in de introductie van lokale gedistribueerde systemen voor de beheersing van fysieke processen; de OT technologie in laag 0, 1 en 2 van de Purdue Enterprise Reference Architecture (zie Figuur 2). Voor de communicatie tussen deze lokale systemen zoals PLCs, RTUs, en SCADA werden specifieke (en vaak proprietary) protocollen gebruikt, zoals Fieldbus, Modbus en HART. Met de opkomst van internet werd de mogelijkheid gecreëerd om lokale OT systemen in toenemende mate op afstand te monitoren en besturen via centrale systemen (laag 2 en 3 in Figuur 2). Ook biedt de vervanging van specifieke communicatieprotocollen door gestandaardiseerde internet protocollen, zoals Ethernet en IP, de mogelijkheid tot verbeterde beheerefficiëntie. Deze verbetermogelijkheid wordt soms expliciet gewenst vanuit OT dienstverleners, maar er treedt ook technologie-push op waarbij nieuwe OT systemen standaard van internetcommunicatie worden voorzien.

De toenemende invoering van communicatiestandaarden levert naast efficiënt beheer nog meer optimalisatiemogelijkheden op die leiden tot een verdere verknoping van OT netwerken en IT netwerken. Het beschikbaar maken van data uit het operationele proces voor nadere analyse, biedt de mogelijkheid om het proces en de logistiek er omheen verder te optimaliseren. Voor deze data analytics[24] moet de data wel beschikbaar gemaakt worden in de ‘enterprise zone’ (laag 4 in Figuur 2). Het gevolg is dat er datatransport (gecontroleerde) koppelingen ontstaan tussen al de lagen van het Purdue model. Door deze ontwikkelingen ontstaat er een toenemende verknoping tussen IT en OT: IT/OT convergentie.

In alle vitale processen zijn specifieke voorbeelden van IT/OT convergentie te zien. Bijvoorbeeld, in elektriciteitsdistributienetwerken wordt gebruik gemaakt van ‘IT voor OT’ systemen, zoals Energy Management System[25] (EMS) en (Advanced) Distribution Management System[26] (ADMS), voor het besturen van de opwekking en distributie van elektrische energie. In spoorwegbesturing is European Rail Traffic Management System (ERTMS) in opkomst, waarmee efficiëntere spoorbenutting wordt beoogd door toepassing van IT in treinen.

[24] Mede aangejaagd door de ontwikkeling en steeds bredere toepassing van Big Data technieken.
[25] https://en.wikipedia.org/wiki/Energy_management_system
[26] https://en.wikipedia.org/wiki/Distribution_management_system

Naast IT/OT convergentie ten behoeve van besturing van OT is er in sommige sectoren ook een toenemende behoefte aan (her)programmeerbare OT. OT systemen worden vaak ontworpen voor specifieke taken die gedurende meerdere decennia ongewijzigd kunnen worden uitgevoerd, zoals het ophalen van bruggen en het transporteren van vloeistof vanuit opslagtanks door pijpleidingen. Dit is echter niet voor alle OT systemen het geval, omdat er in de loop der tijd sprake kan zijn van veranderende functionele eisen. Een voorbeeld is de trend om industriële radarsystemen herconfigureerbaar te maken, zodat de surveillancefunctie ervan aangepast kan worden. Het komt daarom steeds vaker voor dat radarsystemen voorzien zijn van een embedded Linux systeem dat draait op FPGA (*Field Programmable Gate Array*) hardware. Dus niet alleen voor besturing op afstand vindt er IT/OT convergentie plaats, maar ook wordt er steeds meer ‘commodity IT’ gebruikt in OT systemen op laag 0, 1 en 2 van het Purdue model.



Figuur 2: Een vereenvoudigde weergave van het veelgebruikte Purdue Enterprise Reference Architecture model, welke de koppeling van OT en IT netwerken weergeeft.

