

High Level risicoanalyse in vogelvlucht

www.securitydelta.nl/ipcs



Revisie

Datum	Naam	Revisie
14-11-2025	E. ten Bos	Voor final review
Feb 2026	Kwaliteitscommissie	Reviewed

1 Inleiding

1.1 Doel van het document

Dit document beoogt de lezer inzicht te geven in het belang van een high level Risk Assessment en geeft handvatten om deze op efficiënte wijze uit te kunnen voeren.

1.2 Doelgroep

De doelgroep voor dit document bestaat uit de personen binnen organisaties ('asset owners') waarin Operationele Technologie (OT) of Proces Automatiserings (PA) infrastructuur aanwezig is, en die verantwoordelijk zijn voor het managen van de cybersecurityrisico's verbonden aan die infrastructuur. Het is voornamelijk gericht op een bedrijfsgrootte welke past bij het MKB. In dit document wordt de afkorting OT gebruikt.

1.3 Inleiding

De IEC 62443 vereist dat een "Initial cyber security risk assessment" (initiële cyberbeveiligings risicobeoordeling) wordt uitgevoerd. Bij het woord 'risico' in "Initial cyber security risk assessment" wordt meestal gedacht aan "Kans x Effect". In deze context wordt de kans op 1 gesteld aangezien deze beoordeling zich richt op het effect. Er wordt gekeken naar het effect dat een verstoring van een systeem of functie heeft op de bedrijfscontinuïteit, HSE en financiën. Dit wordt gedaan zonder inachtneming van al aanwezige mitigerende maatregelen.

Deze initiële beoordeling helpt bij het prioriteren van verdere (gedetailleerde) risicobeoordelingen. Daarbij wordt nadrukkelijk geadviseerd om eerdere veiligheidsbeoordelingen, dreigingsinformatie van overheden en sectorspecifieke groepen in overweging te nemen.

Structuur:

Om een high level risk assessment (HL-RA) uit te voeren beschrijft dit document de stappen en de context. Het begint met het uitvoeren van een (mini) Business Effect Analyse (BIA) waarin het effect wordt onderzocht van een falend digitaal geautomatiseerd systeem binnen OT. We noemen zo'n systeem het System under Consideration (SUC). De productielocatie of fabriek wordt in verschillende functionele blokken ingedeeld. Per blok dient te worden ingeschat wat het mogelijke effect is van een cybersecurity incident met als doel prioriteiten te achterhalen. Ook dient de onderlinge afhankelijkheid van de functionele blokken bepaald te worden. Met andere woorden de effecten van de verstoring van functionele blokken bepalen op de relevante bedrijfsdomeinen: bedrijfscontinuïteit, HSE en Financiën. Voor de doelgroep worden praktische handvatten aangereikt om dit proces uit te voeren. Enkele valkuilen worden benoemd en praktijkvoorbeelden zijn beschreven ter illustratie.

Dit proces maakt vaak gebruik van een risicomatrix als hulpmiddel om de geïdentificeerde risico's vast te leggen in relatie tot de waarschijnlijkheid en effect van een gebeurtenis. In een High-level risicoanalyse negeren we (zoals gezegd) de waarschijnlijkheid en concentreren we op de mogelijke (worst case) effecten. Hierbij worden bestaande, mitigerende maatregelen niet meegewogen, tenzij het een passieve maatregel betreft die onafhankelijk is van de geautomatiseerde systemen.

Bijvoorbeeld:

1. Een falend SUC kan leiden tot explosie in een ketel, met mogelijk meerdere doden tot gevolg.
2. Een passieve maatregel (afblaasventiel) voorkomt een explosie, en beperkt het effect tot een dag stilstand.
3. In de High-level risicoanalyse nemen we als worst-case effect één dag stilstand. (Dit is het "netto-effect" van een falend SUC.)

