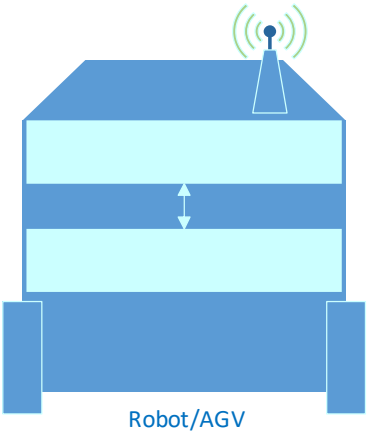
Cybersecurity van robots in de smart industry



Teade Punter, Casper Schellekens, Ron Mélotte, Tom Broumels, Lake Lakeman en Jules Vos.

Eindrapportage KIEM.HTS.03.008

Versie 10, 15 juli 2019

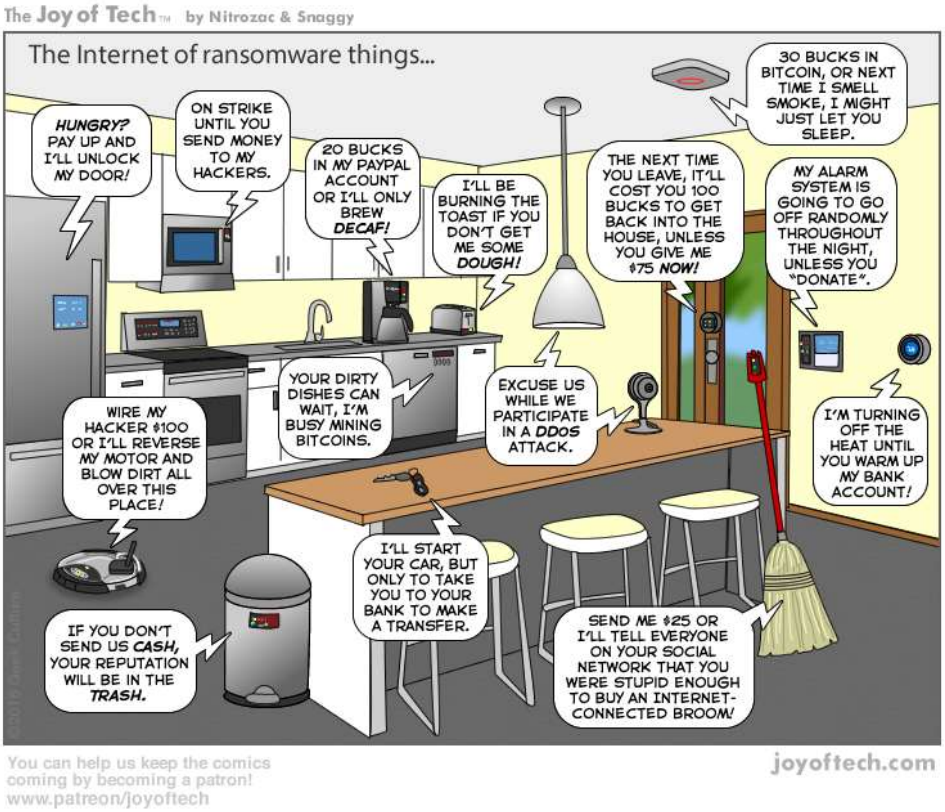
Lectoraat High Tech Embedded Software van Fontys Hogeschool ICT, Eindhoven

Quote – “als alles met alles samenhangt dan wordt het geheel zeer kwetsbaar bij infecties…”

Inhoud

1 Cybersecurity van verbonden industriële systemen

In een wereld waar meer en meer apparaten verbonden worden met het internet[1], wordt het belangrijk dat de apparaten probleemloos met elkaar blijven samenwerken. Alles waar het woord ‘smart’ in voorkomt moet ook ‘smart’ resultaten opleveren. Denk hierbij aan smartphones, smart TV’s en smart thermostaten die ieder data genereren en delen met andere apparaten en gebruikers in het internet. Als deze apparaten niet de goede data krijgen of verkeerd hun eigen data gaan doorgeven aan andere apparaten, dan verdwijnt de smartness van deze systemen. De beveiliging van de communicatie zodat de smart systemen goed functioneren is daarom belangrijk. Cybersecurity is het aandachtsgebied in de software engineering dat zich bezig houdt met beveiliging van communicerende systemen.

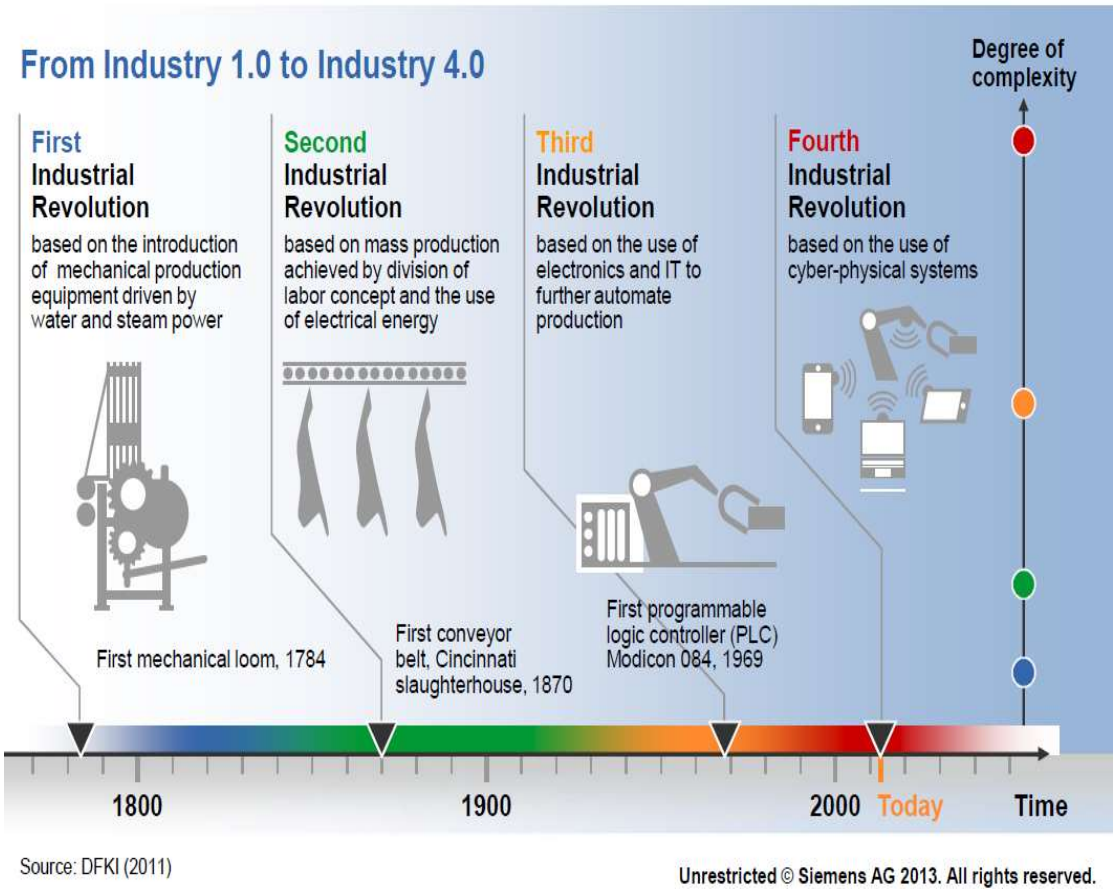


Figuur 1 **Een interpretatie van cybersecurity uitdagingen in de huisomgeving.**

De ontwikkelingen van het Internet of Things (IoT) beinvloeden ook de industriële wereld. In deze wereld, waarin procesautomatisering centraal staat, zorgt het verbinden van industriële apparaten ervoor dat er data stromen ontstaan die voorheen niet zichtbaar waren. Hierdoor wordt het mogelijk om in een keten van toeleveranciers data aan elkaar door te geven. Ook wordt het mogelijk om systemen autonoom aan te sturen zoals met Automated Guided Vehicles (AGVs) aansturing van productielijnen gebeurd.

De verbondenheid van de industriele systemen via het internet, de zgn. cyberspace, wordt steeds belangrijker. In plaats van embedded systemen spreken we daarom steeds vaker van Cyber Physical Systems (CPS) (Lee & Seshia, 2015). Voorbeelden zijn robots, medische apparatuur, (zelfrijdende) auto’s en energie centrales.