De IT/OT convergentie vergt aandacht om tot een weerbare inrichting te komen. De inzichten om tot een veilige inrichting van geconvergeerde IT en OT te komen met een adequaat herstelvermogen zijn beschikbaar. Good-practices zoals inrichting volgens het Purdue model en afscherming van relatief oude OT conform zoals beschreven in IEC 62443 zijn in de praktijk gebruikelijk. Echter, in de praktijk worden deze good-practices nog niet door alle partijen toegepast, of niet consequent genoeg. Vooral ten aanzien van de invoering van industrial IoT, merken partijen op dat de implementatie ervan te snel gaat en men onvoldoende oog heeft voor onnodige blootstelling naar het internet.

In de interviews wordt aangegeven dat OT naar verwachting een vergelijkbare ontwikkeling door gaat maken als IT in de afgelopen 10 jaar. Er wordt verdere standaardisatie verwacht, waardoor de heterogeniteit afneemt, de systeemkoppelingen toenemen en er meer uitbesteding verwacht wordt. Dit is een belangrijke ontwikkeling om de weerbaarheid en het herstelvermogen van IT/OT convergentie op het juiste niveau te brengen voor alle organisaties in de doelgroep van het NCSC.

4.2 Noodzaak OT herstelvermogen door IT/OT convergentie

Vanwege de behoedzame cultuur in het OT domein, verloopt IT/OT convergentie zeer geleidelijk. Het toenemende IT gebruik kreeg meer en bredere aandacht (ook buiten de vitale sectoren) vanaf het moment dat de risico's ervan duidelijker werden. Cyberincidenten die de meeste aandacht trokken waren de Stuxnet aanval op Iraanse nucleaire centrifuges[27] in 2010 en de cyberaanval in de Oekraïne[28] in 2015 die de stroomvoorziening voor enkele uren verstoorde. Deze en andere gebeurtenissen leggen een aantal kwetsbaarheden bloot die zich door IT/OT convergentie in toenemende mate voordoen.

Ten eerste, introduceert IT besturing een centrale component in het systeem. Waar OT traditioneel werd toegepast volgens gedecentraliseerde principes (waardoor incidenten slechts lokale impact hebben die hersteld moet worden), vormt centrale IT besturing een risico op onbeschikbaarheid van een groot deel van, of zelfs de gehele, infrastructuur. Ook het uitvallen van netwerkconnectiviteit tussen centrale IT systemen en OT objecten kan een risico opleveren. Omdat er voor IT en OT heel andere uitgangspunten voor (langere termijn) betrouwbaarheid gehanteerd worden, wordt dit als een serieuze uitdaging ervaren door de ondervraagden.

Een risico dat is gerelateerd aan centrale besturing van OT, is de digitalisering van (slimme) OT systemen zelf. De digitalisering van OT opent meer mogelijkheden voor het geïnfecteerd raken met, en verspreiden van, malware. Hierdoor zullen OT systemen in toenemende mate gepatcht moeten worden en/of zullen de segmentatie en quarantainemaatregelen aangescherpt moeten worden. Hoewel dergelijke maatregelen voornamelijk preventief zijn, is het vanuit het perspectief van herstelvermogen van belang om te realiseren dat centrale, gedigitaliseerde OT een hoger risico hebben om in zijn geheel uit te vallen en/of het zicht op een proces te verliezen.

Ten tweede is de levenscyclus van OT trager dan die van IT, zoals ook besproken in sectie 3.1. Geïnterviewden geven aan dat IT besturingssystemen voor OT vaak zeer gedateerd zijn, omdat deze in de OT levenscyclus meegaan. Daarom komt bijvoorbeeld nog toepassing voor van niet meer ondersteunde software zoals Windows XP (embedded). Zolang de functie die het uitvoert niet verandert, is er geen reden voor vervanging, functioneel gezien[29]. Wel worden risico-gebaseerde maatregelen getroffen, zoals het beschikbaar houden van back-ups of van reserveonderdelen in geval van oude hardware. Bij deze risico's wordt echter voornamelijk gekeken naar uitval door technische oorzaak of door fouten tijdens onderhoudswerkzaamheden. Ondanks dat verouderde IT ook juist een verhoogd risico op cybersecurity incidenten met zich mee brengt, wordt hier in mindere mate rekening mee gehouden.