Het doel is namelijk om het effect te bepalen dat kan optreden door het falen van een digitaal systeem. Het opstellen van een complete risicomatrix behoort dus niet tot een HL-RA. Wel wordt (waar mogelijk) gebruik gemaakt van de effectschaal van een bestaande risicomatrix in de organisatie. Dan is namelijk meteen duidelijk wat het effect op de bedrijfsprocessen is.

Onderstaande tabel geeft een voorbeeld met verschillende effectschalen.

Onderwerp	Laag	Medium	Hoog	Crisis
Effect score	1	2	3	4
Financieel	< 2k EUR	>=2K EUR	>30K EUR	>100K EUR
Reputatie	Lokale media-aandacht	Regionale media-aandacht	Nationale media-aandacht	Internationale media-aandacht
Wet- & regelgeving	n.v.t.	Waarschuwing	Boete	Productie vergunning komt in gevaar
Veiligheid mensen	EHBO, geen absentie noodzakelijk	Beperking op uitvoeren van werk. Korte termijn absentie	Lange termijn absentie door ongeluk	Doden
Operatie	Productie verstoring of vertraging korter dan 3 uur	Langer dan 12 uur productieverstoring	Langer dan 24 uur productie-verstoring of stilstand	Geen concreet zicht op productie herstel
Milieu	Geen	Waarschuwing	Boete	Productievergunning komt in gevaar

De geïdentificeerde scenario's worden in onderstaande tabel nader omschreven. Onderstaande tabel is een voorbeeld met per categorie een voorbeeld van geïdentificeerd scenario.

Scenario	Proces onderdeel	Omschrijving
Crisis	Ketelhuis	Explosie door falend SUC, veroorzaakt door een setpoint aanpassing door onbevoegden.
Hoog	Warehouse	Door falend functioneel blok ernstige schade aan productie-eenheid. Fysiek herstel noodzakelijk van digitale of fysieke onderdelen. Hulp van specialisten moet ingeroepen worden op locatie.

Medium	Enkele palletizer	Door falend functioneel blok lichte schade aan productie-eenheid welke op de werkvloer hersteld kan worden. Ondersteuning van specialisten op afstand noodzakelijk.
Laag	Vul machine	Door falend functioneel blok productie stop of vertraging waar geen fysieke reparatie voor noodzakelijk is. Herstel is mogelijk door eigen personeel op locatie.

Door deze methode te volgen identificeren we welk systeem kan leiden tot incidenten met hoge effect.