[1] Het zgn. Internet of Things (IoT).



Figuur 2 **Stadia van industriële ontwikkeling, tot Industrie 4.0**[2]

Het verbinden van machines, waardoor machine met machines gaan communiceren wordt aangeduid als *Smart Industry*[3]. Dit is de trend in de Nederlandse maakindustrie waarin apparaten meer op elkaar worden afgestemd om zo efficiency en effectiviteit van productie en distributie te verbeteren. Deze slimme bedrijven ontstaan onder andere door hun apparaten met elkaar te laten communiceren waardoor een informatieketen tot stand komt. Zo kan men flexibeler aanpassen en werken. In Duitsland en ook internationaal wordt deze trend aangeduid als *Industrie 4.0*.

In de Smart Industry staat dus het verbinden van machines, en de communicatie ertussen, centraal: de zgn. Machine2Machine (M2M). Door machines in productieprocessen, assemblagelijnen en opslagsystemen met elkaar te verbinden worden verbeteringen verwacht. Internet connectiviteit is hiervoor direct of indirect nodig. Cyber security is daarmee een belangrijk aandachtspunt voor Smart Industry. De risico's op security incidenten worden immers groter naarmate steeds meer systemen op het internet zijn aangesloten.

Een bekend cybersecurity probleem in de industriële wereld was de Stuxnet worm die in 2010 het Iraanse nucleaire programma trof. Het betrof waarschijnlijk een besmetting van het computer systeem van de Iraanse nucleaire installatie via een geïnfecteerde USB stick. De Stuxnet worm, op deze stick, was gericht op het

[2] http://www.siemens.com/innovation/en/home/pictures-of-the-future/industry-and-automation/digtial-factory-trends-industry-4-0.html.
[3] https://www.smartindustry.nl/.

beschadigen van fysieke hardware van de nucleaire installatie. Voor het Iraanse nucleaire programma betekende dit het vervangen van honderden kostbare centrifuges.
Het incident illustreert dat industriële automatisering niet immuun is voor cyber aanvallen. De betreffende aanval kan in het licht van politieke spanningen tussen landen worden geplaatst: een staat die zich volgens andere staten niet op dit gebied mag ontwikkelen. Het betreft hier een vorm van oorlogsvoering. Echter, het incident staat niet op zich. Zo beschrijft de Industrial Security Incident Database[4] ruim 200 incidenten wereldwijd, waarvan een aanzienlijk deel vergelijkbare aanvallen als op de Iraanse Nucleaire installaties betreft.

Cyber security gaat verder dan elektronische oorlogsvoering. Het gevaar ligt ook om de hoek. De auteurs van dit artikel willen u als zelfstandige in het MKB of u als manager niet bang maken. Wij geloven niet in angstverhalen, maar in een nuchtere aanpak. Echter, onze verkennende analyse op het gebied van cyber security laat zien dat cybersecurity relevant is voor het MKB, zeker omdat we in een digitale transformatie, richting Smart Industry, zitten. Onze analyse, uitgevoerd vanuit het lectoraat Hightech Embedded Software van Fontys Hogeschool ICT, laat actuele dreigingen voor MKB industriële omgevingen zien. We hebben kwetsbaarheden aangetroffen in alle door ons onderzochte omgevingen. Ter illustratie drie voorbeelden van kwetsbaarheden in onderzochte omgevingen.
Laatstejaars FHICT studenten in de richting Cyber Security hebben in een realistisch lab omgeving van een belangrijke leverancier van industriële automatisering (bij Actemium) laten zien dat de besturing van programmable logic controllers (PLC's) op verschillende manieren was over te nemen. Dit varieerde van het uitbuiten van kwetsbaarheden in het operating system van het engineering station tot het versturen van gemanipuleerde S7COMM instructies vanuit het engineering station.
Een team bestaande uit tweedejaars FHICT studenten, heeft in een nagebootste AGV omgeving, die representatief is voor AGVs in de MKB-industrie, aangetoond dat het ontbreken van authenticatie en encryptie in de communicatie tussen Engineering station en AVG-systemen het eenvoudig maakte om verkeer te manipuleren. Zo kon de besturing van de AGV worden overgenomen en naar een willekeurige locatie worden genavigeerd.
Het derde voorbeeld betreft een uitgevoerde penetratietest op een kantooromgeving waarin tweedejaars FHICT studenten erin slaagden om toegang te krijgen op het lokale netwerk, via een zgn. wifi cracking attack. Zij stuitten daarbij op Engineering stations waarop zij zonder enige vorm van authenticatie volledige toegang hadden tot PLC's.

In dit artikel/rapport staat de cybersecurity van (mobiele) robots in de *Smart Industry* centraal. Wij verwachten dat robots een belangrijke rol gaan spelen in de Smart Industry. Traditioneel worden robots hoofdzakelijk bij grote bedrijven voor massa fabricage ingezet. Door voortschrijdende ontwikkelingen in Mechatronica en de ICT groeit en verbreedt de inzet van robots zich sterk; bijvoorbeeld bij bedrijfsprocessen in logistiek en kleinschalige fabricage. Door deze bredere inzetbaarheid van robots zijn ze minder afgeschermd en beveiligd en ontstaan ook hier nieuwe cybersecurity

[4] ..https://www.risidata.com/Database. In 2001 opgezet door een onderzoeksteam van de British Columbia Institute of Technology. Op de website staat dat de database tot 2015 is bijgehouden.

uitdagingen die nog onvoldoende aandacht krijgen en om nader inzicht en oplossingsrichtingen vragen.

Steeds meer robots zijn in staat met mensen samen te werken en weten wat ze wel en niet moeten doen om veilig met mensen om te gaan. De zogenaamde collaborative robots (cobots) zijn dan ook met een opmars bezig. De komende jaren zal het steeds normaler worden dat mensen met een robot samenwerken. Dat robots zo nauw betrokken zijn in ons leven, maakt het ook belangrijk dat iedereen is voorbereid op deze samenwerking (Holland Robotics, 2018), (Sparc, 2016). Voor cobots betekent dit dat er data uit de omgeving van de robot verwerkt moet worden om daaruit snel en betrouwbaar conclusies te trekken over de aanwezigheid van mensen en hun intenties. Robots zullen ook steeds vaker in ongestructureerde omgevingen moeten functioneren. Het gaat dan bijvoorbeeld om robotarmen die voorwerpen van verschillende grootte of vorm uit dozen moeten pakken. Een ander voorbeeld zijn de warehouses en productiestraten in de Smart Industry waar Automated Guided Vehicles (AGVs) goederen oppakken (picken) en verwerken voor een vervolgstap, zoals het op een pallet zetten van artikelen. Hier worden robots geacht veilig te reageren wat betekent dat ze bijvoorbeeld om moeten kunnen gaan met situaties waar er onverwacht voorwerpen of zelfs mensen op hun pad staan die hun geplande beweging belemmeren.

Figuur 3 **Voorbeelden van AGVs in de smart industry.**[5]

Wij denken dat het zinvol is om industriële productieomgevingen onder de loep te nemen en we richten ons daarbij op zgn. Automated Guided Vehicles (AGVs), een vorm van mobiele robots. In dit artikel/rapport gaan we daar als volgt op in:

- Wat zijn cybersecurity bedreigingen voor robots in de smart industry? Inventarisatie van bedreigingen, hoofdstuk 2.
- Wat maakt security in de smart industry anders dan beveiliging van conventionele informatiesystemen? Hoofdstuk 3.
- Wat zijn onze bevindingen met de beveiliging van AGVs? hoofdstuk 4 en 5.
- Hoe ziet een aanpak voor robot security in de smart industry er uit? Een voorstel tot maatregelen wordt gegeven in hoofdstuk 6.
- Ten slotte doen wij in hoofdstuk 7 een oproep om cybersecurity van robots in de smart industry te verbeteren.

[5] ..AGVs van (met de klok mee, links beginnen): Prodrive, Omron (Adept), Mobile Industrial Robots (MIR), Vanderlande Industries (Fleet) en Probotics.

2 Bedreigingen voor robots in de smart industry

Dit hoofdstuk gaat in op de bedreigingen voor de Smart Industry. In ons onderzoek is een beperkt aantal artikelen en rapportages met als onderwerp Smart Industry zowel als AGV technologie als (cyber) security gevonden. Er zijn geen noemenswaardige bronnen aangetroffen die beide onderwerpen in duidelijke relatie tot elkaar adresseren.