Beide kwetsbaarheden die IT/OT convergentie introduceert (potentiële verstoring van centrale, gedigitaliseerde besturing en verouderde IT) hebben invloed op OT herstelvermogen. De (preventie- en) herstelmaatregelen tegen deze nieuwe kwetsbaarheden zijn volgens de geïnterviewden in veel mindere mate ingericht dan de traditionele *business-as-usual* maatregelen ten aanzien van technische verstoringen.

[27] https://nl.wikipedia.org/wiki/Stuxnet
[28] https://www.wired.co.uk/article/ukrainian-power-station-cyber-attack
[29] In sommige gevallen treedt echter ook een noodgedwongen vervanging van een ouder OT systeem op, wat een continuïteitsrisico introduceert. Bijvoorbeeld in het geval een systeem wordt vervangen dat interacteert met het verouderde OT systeem, maar dat het nieuwe systeem niet interoperabel blijkt te zijn.

Hoewel deze constatering door alle geïnterviewden wordt bevestigd, is de *urgentie* om aanvullende herstelmaatregelen te treffen onduidelijk. Een aantal observaties dragen bij aan de onduidelijkheid over de urgentie voor aanvullende maatregelen:

- Daadwerkelijke uitval van een vitaal proces door verstoring van centrale IT besturing of verouderde IT heeft zich nog niet voorgedaan bij geïnterviewde organisaties. Hun waakzaamheid komt voornamelijk van incidenten bij buitenlandse sectorgenoten.
- Hoewel enkele organisaties melden dat zij bijvoorbeeld wel te maken hebben met cyberincidenten is geen van de partijen nog slachtoffer geweest van een grootschalige, geavanceerde aanval.
- Bovenstaande punten beïnvloeden niet alleen de inschatting van de kans op grootschalige verstoring van vitale processen, maar ook blijft vooralsnog de maximale impact van een verstoring onduidelijk. Blijven OT verstoringen niet beperkt tot lokale impact ondanks de toename van IT/OT convergentie? Hoeveel schade kan er *worst-case* aangericht worden door een geavanceerde aanval?
- Ook wordt aangegeven dat op cybersecurity van IT/OT weinig sturing wordt ervaren vanuit regelgeving. De Europese NIS directive[30] wordt in veel interviews wel genoemd, maar deze is van toepassing op cybersecurity en wordt niet altijd geïnterpreteerd als zijnde van toepassing op IT besturing van OT. Door een organisatie die dit wel als meldplicht ervaart, wordt bovendien de vraag gesteld hoe ernstig een incident moet zijn om het te melden: “een organisatie doet dit liever niet”.
- Ook het toezicht hierop wordt in Europese landen verschillend ingericht. Een specifieke vraag vanuit de elektriciteitsdistributie sector is bijvoorbeeld waarom er geen verplichting is om cybersecurity audits uit te laten voeren, zoals dit in Duitsland het geval is. Een andere organisatie geeft aan dat er wel een meldplicht is vanuit bijvoorbeeld AVG en milieu wetgeving, maar niet voor het melden van cyberincidenten in de (IT/)OT omgeving.

4.3 Herstelmaatregelen voor gedigitaliseerde OT

Hoewel ze weinig sturing op de te treffen (preventie- en) herstelmaatregelen voor gedigitaliseerde OT wordt ervaren, ontwikkelen organisaties in de vitale sectoren hun eigen maatregelen. Veel maatregelen zijn gericht op het voorkomen van verstoringen en het mitigeren van eventuele gevolgen, en niet per se gericht op cybersecurity incidenten. In alle interviews genoemde gangbare, generieke herstelmaatregelen (dus exclusief preventiemaatregelen zoals *system hardening*) zijn:

- Bewaking middels een operational control center (of meldkamer);
- Beschikbaar zijn, en oefening van een OT incident recovery plan; en
- Back-up & recovery van benodigde digitale gegevens over OT objecten (en in enkele gevallen ook andere maatregelen om aan de hoge beschikbaarheidseisen van relevante (besturing)systemen te voldoen).