2 Uitvoeren van een High-Level Risicoanalyse

2.1 Introductie

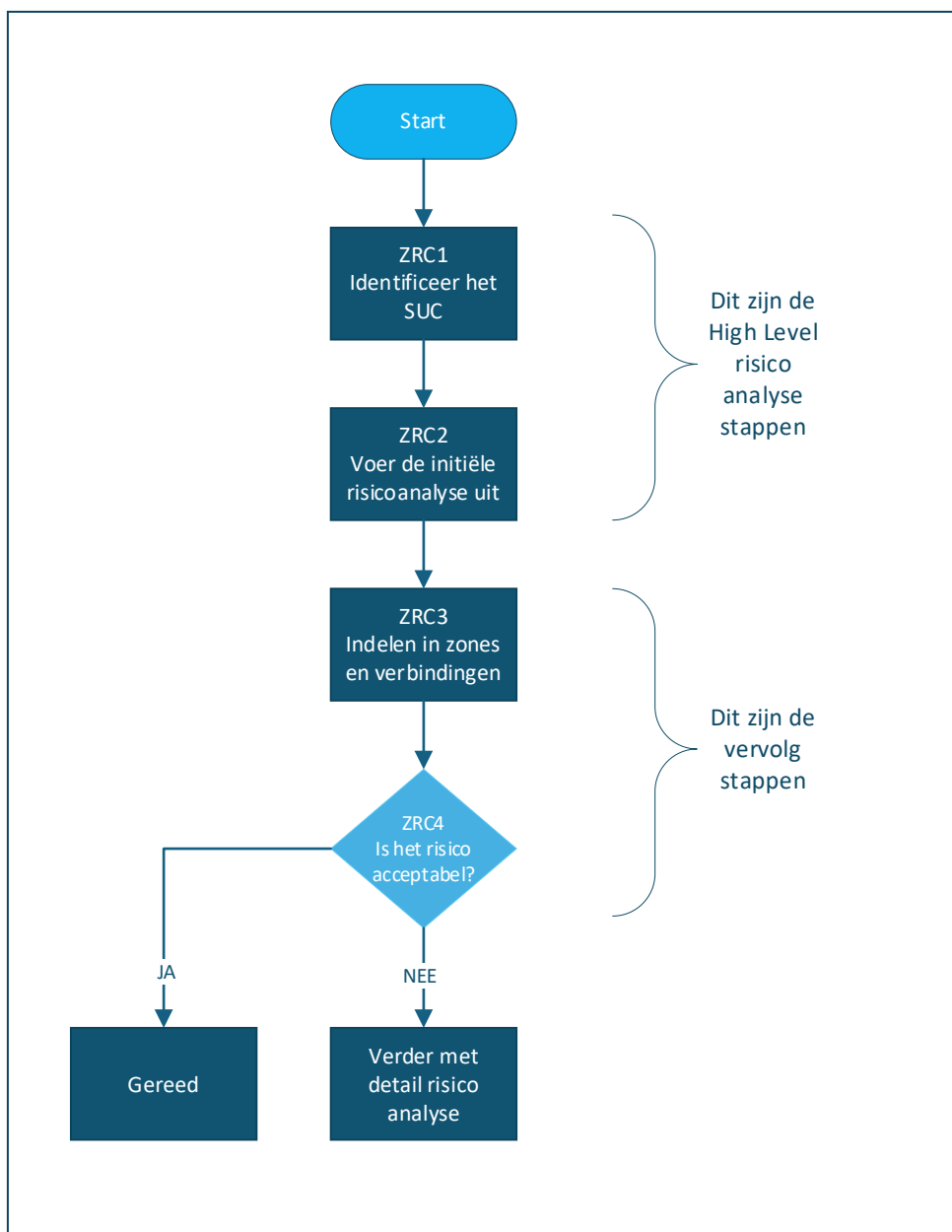
Met een High Level risk analysis wordt in beperkte tijd een eerste beeld gevormd van de belangrijkste cyberrisico's. Hierbij wordt de methode gehanteerd die is afgeleid van de IEC62443-3-2 standaard in vier stappen - ZCR1 tot en met ZCR4 - die zijn weergegeven in Figuur 1 en daarna worden uitgelegd. ZCR staat voor "Zones & Conduit Requirements". Deze twee begrippen hebben betrekking op het segmenteren van computernetwerken.

Een *Zone* is een groepering van systemen en netwerkcomponenten die:

- Functioneel, logisch of fysiek verwant zijn,
- Gelijke cybersecurity-eisen delen,
- Een gemeenschappelijk beveiligingsniveau nodig hebben.

Zones worden gebruikt om het netwerk te segmenteren en zo de risico's te beperken. Door assets met vergelijkbare beveiligingsbehoeften te groeperen, kunnen organisaties gerichte beveiligingsmaatregelen nemen en de complexiteit van hun beveiligingsarchitectuur verminderen.

Een *Conduit* is een logische of fysieke groepering van communicatiekanalen tussen twee of meer Zones. Deze delen ook gemeenschappelijke beveiligingseisen en zorgen voor gecontroleerde en beveiligde gegevensuitwisseling.



Figuur 1 High Level risico analyse in vier stappen

2.2 ZCR1: Identificeer het SuC (System under Consideration)

Om een High Level risicoanalyse te kunnen uitvoeren is het noodzakelijk de functionele blokken te kennen. Deze dienen daarom eerst bepaald te worden voordat in ZCR4 de feitelijke risicobeoordeling gedaan kan worden.