2.1 Voorbeelden van bedreigingen in de industriële automatisering

In het nieuws verschijnen regelmatig berichten van cyberaanvallen. Hieronder worden zes voorbeelden van cyberaanvallen in de industriële automatisering beschreven:

1. Een 'infectie' van de IT-systemen bij 13 van DaimlerChrysler's autofabrieken met de zgn. Zotob worm leidde tot 1 uur stilstand van productielijnen in 2005. De software moest worden gerepareerd. Kosten van de stilstand, waardoor 50.000 medewerkers 5 tot 50 minuten geen productie draaiden is onbekend[6]
2. Ransomware aanval bij machine fabriek Almi in Vriezeveen in 2017. Meer dan 400 gigabyte aan data was hierdoor niet meer te benaderen. Ook richtte het virus schade aan in de geautomatiseerde fabriek. Verder werd de backupserver aangetast. Schade van de aanval voor het bedrijf was € 60.000[7].
3. Het containertransportbedrijf Maersk werd in 2017 zwaar getroffen door ransomware. Het Notpetya virus[8] trof bestandssystemen van het bedrijf die vervolgend geencrypt werden, en tegen betaling weer ontsloten konden worden. Maersk moest ruim 45.000 pc's en 4000 nieuwe servers herinstalleren. Dit kostte ruim 10 dagen waardoor scheepsoperaties vertraging opliepen. Dank zij stroomuitval bij een van haar servers vlak voor de Notpetya aanval was het bedrijf nog in staat haar systemen weer op te starten.[9]
4. Het aluminiumbedrijf Norsk Hydro, met in Nederland vestigingen in Drunen, Hoogezand en Harderwijk, werd in maart 2019 getroffen door een ransomware-aanval. Het betrof het LockerGoga virus dat gecombineerd werd met een aanval op de Active Directory van de computersystemen. Het bedrijf heeft vervolgens alle computersystemen wereldwijd van het bedrijfsnetwerk afgesloten om verspreiding en migratie van het virus tegen te gaan. De aanval heeft het bedrijf geen data gekost[10]. Er is waarschijnlijk geen losgeld betaald, maar de schade door stilstand productie wordt geschat op € 35.000.000[11].
5. In december 2015 werd een regionale electriciteitsdistributie bedrijf in Oekraine (Kyivoblenergo) getroffen doordat de SCADA systemen van het bedrijf illegaal werden bediend door hackers. Met de door hen geïnstalleerde BlackEnergy3 malware werden de schakelkasten in zeven 110kV- en drieëntwintig 35 kV-substations uitgeschakeld. Hierdoor waren 80.000 tot 225.000 eindgebruikers afgesloten van hun stroomvoorziening.

[6] https://www.eweek.com/security/zotob-pnp-worms-slam-13-daimlerchrysler-plants.

[7] https://www.deondernemer.nl/nieuwsbericht/173403/cyberaanval-ondernemer-60-000-euro.

[8] https://en.wikipedia.org/wiki/Petya_(malware).

[9] https://www.agconnect.nl/artikel/stroomstoring-blijkt-ransomware-redding-voor-maersk.

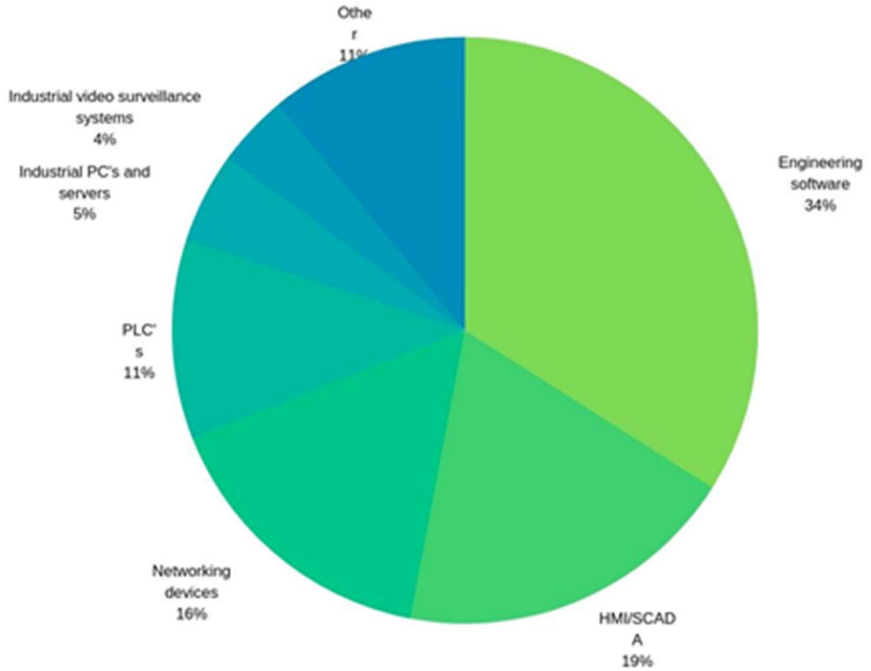
[10] https://tweakers.net/nieuws/150464/ransomware-treft-grote-noorse-aluminiumfabrikant.html.

[11] https://betanews.com/2019/04/09/understanding-lockergoga-ransomware/.

6. Tenslotte een voorbeeld dat meer in de AGV-context is te plaatsen, namelijk de hack door de hackers Miller en Valasek van de Jeep Cherokee van journalist Andy Greenberg. Zij konden de volumeknop van de autoradio instellen, maar ook de autofuncties als versnellen en vertragen overnemen[12].

De voorbeelden laten zien dat er veel toepassingen zijn waar het gaat om industriële automatisering. De voorbeelden laten ook zien dat de systemen op verschillende manier kunnen worden aangevallen. Het kan bijvoorbeeld gaan om malware, ransomware, of (D)DOS aanvallen. De voorbeelden tonen ook dat er verschillende typen aanvallers zijn: criminelen die uit zijn op losgeld door ransomware te installeren, voorbeelden 2 en 3. De aanvallers zijn echter niet altijd duidelijk, de vraag "wie maakt ons het leven zuur?" is soms niet direct duidelijk bij een aanval. Het kan gaan om nationale staten, zoals waarschijnlijk Rusland in voorbeeld 5, die bijvoorbeeld ook bedrijfsgeheimen kunnen stelen voor eigen gewin. Maar er kan bijvoorbeeld ook sprake zijn van een wraakactie van ex-werknemers door systemen van de (ex) werkgever te hacken.

Hoe zit het met AGVs?
Kaspersky (2018a) analyseert Industriele Computer Systemen (ICS) incidenten. Het onderstaande overzicht geeft percentages van incidenten per type component in de industriele automatisering.

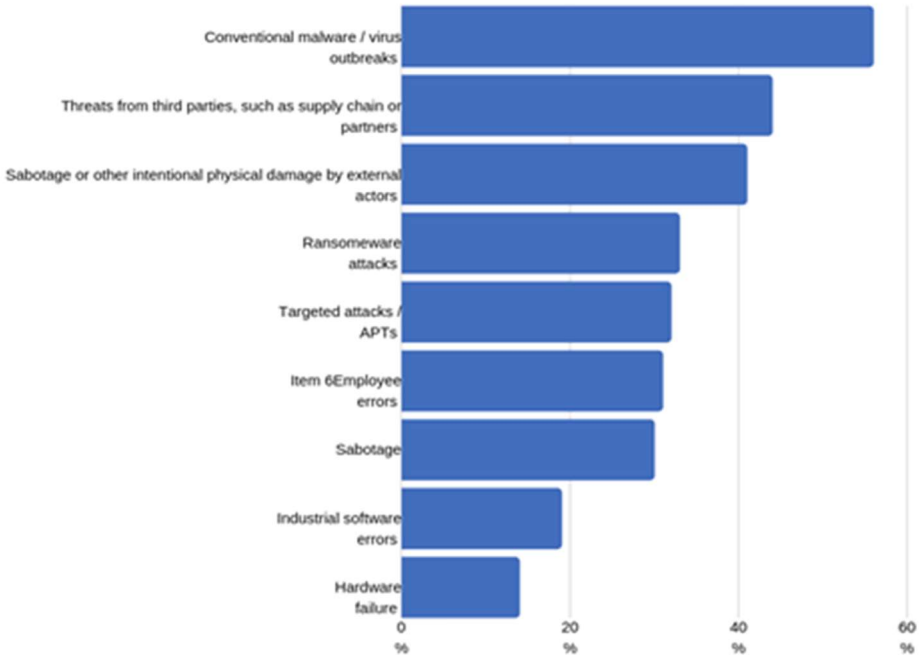


Figuur 4 **Verdeling van kwetsbaarheden (vulnerabilities) van ICS componenten.**

De ondervraagde organisaties in het ICS domein schatten in dat er een behoorlijke kans is om doelwit te worden van cyber security aanvallen: incidenten. Cyber Security op ICS gebied krijgt veel prioriteit. Tegelijkertijd zegt 55% van de organisaties niet te maken hebben gehad met incidenten in het afgelopen jaar. Als