[30] https://digital-strategy.ec.europa.eu/en/policies/nis-directive

Over de inrichting van deze maatregelen geven de geïnterviewden aan dat het redelijk goed gesteld lijkt te zijn. De precieze stand van zaken valt echter lastig vast te stellen, omdat er geen harde toetsingsgegevens (bijvoorbeeld vanuit verplichte audits) beschikbaar zijn. Voor de eisen aan, en inrichting van, herstelmaatregelen wordt vaak verwezen naar industrie standaarden waaronder de IT security georiënteerde standaarden serie IEC 62443 (Cyber Security for Industrial Automation and Control Systems)[31] en IEC 62351. Eén van de geïnterviewden noemt ook de laagdrempelige security check voor proces automatisering gepubliceerd door het DTC[32], die is opgesteld door een consortium met daarin ook NCSC.

Rode knop voor IT/OT scheiding

Zoals in sectie 3.1 aangegeven is implementatie van OT vrij nauw verbonden met het vitale proces waarvoor de OT wordt ingezet. Afgezien van de hierboven genoemde generieke maatregelen is tijdens de interviews een specifieke maatregel genoemd, die conceptueel wel breder toepasbaar is. Deze specifieke maatregel betreft een elektriciteitsdistributeur die een "*rode knop voor IT/OT scheiding*" heeft ontwikkeld. Met deze mitigerende maatregel zou distributie van elektriciteit operationeel kunnen blijven, als besturing- of bewakingsfuncties op hoger niveau (bijvoorbeeld in de manufacturing of enterprise zone in het Purdue model van Figuur 2) uitvalt[33]. Tijdens dit onderzoek hebben meerdere organisaties aangegeven dat een dergelijke maatregel als good-practice beschouwd wordt. Het is duidelijk dat een dergelijke "rode knop" alleen toegevoegde waarde biedt voor een processysteem (in dit geval een elektriciteitsnetwerk) dat in hoge mate autonoom kan en mag functioneren. Ook is de maatregel niet onder alle omstandigheden van toepassing; de maatregel is vooral gericht op het voorkomen van moedwillige vervolgschade aan de OT via de IT besturing en is alleen effectief als deze tijdig wordt uitgevoerd. Toch is een dergelijke mitigerende *rode knop maatregel* interessant en zien we een parallel met de Internet *kill-switch* maatregel die in de voorgaande studie naar IT herstelvermogen genoemd werd.

Operational control center en het Security Operation Center

Ten aanzien van herstelvermogen in geval van cyberincidenten is in sommige interviews de relatie tussen het operational control center (OCC) en het security operation center (SOC) aan de orde gekomen. In sommige organisaties zijn dit nog twee afzonderlijke centra binnen de organisatie en/of is de transitie om IT en OT security in overeenstemming met elkaar te brengen nog in gang. Het OCC is ingericht voor procesbesturing, en valt typisch onder de verantwoordelijkheid van de management eenheid daarvoor (zoals asset management). Het SOC is cybersecurity georiënteerd en valt meestal onder verantwoordelijkheid van de IT eenheid. In Figuur 2 zou het OCC typisch worden geplaatst in laag 3, terwijl het SOC vooral nog gezien wordt in de enterprise zone in laag 4 / 5. Het gevolg is dat het OCC en het SOC in de praktijk naast elkaar staande operations centers kunnen zijn.

[31] https://en.wikipedia.org/wiki/IEC_62443
[32] https://www.digitaltrustcenter.nl/tools/doe-de-security-check-procesautomatisering
[33] In Figuur 2 zou deze rode knop bijvoorbeeld geïmplementeerd kunnen worden via de (firewall) koppeling tussen de manufacturing zone en de cell/area zone.

OT en digitale soevereiniteit

Tijdens sommige interviews zijn er opmerkingen gemaakt over OT in relatie tot digitale soevereiniteit. Hoewel dit onderwerp niet direct gerelateerd is aan OT herstelvermogen, wordt aangegeven dat de afhankelijkheid van een beperkt aantal buitenlandse OT leveranciers een risico vormt voor de beschikbaarheid en leveringszekerheid van vitale infrastructuur (en daarmee de nationale veiligheid). Dit resulteert erin dat vitale infrastructuuraanbieders met OT in beheer, overwegen om hun positie ten aanzien van digitale soevereiniteit te herzien en te verbeteren. In dat kader is de verwachting dat de behoefte aan OT van ‘eigen bodem’, en bijbehorende herstelmiddelen, in de toekomst zal toenemen.