Door de onderstaande stappen te volgen, kan een fabriek zijn functionele blokken effectief bepalen. Deze functionele blokken worden in stap ZCR4 gebruikt worden om de risicobeoordeling m.b.t. versterking door cyberactiviteiten uit te voeren.

Iedere productielocatie of -eenheid kan onderverdeeld worden in verschillende productieprocessen (functionele blokken). En ook met betrekking tot cyberweerbaarheid en de risico-evaluatie van verstoringen door cyberactiviteiten. De stappen en overwegingen om dit proces te structureren zijn:

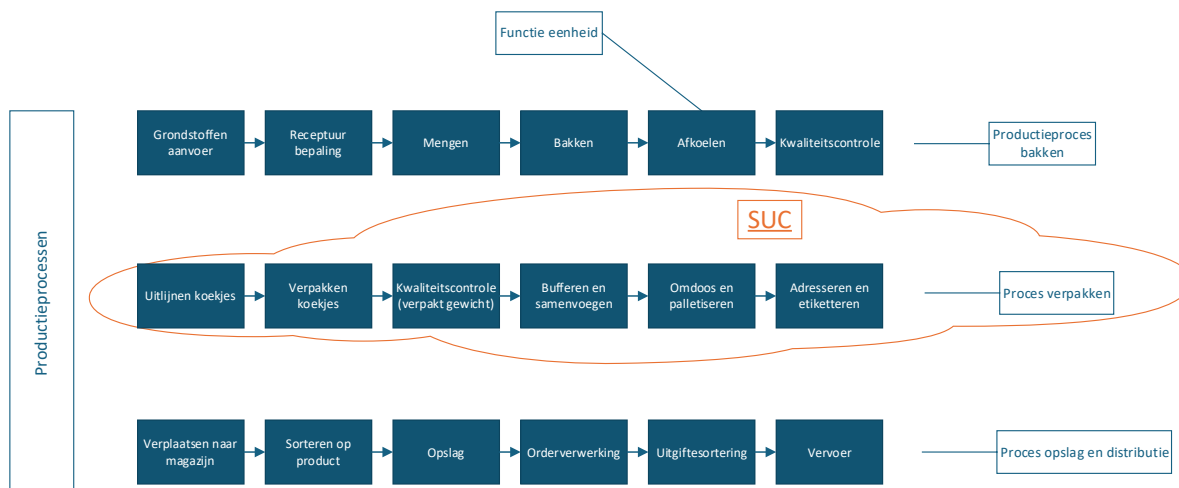
1. **Identificeer de productieprocessen:** Begin met het in kaart brengen van de verschillende productieprocessen die binnen de fabriek plaatsvinden, let er daarbij op dat de grenzen eenduidig zijn bepaald. Dit omvat het in kaart brengen van de productieprocessen in de vorm van een procesblokschema of plattegrond met omschrijving (voorbeeld gegeven in figuur 2). Gebruik hiervoor minimaal een geografische tekening met afbakening van de fysieke grenzen en een diagram met de functionele grenzen. Het gaat erom dat van de onderdelen die samen een functie vervullen kan worden bepaald wat de invloed is op de business bij een verstoring ten gevolge van een cyberincident. Bepaal de scope ook in relatie tot de grootte van het bedrijf en de afhankelijkheid van automatisering in de functionele onderdelen. Voorbeelden: grond- en hulpstoffenontvangst, productie, assemblage, verpakking en distributie & transportketen.
2. **Bepaal de benodigde productiefactoren:** Voor elk productieproces moet je vaststellen welke productiefactoren vereist zijn. Productiefactoren zijn bijvoorbeeld: machines, gebouwen, gereedschappen, infrastructuur, arbeid, natuurlijke hulpbronnen, grond- en hulpstoffen en energiebronnen.
3. **Analyseer de interacties:** Bepaal welke data & informatie wordt uitgewisseld tussen verschillende productiefactoren. Dit kan helpen bij het identificeren van bottlenecks of overlappings, en het optimaliseren van de communicatielijnen. De vraag die hier beantwoord wordt luidt: "Wat is de invloed op de bedrijfscontinuïteit als de datastroom of -integriteit wordt verstoord ten gevolge van een cyberincident?".
4. **Leg de indeling van de fabriek vast:** De fysieke indeling van de fabriek kan ook van invloed zijn op de productieprocessen. Overweeg een plattegrond die de efficiëntie maximaliseert, zoals een lijnopstelling of een cellulaire indeling, afhankelijk van het type productie.
5. **Inventariseer de gebruikte technologie:** stel een overzicht op van de gebruikte automatiseringstechnologie (computer- en netwerksystemen) in gebruik in de productieprocessen. De eerder beschreven productieprocessen kunnen gebruikmaken van diverse automatiseringssystemen. De automatiseringscomponenten die samen een volledige automatiseringsoplossing vormen worden gedefinieerd als een System under Consideration (SuC). Een SUC kan subsystemen bevatten. Voorbeelden van SUCs en subsystemen zijn:
 - Proces- en machinebesturingssystemen;
 - PLC/SCADA/DCS;
 - Manufacturing Execution Systems;
 - Manufacturing Operations Management Systems;
 - Laboratory Information Management Systems;
 - Data Historian;
 - Instrumentele veiligheidssystemen (SIS);
 - Fire & Gas systemen;
 - Gebouwautomatisering;
 - Communicatiesystemen;
 - Onderhoud Informatie Systeem.