[12]..https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

daarvan wel sprake is, dan was in 64% van de gevallen conventionele malware/virussen, 30% ransomware, 27% (menselijke) fouten de oorzaak. Oorzaken als gerichte aanvallen (16%), data lekken en spionage (14%), sabotage van buitenaf (9%) en sabotage door medewerkers (5%) staan lager op de lijst van oorzaken van indicenten. Van derde partij bedreigingen, zoals supply chain partners, was in 20% van de incidenten sprake. De door Kaspersky ondervraagde bedrijven maken de volgende inschatting van hun bedreigingen, meting 2017[13]:



Figuur 5 **Overzicht van de inschattingen op de vraag 'wat is top 3 cyber security bedreigingen van uw industriele automatisering?**

Als we uitgaan van omgevingen waarin AGVs worden toegepast, dan zou dat naar schatting tussen 7% (Commercial facilities) en 23% (critical manufacturing) zijn van de in de survey beschreven ICS gerelateerde incidenten.
90% van de ondervraagden gaf aan Wireless netwerken voor de ICS omgevingen te gebruiken. Ook geeft zo'n 40 procent aan cloud diensten als SCADA as-a-service geïmplementeerd te hebben of binnen een jaar te willen implementeren.

2.2 Gevolgtrekkingen: AGV, Incident/response, Risico

Op basis van de bovenstaande voorbeelden en de incidentoverzichten:

1. Denken we dat bedrijven pas na daadwerkelijke aanval aandacht voor krijgen voor een betere beveiliging.
2. Lijkt het onmogelijk om systemen volledig te beveiligen. Er zullen altijd zwakheden zijn die kunnen worden misbruikt. 100% veiligheid bestaat niet.
3. Hebben wij geen voorbeelden gevonden van cyber security aanvallen waarin AGVs zijn betrokken.

[13] .. https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf.

Naar aanleiding van 3 is in het kader van het project een casus rondom cybersecurity uitgevoerd, zie hoofdstuk 4.

Uit 2 leiden we af dat het belangrijk is om acuut te reageren op actuele bedreigingen: op een incident volgt een response.
Richtlijn – leg een incident response administratie aan – welke aanvallen zijn er geweest en hoe is daarop gereageerd, met welk effect?

Uit 1 en 2 leiden we af dat het nodig is om risico-denken te gebruiken. Als 100% beveiliging onmogelijk lijkt dan is het nodig om de meest bedreigende incidenten te voorkomen. Dit betekent dat het compliance denken, waarin een systeem gecheckt wordt, moet worden omgebogen naar denken in een wereld van risico's. Wat zou er allemaal kunnen gebeuren?
Risico gaat over waarschijnlijkheid (P) en de impact (I) van de bedreigingen. Risico = P x I.

- Waarschijnlijkheid van een dreiging is de kans op een daadwerkelijk succesvol uitgevoerde aanval.
- Impact van een dreiging is de gevolgen, de schade, die optreden als de dreiging optreedt. In het voorbeeld van Maersk bijvoorbeeld het uitvallen van 4000 PCs, maar ook het verlies van werk omdat er 10 dagen nodig is om systemen op te starten.

Het inschatten van risico's wordt door verschillende factoren bepaald. De manier waarop dit gebeurt wordt voor een deel bepaald door de aard en het beleid van de specifieke organisatie. In de business van alledag lijkt er soms minder aandacht voor te zijn. Met de bovenstaande voorbeelden is de notie er achteraf wel. Zowel waarschijnlijkheid als impact zijn behoorlijk afhankelijk van de bedrijven en systemen, daarom gaan we hier niet in algemene zin op risico's in. Wel gaan we in op de bedreigingen zoals die vanuit standaarden worden gezien, zie paragraaf 2.3

Richtlijn – denk in risico's – bepaal mogelijke bedreigingen en de impact er van. Voor een dergelijk risk-assessment regelmatig uit. Bepaal daarbij per bedreiging kans (P) en impact (I) en stel daarbij contingenties en mitigaties op.

Mitigaties zijn de acties die genomen worden om het risico te voorkomen. Een bekend voorbeeld is het risico dat een koe tijdens het drinken in een sloot valt. Een tegenmaatregel is om een hek om het weiland te zetten. Contingenties daarentegen zijn de acties die genomen kunnen worden op het moment dat het risico optreedt. In het geval van het risico dat de koe tijdens het drinken in de beek valt is dat het paraat hebben van een draaiboek om te kunnen handelen, zoals een takelwagen of het draaiboek met het telefoonnummer van het takelwagenverhuurbedrijf.

2.3 Bedreigingen – ICS vs NCSC CSAN

Om tot een reële set van mogelijke dreigingen te komen is het van belang om een inschatting te maken van de betrokken actoren: de beweegredenen (motivatie) en middelen (ook: kennis) van deze partijen zijn immers bepalend voor de daadwerkelijk te verwachten aanvallen, ofwel de dreigingen.

<u>Dreigingen en actoren</u>

In de volgende paragrafen worden ICS specifieke dreigingen op het gebied van digitale security beschreven en daarmee samenhangend de actoren die verantwoordelijk zijn voor de dreigingen. In een aantal typologieën worden actoren als onderdeel van de dreiging gezien. Daar is iets voor te zeggen omdat actoren en dreigingen onlosmakelijk met elkaar verbonden zijn. Voor dit onderzoek kiezen we ervoor dreigingen en actoren los te beschouwen.

Actoren

Het onderzoek "Towards a new cyber threat actor typology" van TU Delft voor Nationaal Centrum Cyber Security (NCSC) (de Bruijne e.a., 2017) gebruikt diverse typologieën om actoren te classificeren.

- Sommige typologieën worden op maat ontwikkeld, door uit te gaan van geanalyseerde incidenten in relatie tot de organisatie waar het om gaat. Werkwijzes en gewoonten van actoren worden genoemd als goede basis om een typologie op te baseren. Omdat vaak empirische kennis ontbreekt (o.a. vanwege vertrouwelijkheid) over deze incidenten is een typologie als deze lastig te realiseren. Ook voor ICS incidenten en zeker AGV gerelateerde incidenten is dit het geval.
- Actoren zijn geclassificeerd in een beperkt aantal klassen of tot een meer uitgebreide hoeveelheid klassen.
- Actoren zijn beschreven voor een(Cyber) security domein.
- De meest typologieën hebben met elkaar gemeen dat de totstandkoming van de typologie onduidelijk is.
- Daarnaast wordt in NCSC CSAN (2018) opgemerkt dat grenzen tussen actoren lijken te vervagen.

Een typologie voor AGV gerelateerde security bedreigingen hebben we tijdens onze inventarisatie nog niet kunnen vinden. We gaan daarom uit van een redelijk passende ICS security specifieke typologie. Typologieën die ons inziens dan in aanmerking komen zijn:

- US ICS CERT - U.S. Industrial Control Systems Cyber emergency Response Team typologie.
- NCSC CSAN - *Threat actor* typologieën in de Dutch CSAN[14].

Zie tabel 1.

Het vergelijken van de klassen van de twee typologieen laat zien dat de NCSC typologie geen actoren mist ten opzichte van de meer specifieke US ICS CERT variant (industrial spies zijn een specifiek voorbeeld van criminals). Wel omvat de NCSC typologie Insiders en Unintentional acts als categorieen. Omdat incidenten op ICS vlak denkbaar zijn waarbij kwaadwillenden insiders zijn of er geen kwade bedoelingen in het spel zijn, lijkt de NCSC typologie completer.
Omdat de NCSC recent een vernieuwde actor typologie heeft aangenomen gebaseerd op internationaal onderzoek naar actor typologieen en een meer volledige beeld schetst dan de US ICS CERT variant kiezen we in dit onderzoek voor de actor typology van de NCSC.