5 Conclusie en toekomstig onderzoek

In dit hoofdstuk worden de algemene conclusies beschreven. Deze conclusies zijn gebaseerd op alle onderzoeksactiviteiten zoals beschreven in hoofdstuk 2, inclusief de afgenomen interviews en de review door experts vanuit de IACS expert board. Hiertoe zullen de onderzoeksvragen worden beantwoord in sectie 5.1. Afsluitend zullen de mogelijkheden voor toekomstig onderzoek en vervolgstappen worden behandelt in sectie 5.2.

5.1 Onderzoeksvragen

Welke aspecten zijn er van belang om herstelvermogen in te richten voor OT infrastructuren bij de doelgroepen van het NCSC?
De aspecten die relevant zijn voor de inrichting van herstelvermogen voor OT infrastructuren zijn sterk vergelijkbaar met de geïdentificeerde aspecten voor IT herstelvermogen uit een eerder onderzoek[34]. De relevante aspecten zijn onder te verdelen in: 1) voorbereiden op herstel , 2) herstel-in-uitvoering, 3) leren van uitvoering en 4) overige aspecten (met name: oefeningen, afstemming met ketenpartners en collectief herstelvermogen).

Een belangrijk aandachtspunt voor OT herstelvermogen is het effect van IT/OT convergentie. Deze convergentie vergroot het risico op cybersecurity incidenten en het vergroot ook de potentiële impact van incidenten omdat grotere delen van, of zelfs de gehele, infrastructuur kan uitvallen. Hoewel deze constatering door alle geraadpleegde experts wordt bevestigd, is de urgentie om aanvullende herstelmaatregelen te treffen onduidelijk.

Wat is er anders ten opzichte van de situatie bij IT infrastructuren?
Relevante verschillen voor OT ten opzichte van IT komen voort uit een samenspel van technische eigenschappen, organisatie culturele omstandigheden en sectorale kenmerken.

- Technische OT eigenschappen (die verschillen van IT en) die invloed hebben op herstelvermogen zijn (a) een sterke koppeling tussen de gebruikte systemen en het onderliggende fysieke proces; (b) (geografisch) decentrale inrichting van OT systemen; en (c) een lange levensloop en gemiddeld hoge leeftijd van de gebruikte systemen.
- Het verschil in IT en OT organisatiecultuur bestaat uit de sterkere nadruk op de veiligheidscultuur in de OT. Deze cultuur zorgt ervoor dat safety zeer prominent wordt meegenomen in herstelvermogen eisen en afwegingen (safety-first). In tegenstelling tot in de IT, waar eisen voor herstelvermogen sterker gericht zijn op confidentiality, integrity, en availability.
- OT doelgroep organisaties van het NCSC acteren in een verscheidenheid aan sectoren en toepassingsdomeinen, waarin er sectorale verschillen bestaan ten aanzien van bijvoorbeeld de marktinrichting, het innovatietempo van infrastructuur en IT/OT en karakteristieken van het primaire proces (bijvoorbeeld incidenteel of continue van aard). Vanwege de sterke koppeling tussen OT en het fysieke proces hebben deze verschillen meer invloed op de toepassing van OT dan die van IT.

De heterogeniteit van de toepassing van OT komt tot uiting in een aantal facetten van OT herstelvermogen:

[34] Publicatie, zie ook voetnoot 1 en 8.

- De eisen aan OT herstelvermogen verschillen per (vitale) sector en de regelgeving en het toezicht is sectorspecifiek[35], waarbij ook van belang is of een sector vitaal is of niet.
- De getroffen herstelmaatregelen zijn veelal specifiek op proces, omdat de fysieke processen dicteren welke maatregelen mogelijk zijn. Ook zijn, vanwege de verbondenheid met de fysieke wereld, de hersteltijden typisch langer in de OT dan men gewend is in de IT.
- De mate van IT/OT convergentie verschilt per sector en daarmee verschilt ook de relevantie van cybersecurity, in die zin dat een hoge mate van IT/OT convergentie de implementatie van adequate cybersecurity maatregelen nog belangrijker en urgenter maakt. Echter, wanneer er geen sprake is van IT/OT convergentie, betekent dat niet dat er geen cybersecurity risico's aan de orde kunnen zijn.