Maak een overzicht van betrokken computer- en netwerksystemen in de scope en geef aan waar er interactie is met de buitenwereld. Geef een opsomming van de componenten in de scope en een inschatting van de wijze van automatisering. Stel de volgende vragen:

- Is er een besturingssysteem?
- Zijn systemen verbonden?

- Welke systemen functioneren min of meer onafhankelijk van elkaar? (Systemen met sterke onderlinge afhankelijkheid meenemen in scope.)

6. **Evaluatie en aanpassing:** Het is belangrijk om periodiek de productieprocessen te evalueren en aan te passen aan veranderingen.



Figuur 2: Een koekjesfabriek waarbij de verpakingsstraat is gekozen als SUC van de risico analyse.

2.3 ZCR2: Voer een initiële risicoanalyse uit

Risicobeoordeling is het totale proces van gevaar identificatie, risicoanalyse en risico-evaluatie. Risicobeoordeling geeft inzicht in risico's, de kwetsbaarheden, hoe kwetsbaarheden kunnen worden misbruikt (hun oorzaken), gevolgen en de waarschijnlijkheden. Dit maakt geïnformeerde keuzen mogelijk over:

- Of een activiteit ondernomen moet worden;
- Waarschijnlijkheid op misbruik van kwetsbaarheden minimaliseren
- Of risico's moeten worden gemitigeerd;
- Ondersteunt het kiezen tussen opties met verschillende risico's;
- Ondersteunt bij het prioriteren van risico mitigerende maatregelen;
- Ondersteunt het kiezen van de meest geschikte risicobehandlungsstrategieën die niet acceptabele risico's terugbrengt tot een aanvaardbaar niveau.

Volgens IEC 62443 moet er een eerste cyberbeveiligingsrisicobeoordeling worden gedaan. De Business Impact Analysis (BIA) is hiervoor een veel gebruikte methode. Het doel van een BIA is te bepalen wat de gevolgen zijn van een cyberincident voor vertrouwelijkheid, integriteit en beschikbaarheid van informatie. De snelheid van herstel is grote mate bepalend voor het effect op de bedrijfsvoering.

Bij het woord 'risico' wordt meestal gedacht aan "Kans x Effect". In de context van een BIA wordt de kans op 100% gesteld, aangezien de BIA-studie zich richt op het effect dat een verstoring van een (deel)systeem of functie heeft op de bedrijf continuïteit, HSE, financiën of andere voor het bedrijf relevante prestatie-indicatoren. De effectbeschrijving wordt opgesteld zonder inachtneming van aanwezigheid of mogelijke technische of organisatorische maatregelen.