[14]..NCSC, 2018, https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html). Deze typologie is een ingedikte versie op basis van het resultaat van het onderzoek "Towards a new cyber threat actor typology".

US ICS CERT	NCSC, CSAN 2018
Governments	Nation-state/state-sponsored
Terrorists	Terrorists
Industrial spies and organized crime groups	Criminals
Hacktivists	Hacktivists
Hackers	Cyber vandals and script kiddies
	Insiders
	Unintentional acts

Tabel 1 – Vergelijking ICS CERT vs NCSC CSAN

Threats/bedreigingen

Ook voor threats zijn verschillende typologieen te vinden. Een typologie die bruikaar is voor ons onderzoek is van ENISA, genoemd in het document "ENISA Good practices for security of IoT" uit 2018. Deze typologie is gebaseerd op de meer algemene Threat typologie van ENISA uit 2016. Hoe deze typologie tot stand is gekomen is ons niet bekend. Wel is deze typologie uitgebreid en toegespitst op Industrial Internet of Things (IIoT).
Het Cyber Security Assessment Netherlands 2018 van het NCSC benoemt ten opzichte van ENISA welke targets (organisaties) welke dreigingen door welke actoren relevant zijn. Met relevant wordt bedoeld: de actoren hebben de motivatie en middelen om een aanval uit te voeren, of een soortgelijke dreiging is eerder geobserveerd. Daarom kiezen we er, naast eerder genoemde redenen, in ons onderzoek voor de typologie van het NCSC te hanteren voor threat actoren en threats. Gezien de omgeving waarin AGVs worden ingezet richten we ons vooral op de target 'Private Organisation', maar eventueel ook op de target 'Critical systems/organisations'.

Actor	**Threats gerelateerd aan Private organisations**	**Threats gerelateerd aan Critical systems/organisations**
Nation-state/state-sponsored	Sabotage (!) Disruption (!) Espionage	Espionage (!) System manipulation
Criminals	Information thef (!) Information manipulation (!) Disruption (!) System manipulation	Disruption (!) System manipulation
Terrorists		Sabotage (-)
Hacktivists	Disruption Information theft Information manipulation (-)	Disruption Information manipulation (-)
Cyber vandals and script kiddies	Disruption Information theft (-)	Disruption Information theft (-)
Insiders	Information thef Disruption (-)	Information thef Disruption (-)
Unintentional acts	Breakdown/failure Leak (-)	Breakdown/failure Leak (-)

! = grotere dreiging, "-" = kleinere dreiging

Tabel 2 – Threats volgens NCSC.

Duiding

Er is beperkte informatie beschikbaar over totstandkoming van actor typologieën en threat classificaties en concrete incidenten. Een AGV-specifieke actor of dreiging typologie hebben we niet kunnen vinden. Daarom zijn de bevindingen gebaseerd op onderzoek naar het meer algemene ICS. Omdat het gebruik van AGV systemen niet 1-op-1 samenhangt met toepassing van ICS kunnen we alleen voorzichtige uitspraken doen over mogelijke actoren en dreigingen op het gebied van AGVs.
Een vervolg op dit punt zou kunnen bestaan uit het verzamelen, valideren en analyseren van incidenten (o.a. uit de RISI database, vulnerability onderzoek/pentests, en meer specifieke interviews) met betrekking tot AVG security en op basis van die analyse clusters van actoren en/of dreigingen benoemen.

Omdat we voor ons onderzoek op zoek zijn naar zowel threat actoren als threats ligt het voor de hand om de topologie zoals de NCSC deze hanteert over te nemen. Deze is gebaseerd op een uitgebreid vergelijk van typologieën en daarnaast claimt het NCSC bij het relateren van threat actoren en threats rekening te houden met zowel eerdere incidenten als motivatie/mogelijkheden van actoren.

Op ICS security gebied wordt een dreiging reëel geacht en heeft security prioriteit. Het is niet duidelijk of dat voor omgevingen waar AGVs worden toegepast ook het geval is. Wel is duidelijk dat incidenten in verschillende componenten van ICS voor kunnen komen en dat ook indirecte oorzaken (bijv. via 3rd party software) worden genoemd. Het is denkbaar dat als een organisatie niet direct interessant is voor een actor, deze wel als interessant startpunt of schakel kan worden gezien. Met andere woorden: security gaat over de hele keten, dus elk deel in de keten, waaronder ook 3rd party software. Denk daarbij bijvoorbeeld ook aan discussie rondom Huawei als leverancier in 5G netwerk[15].
Dreigingen die in de CSAN worden aangemerkt als belangrijke dreiging worden minder vaak gemeld door geïnterviewde organisaties dan dreigingen die als minder belangrijk worden aangemerkt. Het is mogelijk interessant om nader te onderzoeken waar dat verschil mee te maken heeft (andere onderzochte doelgroep? aanvallen deels onopgemerkt aangezien weinig monitoring een veel voorkomende zwakheid is volgens US ICS CERT?, al veel geïnvesteerd op beveiligen tegen belangrijkste dreigingen?). Aan de andere kant is het de vraag of dat nadere, AGV-specifieke informatie oplevert.

[15] ..https://www.rtlz.nl/algemeen/politiek/artikel/4675006/tweede-kamer-wil-geen-5g-met-huawei-na-spionageschandaal.

3 Smart Industry en AGVs - Wat maakt industriële automatisering anders dan kantoorautomatisering?[16]

In deze paragraaf wordt Industriële automatisering tegenover de kantoorautomatisering (KA) geplaatst, om de karakteristieken van cybersecurity in robots in de *Smart Industry* scherper te kunnen optekenen. Binnen de industriële automatisering richten we de blik dan op Robots in de *Smart Industry*.

Industriële automatisering (IA) betreft de automatisering van processen in de (fysieke) productie en assemblage, zoals de lopende band, en het aansturen van machines, zoals CNC freesmachines. Het kan ook om besturing van grotere systemen gaan. Industriële automatisering is zo op te vatten als Operationele Technologie (OT), waarbij OT alle systemen betreft voor aansturing, monitoring en communicatie van productie installaties. Dus ook voor vitale processen zoals waterzuiveringen, waterwerken, energiecentrales, gaswinning, (petro)chemie enzovoorts. Zo worden dan bijvoorbeeld ook gebouwbeheersingssystemen als onderdeel van OT gezien, terwijl sommigen zelfs dat toegangscontrole van systemen, incl. camerabewaking, als OT opvatten.

Kantoorautomatisering betreft het digitaliseren van (administratieve en logistieke) processen en het verwerking van gerelateerde data. Het wordt uitgevoerd met behulp van computers. Voorheen waren dit mainframes, tegenwoordig zijn het (verbonden) personal computers en ondersteunende server applicaties, waarbij data vaak worden bijgehouden in de cloud. Op de computers draaien applicaties die met elkaar verbonden zijn, vaak door het uitwisselen van data.

De besturing van de machines en systemen wordt digitaal uitgevoerd. Industriële automatisering wordt uitgevoerd met controllers, zoals programmable logic controllers (PLCs) [17] en industriële PCs (IPCs) die delen van processen of machines besturen. PLCs zijn van oudsher goed in het besturen van (productie)logica, zoals Aan-Uit schakelingen in sequentiële (proces)stappen. PLCs komen we bijvoorbeeld tegen in de bagagebanden van Vanderlande en in de attracties van de Efteling. PLC bevatten steeds vaker internet verbindingen.

Naast PLC, IPC zijn er ook nog grotere gedistribueerde controle systemen (DCSs) die grotere eenheden aansturen en die ook nog gedistribueerd werken: DCS zijn gekoppeld via een control bus en werken als een geheel, hoewel ze vaak niet op dezelfde locatie staan.

Alle, PLCs, IPCs en DCSs sturen één of meerdere productie processen, de zogenaamde ‘plant’ (fabriek), aan. Er worden sensoren gebruikt om te registreren wat er in het productie proces gebeurt. De PLCs dienen ook als input om actuatoren correct in te stellen (proces control). In de plant worden sensoren gebruikt om te registreren wat er in het productie proces gebeurt of om de status van de machine bij te houden, bijvoorbeeld toerental of temperatuur. Verder worden er actuatoren gebruikt om de plant aan te sturen, bijvoorbeeld door motoren in een bagage band aan te sturen of kleppen open/dicht te sturen.

Om het te automatiseren proces op een hoger abstractieniveau te beschrijven worden vaak nog andere niveaus onderkent, zoals een supervisor (opzichter), die zgn.