Wat is de stand van zaken op het gebied van herstelvermogen bij OT doelgroep organisaties?

Uit interviews blijkt dat organisaties naar hun beste inzicht hun eigen verantwoordelijkheid nemen ten aanzien van herstelvermogen, en ze geven aan vertrouwen te hebben in hun herstelvermogen.

Een meer concrete bepaling van de stand van zaken ten aanzien van het OT herstelvermogen is nauwelijks mogelijk. Daarin spelen de sector verschillen tussen de OT toepassingen een voorname rol. Ook is volgens meerdere organisaties de regelgeving over herstelvermogen daarvoor niet specifiek genoeg is en het toezicht te vrijblijvend ingericht, in vergelijking met andere Europese landen. Hierdoor ontbreken concrete gegevens over OT herstelvermogen (bijvoorbeeld objectieve auditresultaten over aanwezigheid en effectiviteit van specifieke maatregelen), waardoor de status ten aanzien van OT herstelvermogen niet scherper kan worden vastgesteld dan via expertinschattingen.

Wel zijn er twee specifieke aandachtspunten voor OT herstelvermogen vastgesteld. Ten eerste, in de context van IT/OT convergentie is er op vlak van cybersecurity nog de meeste twijfel of (het tempo van) de door organisaties getroffen maatregelen voldoende zijn. Daarnaast is er twijfel over het vermogen om te herstellen na een grootschalig incident die meerdere sectoren raakt. Hier is nauwelijks ervaring mee in Nederland en er zijn weinig concrete cross-sectorale afspraken over herstelmaatregelen of oefeningen daarvan.

5.2 Toekomstig onderzoek en vervolgstappen

De interviews met domeinexperts en OT infrastructuur beheerders verschaffen eerste kwalitatieve inzichten. Een kwantitatieve analyse van risico's ten aanzien van IT/OT convergentie en verouderde IT zou de urgentie om hiervoor aanvullende herstelmaatregelen te treffen kunnen verduidelijken. De basis hiervoor zou in een (eventueel te ontwikkelen) self-assessment kunnen liggen, bijvoorbeeld met een doorontwikkeling van het self-assessment ontwikkeld in 2021[36], en toepasbaar te maken voor partijen met OT infrastructuren.

[35] Tot op zekere hoogte geldt dit ook voor IT. Echter, voor IT zien we dat sommige regelgeving, zoals AVG, generiek van toepassing zijn en dat regelgeving in verschillende sectoren vaak gebaseerd is op generieke informatiebeveiligingsstandaarden.

[36] Zoals in de leeswijzer is uitgelegd zijn er aanverwante resultaten welke al zijn opgeleverd, of nog moeten worden opgeleverd. Hieronder valt ook het self-assessment waar we hier aan refereren. Dit is een onderzoeksresultaat welke naar alle waarschijnlijk in 2022 door het NCSC in gebruik zal worden genomen.

Op basis van dit onderzoek is aan te bevelen om duidelijke en uniforme kaders te stellen over het herstelvermogen van vitale OT infrastructuren en effectief toezicht daarop. Dit behelst ook het delen van meer informatie en cross-sectorale afstemming ten aanzien van herstelvermogen. Specifiek is er behoefte aan meer duidelijkheid over:

1. de verwachtingen richting vitale OT infrastructuur aanbieders ten aanzien van normen voor herstel van hun operationele processen;
2. de (periodieke) toetsing van de toepassing van deze normen;
3. aanscherping van de NIS directive door de scope duidelijker te verbreden van IT naar IT en OT; en
4. een richtlijn voor organisaties over een geschikte wijze van samenwerking tussen en/of integratie van OCC en SOC.

Uit het onderzoek blijkt dat er ten aanzien van OT herstelvermogen een rol voor het NCSC voorzien wordt. Een verdere inventarisatie van de behoefte van doelgroep organisaties zou een grondslag kunnen bieden voor de positionering van het NCSC.