Enkele belangrijke vragen bij een BIA-studie zijn:

- Wat zijn de belangrijkste continuïteitsrisico's voor uw organisatie?
- Wat is er nodig om uw organisatie nog beter te beschermen?
- Hoe belangrijk is business continuity management voor uw organisatie?

Met een BIA-studie wordt:

- Inzichtelijk gemaakt wat de meest kritische afhankelijkheden en continuïteitsrisico's zijn;
- Worden de huidige beheersmaatregelen en herstelcapaciteit geëvalueerd;
- Kwantificeren van het potentiële effect op de kernprocessen en klantbediening;
- Aanvullende maatregelen om het risicoprofiel en de weerbaarheid te verbeteren;

De (initiële) beoordeling van verstoringen tijdens de BIA helpt bij het prioriteren van verdere (gedetailleerde) risicobeoordelingen. Daarbij wordt nadrukkelijk geadviseerd om eerdere veiligheidsbeoordelingen, dreigingsinformatie van overheden en sectorspecifieke groepen in overweging te nemen.

Voorbeeld

In de voedingsmiddelen of farmaceutische industrie zal een machine zal beschermd moeten zijn tegen onrechtmatige receptveranderingen.

Vragen zijn dan:

- Hoe zal het compromitteren van het systeem, de machine, de productievoortgang of productveiligheid verstoren?
- Welke in- of externe onbevoegde partijen kunnen de data en informatie compromitteren.
- Waar komen de dreigingen vandaan?

Afhankelijk van de aard van de onderneming kan het dreigingsniveau anders zijn. Vraag je af:

- Werk ik met grondstoffen die gevaarlijk zijn voor de gezondheid?
- Worden er bewegingen aangestuurd?
- Is mijn functie afhankelijk van, of lever ik, openbare gegevens, bijv. file-informatie, weersverwachting?
- Is er een toegangs- en screeningsbeleid van toepassing?
- Wat kost een uitval of verstoring van het systeem inclusief claims?

Als in de functionele eenheid onderdelen worden opgenomen uit de automatisering waar geen systeem- of applicatiesoftware in zit, neem dit dan wel mee in de risicobeoordeling maar documenteer dan dat er geen digitaal effect is.

Voor het bepalen van welke dreigingen worden meegenomen, kan bijvoorbeeld gebruik worden gemaakt van de Common Attack Pattern Enumeration and Classification (CAPEC™) database¹. Deze biedt zes gemeenschappelijke aanvalscategorieën die dit proces aanzienlijk kunnen helpen:

- Social Engineering: toegang krijgen tot het systeem door mensen te manipuleren of uit te buiten
- Supply Chain: het systeem wijzigen tijdens de productie van componenten, opslag of levering
- Communicatie: blokkeren, manipuleren of stelen van communicatie

¹ Andere methodes die gebruikt kunnen worden zijn bijvoorbeeld Mitre, Stride, Coras. Belangrijk is dat het overzichtelijk blijft en begrijpelijk voor de deelnemers aan de risicoanalyse.

- Fysieke Beveiliging: toegang krijgen tot het systeem door zwakke beveiligingsmaatregelen te overwinnen
- Software: toegang krijgen tot het systeem via kwetsbaarheden in softwaretoepassingen
- Hardware: toegang krijgen tot het systeem door de fysieke hardware van netwerkkaparameters te manipuleren

Notitie: bij het aanwijzen van de kwetsbaarheden is het uitgangspunt om dit te doen zonder dat er al beheersmaatregelen zijn genomen. Hier gaat het over niet-gemitigeerd risk. Dit is vooral om te voorkomen dat op basis van ongefundeerde aannames conclusies worden getrokken:

Hiervoor drie tips:

- Expliciteer de aannames aan de systemen. Een handmatig bediende brug kun je niet op afstand hacken. Als hier later eens een besturing opgezet wordt, dan doe je de risicoanalyse opnieuw.
- Expliciteer de omgeving. Als je systeem gemaakt is voor een specifieke omgeving, dan mag je daar wel rekening mee houden, maar dan is dat wel een voorwaarde bij de nadere uitwerking.
- Leun nooit zomaar op al genomen technische maatregelen. Bijvoorbeeld netwerksegmentatie kan een goede beveiliging leveren, maar is bijna nooit waterdicht.