[16] In samenwerking met Jules Vos (TNO), mei 2019.

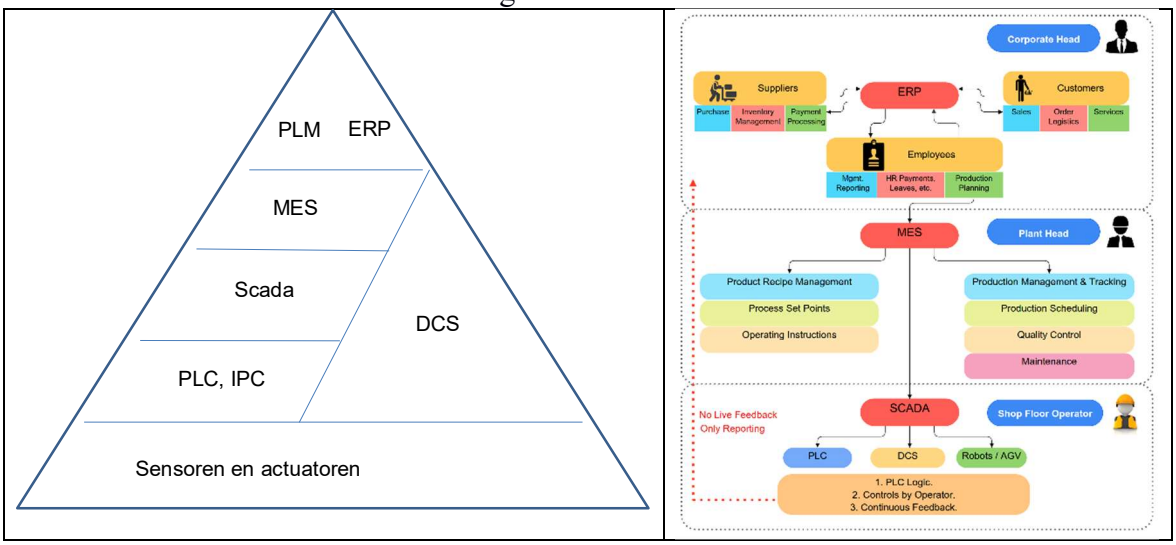
[17] https://www.at-automation.nl/plc-programmable-logic-controller/.

supervisory control uitvoert (Wonham, 2010), waarbij dan vervolgens ook de data van het productieproces een rol spelen. Dit wordt vaak aangeduid als Supervisory Control and Data Acquistion (SCADA). Het doel van SCADA is het samenbrengen van procesdata en de aansturing van PLC's en IPCs, waarbij verschillende merken en typen kunnen gecombineerd worden. Het samenbrengen van data en controllers in 1 omgeving helpt bij diverse besturingsfuncties, zoals monitoring, bedieningen, data archivering en trendanalyses. Daarnaast kan bijvoorbeeld slim alarm management, optimalisatie van applicaties (advanced control) en het toesnijden van data op specifieke gebruikersgroepen worden toegepast.

De data die het SCADA niveau gebruikt zijn vaak weer afkomstig uit bovenliggende niveaus/systemen, zoals het Enterprise Resource Planning (ERP) en het Production Logistic Management (PLM) system. Tussen ERP en PLM aan de ene kant en SCADA aan de andere kant kan er een Manufacturing Execution System (MES)[18] worden ingezet voor het aansturen van continue (fabricage) processen. De 'plant' wordt bestuurd door een PLC/SCADA combinatie, productie wordt aangestuurd (en geoptimaliseerd) door MES.

Parallel aan SCADA kan ook een gedistribueerde controle systeem (DCS) worden geplaatst. Het DCS werd ontwikkeld voor (complexe) regeltechniek, dus bijvoorbeeld voor het traploos schakelen (tussen 0 en 100%) van een klep of motor. PLCs en DCS controllers gaan steeds meer op elkaar lijken. Gedistribueerd wil zeggen dat het de controller naar het installatie onderdeel toebrengt en de controllers met een control bus verbindt. Dat spaart (veel) bekabeling. Je kunt zelfs een complex gedistribueerd systeem maken waarbij vele kilometers overbrugd worden. Een voorbeeld van een DCS toepassing is het gasveld in Groningen, waarbij tientallen DCS omgevingen (met kleine onbemande controlekamers) koppelen met de centrale controlekamer in Hoogezand[19]. Een DCS is SCADA en PLC in één.

De onderstaande figuur drukt de relaties uit tussen de hiervoor beschreven niveaus in de industriële automatisering.



Figuur 6 **Twee interpretaties over de niveaus in industriële automatisering, links[20], rechts[21].**

[18] ..https://nl.wikipedia.org/wiki/Manufacturing_execution_system.

[19] ..https://www.yokogawa.com/nl/library/resources/references/nederlandse-aardolie-maatschappij-bv-nam-groningen-long-term-glt-project/.

[20] ..Geïnspireerd op figuur uit (ABN AMRO, 2016) https://insights.abnamro.nl/2016/02/industrial-internet-of-things/.

[21] ..http://ategroup.com/ecoaxis-blog/can-iiot-be-the-bridge-between-erp-mes-and-scada/.

De besturing middels industriële automatisering kent een aantal specifieke kenmerken die het verschil met het kantoor domein (deels) verklaren. Dit beïnvloedt de security eigenschappen van de systemen in de Smart Industry.
Eerst worden een aantal karakteristieke verschillen tussen KA en OT genoemd, daarna wordt op specifiekere verschillen ingegaan, waarmee de cyber security benadering ervan een eigen invalshoek krijgt.
OT-systemen zijn **lange tijd in gebruik**. De gemiddelde levensduur van een SCADA/PLC/DCS omgeving is 15 jaar of meer. Dit is heel anders dan in een kantooromgeving.
In de kantooromgeving wordt **beheer**, bv volgens ITIL processen, vaak heel gestructureerd uitgevoerd. In de OT wordt ITIL niet of nauwelijks toegepast. Door de complexiteit en de vereiste beschikbaarheid is er meer een mentaliteit van 'niet aankomen als het niet nodig is, zolang het draait is het goed'. Doordat het geen uniforme omgeving is, en de kennis van systemen vaak bij de leverancier zit en veel minder bij eindgebruikers, wordt het beheer heel anders uitgevoerd. Veel bedrijven besteden beheer uit, via onderhoudscontracten, aan de leveranciers. Dat kunnen vele leveranciers zijn, dus om dat te structureren op een ITIL-wijze, in alle onderhoudscontracten/SLA's met de leveranciers, is een complexe opgave.
Het OT is vaak opgebouwd uit **diverse systemen met specifieke functies**. Het zijn systemen die voor algemene regelingen zorgen, of voor elektrische aansturingen (electronic switchboards), compressoren, generatoren, brandbestrijding, koeling/ventilatie (HVAC), veiligheid, afvalwater etc. Deze lappendeken van systemen, vaak uit verschillende generaties, met verschillende operating systems, waarvan soms ook nog eens weinig kennis is, van verschillende leveranciers, maakt het OT complex. Het is meestal niet, zoals in een kantoor omgeving vaak wel het geval is, een uniforme omgeving.

Nadruk op C-I-A: Confidentiality-Integrity enAvailability). In de kantooromgeving is de volgorde van belangrijkheid over het algemeen C-I-A. Confidentialiteit van data is vaak het meest kritisch. In de OT is dat (nagenoeg) nooit het geval. In bedrijven waar veiligheid het meest belangrijk is, is integriteit van data (en dus ook systeemfunctionaliteit) het belangrijkste zoals bijvoorbeeld in de (petro)chemie. Een functie moet werken als het nodig is, bijvoorbeeld het sluiten van een veiligheidsklep in noodsituaties. Daarna komt beschikbaarheid, want de productie mag minimaal verstoord worden. Dus de volgorde is I-A-C. In bedrijven waar veiligheid niet of minder speelt is beschikbaarheid het meest belangrijk. Data integriteit, bv verkeerde fabricage instellingen waardoor er productkwaliteitsproblemen ontstaan, is daarna belangrijk. Volgorde dus AIC.