6 Appendices

6.1 Interview vragenlijst template

Introductie en structuur van interview
Definitie: *OT herstelvermogen is de mate waarin een organisatie efficiënt en effectief in staat is om verstoord geraakte functionaliteit, die voorzien wordt door OT, weer beschikbaar te maken.*

Definitie incident / calamiteit / disaster @uit ITU standaard?

Introductie geïnterviewde

Introductie organisatie en sector

Wie zijn de voornaamste spelers?

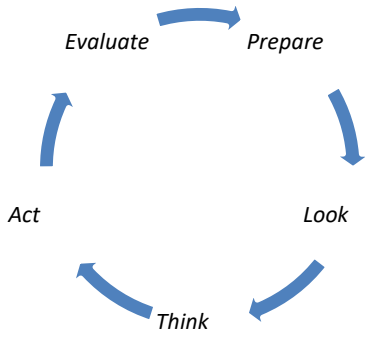
Welke OT wordt gebruikt?

Wat is belang van OT beschikbaarheid en herstelvermogen?

Wat voor incidentcategorieën worden er gebruikt? Hoe worden incidenten geïnterpreteerd in de sector?

We voeren graag de discussie over hoe de organisatie omgaat met het inrichten van maatregelen om na een verstoring, uitval of misbruik van de OT en daarop gebaseerde processen zo efficiënt en effectief mogelijk te kunnen herstellen. Hierbij zijn we geïnteresseerd in zowel in de technische, procesmatige als de menselijke aspecten van deze maatregelen.

We zullen vragen stellen aan de hand van de volgende fases in herstelvermogen:



Fase 1 - *PREPARE*:
Wat zijn de voorbereidende activiteiten die jullie hebben getroffen met het oog op toekomstig herstel na een incident?

Op wat voor soort incidenten bereiden jullie jezelf voor? **Welke preventieve maatregelen worden typisch getroffen?** **Rekening houdend met een incident, is er een herstelplan opgesteld?** **Vanuit welke bedrijfsmatige drijfveren is het herstelplan opgesteld?** **(in hoeverre speelt regelgeving hierbij een rol?)**

Fase 2 – 4 – *LOOK THINK ACT*

Kunnen jullie ons door een incident heenlopen, vanaf de fase dat het incident opgemerkt wordt, door de beslissingen die genomen worden tot aan de uiteindelijke uitvoering.

Kunnen jullie aan de hand van voorbeelden uitleggen hoe doorgaans een incident wordt opgemerkt?

Hoe bepalen jullie de oorzaak van een incident?

Hoe bepalen jullie de impact van een incident?

Hoe bepalen jullie de te treffen herstelacties, en in hoeverre hangt dit af van het type incident?

Wie bepaalt wat de juiste herstelacties zijn?

Wat zijn de eisen/criteria die jullie meenemen bij het bepalen van de juiste herstelacties?

Hoe gaat de uitvoer van het herstelproces in de praktijk in zijn werk?

Wanneer gaan jullie over tot actie, en wie doet dat (vooral voor security incidenten interessant)?

Is er ruimte voor improvisatie en afwijking van het plan?
Kunnen jullie voorbeelden noemen?
Werken jullie hierin cyclisch?

Fase 5 – *EVALUATE*:

Hoe evalueren jullie incidenten, en kan je hier voorbeelden van noemen? **Wat doen jullie met de "lessons learned" uit evaluaties?** **Kunnen jullie voorbeelden noemen van implementatie van "lessons learned"?**

Overige onderwerpen – *EXERCISE & COLLECTIVE RECOVERY*:
Wordt er buiten de incidentafhandeling “in het echt” ook geoefend?

Daarnaast, hoe ziet het collectieve herstelproces eruit? Dat wil zeggen, herstel in de context van een complexe samenwerking met ketenpartijen?

Wordt het herstelproces geoefend? (Zowel voor een kleine als grote calamiteit)
Hoe werkt dit met risicovolle oefeningen?
Is er sprake van collectief herstel?
Welke partijen spelen een rol binnen collectief herstel?
Bij een incident in uw organisatie, hoe wordt er samengewerkt met ketenpartners?
Bij een incident bij een ketenpartner, hoe kan uw organisatie bijdragen aan herstelvermogen bij de partner?