Blijf ook niet hangen in discussies of het wel of niet kan. Bij twijfel ga ervan uit dat de situatie zich voordoet in de vorm van een “wat als” vraag.

Analyseer de risico's van het SuC. Deze kwetsbaarheid en dreiging bepalen de ergste scenario's en effecten die voortkomen uit storingen in het IACS (Industrial Automation and Control System). Gebruik de risicomatrix die ook voor een detail risicoanalyse wordt gebruikt, maar laat de kans op 100% staan. Hieruit volgt dan het maximale effect.

2.4 ZCR3: Indelen in zones en conduits:

Het indelen in zones en conduits volgt op het High Level Risk Assessment.

Verdeel het SuC vervolgens in verschillende Zones en Conduits om een gedetailleerde analyse voor te bereiden. Gebruik daarbij als uitgangspunten:

- Scheid de IT-zone van de OT-zone(s);
- Definieer specifieke zones voor de Safety Instrumented Systems (SIS);
- Definieer specifieke zones voor tijdelijk aangesloten (service) apparatuur;
- Definieer zones voor draadloze netwerken;
- Scheid de zones die via externe netwerken zijn verbonden.

Bij het scheiden van Zones is het essentieel de overgangen te beoordelen. Deze beoordeling is leidend in de configuratie van de Conduits. Bijvoorbeeld welk protocol mag wel en welk protocol is niet toegestaan. Aannames van zone overgangen komen vaak voort uit impliciete eisen die bij iemand in het hoofd zitten. Maak deze eisen expliciet en toets nu al of deze realistisch zijn. Wat gebeurt er als de zones niet gescheiden zijn?

2.5 ZCR4: Bepaal of het totale risiconiveau het toelaatbare niveau overschrijdt:

Deze risicobeoordeling kan uitgevoerd worden als een mini Business Impact Analyse (mini-BIA) als gevolg van cyberactiviteiten. Vanuit de BIA is het mogelijk om dit risiconiveau te beoordelen en te vergelijken met wat door de organisatie wordt getolereerd. Beoordeel of het totale risiconiveau hoger is dan wat door de organisatie wordt getolereerd. Als dit het geval is, moet een gedetailleerde risicobeoordeling van elke zone worden uitgevoerd.

Het resultaat van deze stappen dient gedocumenteerd aangeboden te worden aan het management voor een goedkeuring van de eigenaar van de asset.

Met deze stappen is inzicht gegenereerd in waar en hoeveel afhankelijkheid en risico er zit in automatisering. Hiermee is aanvullende informatie ten opzichte van de BIA verkregen. Dit helpt in het prioriteren van risico's en het opstellen van en invoeren van beheersmaatregelen.

Voorbeelden van risico's

Enkele voorbeelden van risico's die uit een high level risico assessment kunnen komen, zijn:

- Een matige kans op een malwarebesmetting die netwerkproblemen veroorzaakt in het OT-netwerk, wat resulteert in verminderde zichtbaarheid van het industriële proces in de controlekamer (compromitteren integriteit). Dit zou mogelijk noodsituaties kunnen veroorzaken.
- Een lage kans dat een aannemer met criminele intentie en fysieke toegang tot het controlesysteem de daarin aanwezige informatie onderschept en met succes controlecommando's wijzigt, wat schade aan de faciliteit veroorzaakt.