Beperkte mogelijkheden tot onderhoud/patching - In de industriële automatisering is sprake van batch en continue productieprocessen. In een continu proces (24/7) is het niet zomaar mogelijk om tijdens het proces onderhoud uit te voeren. Er moet dus een productiestop ingepland worden of er moet een vooraf gepland onderhoudsmoment gebruikt worden om het systeem onderhoud te doen. Productie stops zijn duur en vaak contractueel lastig, en ingeplande onderhoudsmomenten kunnen in tijd ver uit elkaar liggen. Het laden van security patches wordt uitgevoerd tijdens de onderhoudsmomenten en wordt hiermee dus sterk beïnvloed.

Late software upgrades - Van proces computers (PLC,SCADA, DCS etc.) wordt een hoge beschikbaarheid verwacht. Het gevolg hiervan is dat leveranciers van proces

computers niet snel upgrades, met de laatste Windows OS, op de markt zetten. Men werkt defensie en loopt ongeveer 1-2 jaar achter op besturingssysteem ontwikkelingen. Er wordt afgewacht totdat de kinderziektes uit een OS zijn verdwenen, voordat een upgrade wordt uitgebracht. Zo heeft men ook meer tijd om upgrades te ontwikkelen en te testen. Betrouwbaarheid mag er nooit onder lijden. Er wordt alleen nieuwe release gedaan als alles goed is getest. In enkele gevallen hebben leveranciers OS-versies overgeslagen. Yokogawa DCS is bijvoorbeeld van Windows7 naar Windows10 gegaan. Windows 8 vond men niet stabiel genoeg.

Upgrades van proces computer zijn over het algemeen **duur en complex**, in tegenstelling tot de meeste vervangingen in de kantooromgeving. Dit heeft een aantal oorzaken:

a. Productiestops kosten vaak veel geld omdat er dan meerdere dagen, of soms langer, niet geproduceerd wordt
b. Er kunnen compatibiliteitsproblemen ontstaan met de controllers (PLC, DCS controller) waardoor de connectie tussen controller en beeldschermstation, proces data collector of verbinding naar een andere domeinen niet meer werkt waardoor bijvoorbeeld nieuwe processorkaarten aangeschaft en geïnstalleerd moeten worden
c. Kosten kunnen hoog zijn door nieuwe software licenties van PLC/SCADA/DCS leveranciers, inhuur van specialistische engineers, nieuwe configuratie doordat niet alle software *upward compatible* is

Een upgrade van een DCS of SCADA omgeving kan in de miljoenen euro's lopen exclusief productieverliezen. Door de hoge kosten van het up-to-date houden van systemen bestaan er nog altijd veel systemen in de OT wereld waarvan de **'beveiliging over datum'** is en die dus niet meer goed beveiligd zijn door een up-to-date OS, zoals Windows XP, NT, W7 of Windows CE.

Fysieke impact – Het feit dat in de industriële automatisering machines, zoals rondrijdende robots en snijmachines worden aangestuurd bepaalt dat de fysieke impact bij IA anders is dan bij kantoorautomatisering. Immers de robot kan mensen aanrijden, de snijmachine kan dichtslaan en mensenhanden eraf snijden. Dit maakt veiligheid (E: safety) een belangrijke kwaliteitseigenschap. Het ordelijk verloop van de geprogrammeerde logica in deze machines bepaalt of hun bedoelde functionaliteit wordt uitgevoerd. Beveiliging (E: security) kan van invloed zijn op de geprogrammeerde logica: door het omzeilen van de beveiliging kunnen kwaadwillende of onbewust onbekwame mensen de machine op een andere wijze gebruiken dan bedoeld. Zo kunnen veiligheidsrisico's ontstaan. Beveiliging is daarmee van invloed op veiligheid. Als een robot niet voldoende secure is dan is deze mogelijk ook niet safe.

De **verbondenheid van machines** in de industriële automatisering maakt dat er afspraken over communicatie moeten worden gemaakt. Hiervoor worden verschillende standaarden gebruikt. Zo zijn er inmiddels machine-to-machine (M2M) standaarden ontwikkeld, die helpen bij het realiseren van het zgn. Industrial Internet-of-Things (IIOT).
Een belangrijke taal daarin is OPC-UA voor machine naar machine (M2M) communicatie. OPC –staat voor OLE (Object Linking and Embedding) Process Control, dit is gebaseerd op (D)COM. OPC-UA is de OPC Unified Architecture en is

een verbetering van OPC[22]. Zie voor een introductie[23] en uitgebreidere beschrijving[24]. Bij OPC-UA wordt expliciet aandacht gegeven aan security, zie[25]. OPC-UA is niet de enige manier om machines te verbinden[26], maar wordt door sommigen gezien als de standaard om tussen machines te communiceren.

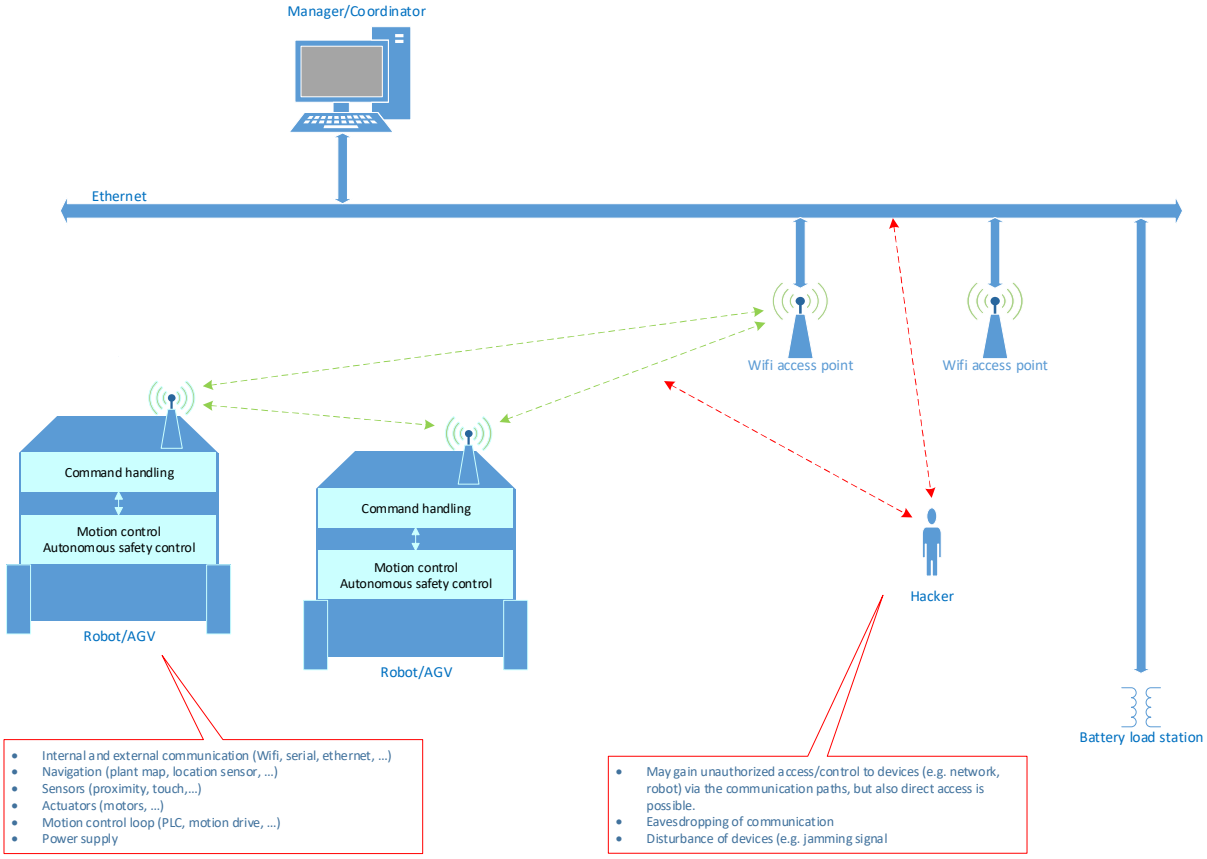
Hiervoor werd bij OT aangehaald dat het vaak diverse systemen met specifieke functies betreft. Dit betekent dat er vaak modulair een OT-systeem wordt opgebouwd uit 'standaard' componenten waarin die onderling samenhangen. Het gaat dan om sensoren, maar ook om actuatoren en de PCs en IPCs, die in de industriële automatisering wordt gebruikt en waarvan de **variëteit en de afhankelijkheid tussen de onderdelen** van grotere invloed is op cybersecurity dan dat in de informatiesystemen wereld het geval is. Deze variëteit geeft uitdagingen voor de fysieke beveiliging in een robot. Het toevoegen van een nieuw device kan de bestaande beveiliging bedreigen. De variëteit in sensoren heeft ook impact op de data afkomstig van deze sensoren. Naarmate er meer, geavanceerde sensoren in robots komen, in samenhang met ongestructureerde toepassingsgebieden, wordt het nog belangrijker aandacht te geven aan de betrouwbaarheid van de data. Aspecten die rondom beveiliging spelen betreffen bijvoorbeeld het onderscheppen van data – bijvoorbeeld d.m.v. een man-in-the-middle attack en de correctheid van de data – wat is de tolerantie van de robot/IA om met onjuiste input om te gaan?