3 Het creëren van draagvlak

Het creëren van draagvlak bij het management voor maatregelen tegen cyberrisico's in een fabrieksomgeving vereist een strategische aanpak die zowel de technische als de bedrijfskundige kant belicht. De doelgroep is het managementteam en directie. Beschrijf daarom de risico's op een hoog niveau en laat de detailinvulling weg. Hier zijn enkele concrete stappen die genoemd kunnen worden:

1. Maak het risico tastbaar

- Gebruik praktijkvoorbeelden van cyberaanvallen op vergelijkbare fabrieken (bijv. ransomware-aanvallen op OT-systemen).
- Toon het effect: leg uit wat de gevolgen kunnen zijn voor productie, veiligheid, reputatie en compliance.
- Gebruik statistieken of incidenten uit de sector (bijvoorbeeld vanuit de NIS2-richtlijn).

2. Vertaal risico's naar de business

- Laat zien wat een cyberincident kost: stilstand, herstelkosten, boetes, reputatieschade.
- Een kosten-batenanalyse zal in een stadium uitgewerkt moeten worden. Wat kost een maatregel versus wat bespaart het bij een incident?

3. Sluit aan bij strategische doelen

Koppel cybersecurity aan thema's die al op de agenda staan, zoals:

- Continuïteit van productie
- Veiligheid van personeel
- Kwaliteit en betrouwbaarheid
- Compliance met regelgeving

4. Betrek de juiste stakeholders

- Werk samen met bijvoorbeeld productie, IT, OT, compliance en financiën.
- Laat zien dat cybersecurity een gedeelde verantwoordelijkheid is.

5. Gebruik visuele en begrijpelijke communicatie

- Stem je boodschap af op je doelgroep.
- Vermijd technisch jargon.
- Gebruik infographics, risico heatmaps of scenario's om je verhaal kracht bij te zetten.

Afkortingen en begrippen

BIA	Business Impact Analysis
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid (ook wel als CIA aangeduid)
CAPEC™:	Common Attack Pattern Enumeration and Classification (database)
CIA	Confidentiality, Integrity en Availability (ook wel als BIV aangeduid)
CSMS	Cyber Security Management System.
DCS	Distributed Control System
EHBO	Eerste Hulp Bij Ongelukken
HL-RA	High Level Risico Analyse
HSE	Health, Safety & Environment
IACS:	Industrial Automation and Control Systems
IPCS	Industriëel Platform Cyber Security
IT	Information Technology
KPI	Key Performance Indicator
MKB	Midden- en KleinBedrijf
IEC:	International Electrotechnical Commission.
NIS2:	Network and Information Systems (NIS2 Directive)
OT:	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control And Data Acquisition
SIS	Safety Instrumented System
SL	Security Level (gespecificeerd in IEC62443-3-3)
SRP	Safety reliability Productivity
SUC	System under Consideration (het te onderzoeken systeem/ bedrijfsdeel)
ZCR	Zone and Conduit Requirements

Kijk voor meer informatie over het IPCS op <https://securitydelta.nl/ipcs>

Andere publicaties van het IPCS zijn:

- Elevator Pitch Board Level IEC 62443
- Elevator Pitch Vendors IEC 62443
- Korte beschrijving delen van de IEC 62443
- Korte handleiding start IEC 62443
- Incident respons/Incident recovery
- Cybergevoeligheid van tijd
- CMDB en tooling

Deze publicaties kunt u opvragen via <https://securitydelta.nl/ipcs>.

Auteurs

Naam
Eric ten Bos
Gert Ippel
Gert Sloof
Philip Roodzant
Ewald Coenraad
Philip Westbroek
Erik Vinke
Michael Theuerzeit

Met dank aan Thomas Vasen, Rob Hulsebos en Michael Theuerzeit voor het redigeren van de teksten, en de overige leden van de 'IPCS-werkgroep IEC 62443' voor het reviewen van dit document.



ipcs@securitydelta.nl
www.securitydelta.nl/ipcs