Conclusie:
AGVs zijn een vorm van Operationele Technologie (OT). Hiervoor zijn een aantal specifieke cybersecurity aspecten van OT behandeld. Wij denken dat de volgende OT-aspecten relevant zijn voor AGVs:

1. beperkte mogelijkheden tot onderhoud/patching – als de software op de AGV is geïnstalleerd, worden er geen updates meer gemaakt.
2. fysieke impact – de AGV moet onder controle worden gehouden, om geen fysieke schade te veroorzaken.
3. verbondenheid van machines in de industriële automatisering maakt dat er afspraken over communicatie – AGVs zijn op te vatten als speciale machines – machines op wielen- die worden toegevoegd in het machine netwerk. **Cybersecurity van AGVs kan worden bedreigd als de fysieke- en netwerk toegang wordt bedreigd**.
4. variëteit en de afhankelijkheid tussen de onderdelen – Een AGV wordt, net als andere OT systemen opgebouwd uit sensoren en actuatoren, met daarbij een controlesysteem, zoals PLC of IPC. Bij het programmeren van AGVs wordt veel aandacht besteedt aan het zo juist mogelijk registreren van de omgeving (vaak aanduid als de 'wereld') rondom de robot. Het manipuleren van de sensoren, en het zo bewust foute informeren van de AGV beïnvloed de werking van AGVs negatief. Verder is het correct combineren van de componenten essentieel voor de juiste werking. **Cybersecurity van AGVs wordt bedreigd als sensoren en communicatie tussen de systeemcomponenten verkeerde inputs ontvangen.**

[22] Verbeteringen zijn bijvoorbeeld dat het niet meer gebaseerd is op OLE en DCOM en dat het nu multiplatform (linux, ios, windows ,…) is.
[23] https://www.youtube.com/watch?v=-tDGzwsBokY
[24] https://documentation.unified-automation.com/uasdkhp/1.0.0/html/_l2_ua_node_ids.html
[25] https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Security-Advise-EN.pdf
[26] Bijvoorbeeld INTER-IoT https://inter-iot.eu/

In figuur 7 wordt overzicht van algemene kwetsbaarheden in AGV gegeven. Nu de AGV specifieke cybersecurity aspecten bepaald zijn wordt in hoofdstuk 4 een casus gepresenteerd waarin de cybersecurity van een AGV is geanalyseerd. In hoofdstuk 0 wordt overzicht van interviews met bedrijven gepresenteerd.

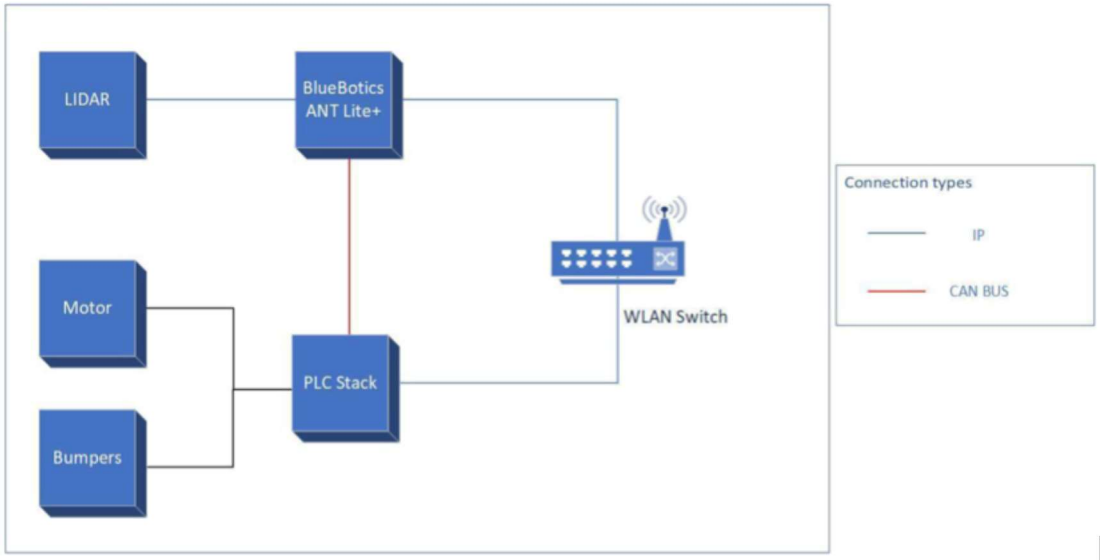


Figuur 7 Overzicht van kwetsbaarheden in AGVs.

4 Bevindingen – Casus AGV producent

Het volgende betreft de resultaten van een *penetration test* die is uitgevoerd door studenten van FHICT bij een producent van AGVs. Het bedrijf wilde weten hoe veilig haar AGVs zijn. De studenten (2e jaar, 4e semester) hebben onder begeleiding van hun docent zelfstandig de *pentest* uitgevoerd. De pentest is in 2017 en 2018 uitgevoerd. Door de vertrouwelijkheid van de informatie wordt het bedrijf hier verder niet genoemd. Met de bevindingen is contact opgenomen met de ontwikkelaar en zijn benodigde beveiligingsmaatregelen opgenomen in de handleiding voor klanten.

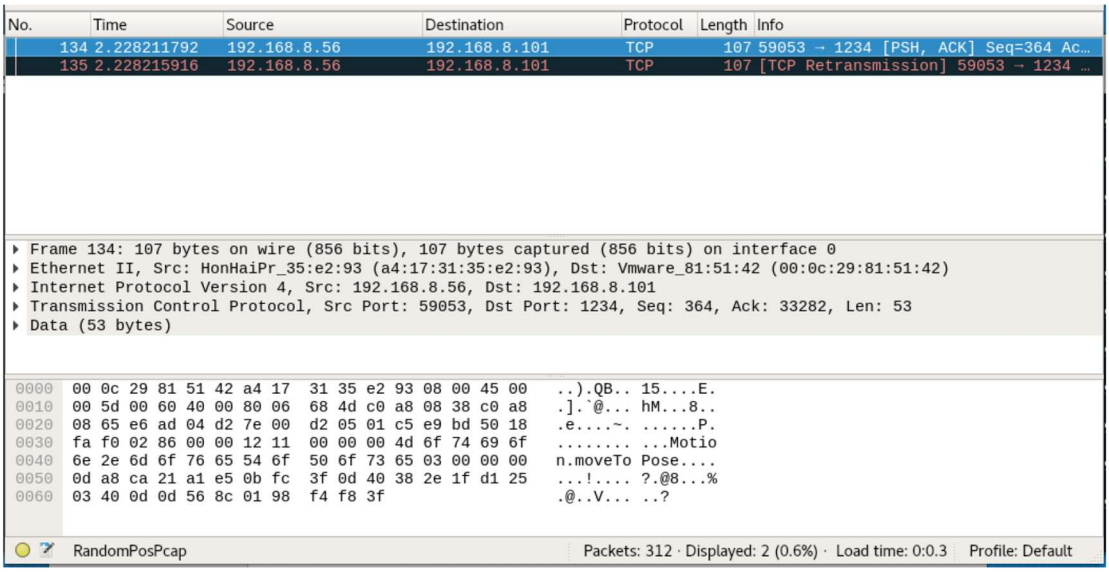
De AGV is een logistieke robot die wordt aangestuurd via zogenaamde fleet manager software. Deze software stuurt de AGV aan met bestemming coördinaten. De AGV heeft op het interne systeem kaarten van de omgeving om de route naar het coördinaat zelfstandig te kunnen bepalen. Ook zijn er safety systemen, bumpers en een licht radar (LiDAR) die er voor zorgen dat de AGV onderweg niet tegen objecten of mensen aan kan botsen. De interne hardware architectuur van de AGV is weergegeven in de figuur hieronder.



Figuur 8 **Interne hardware architectuur van de AGV.**

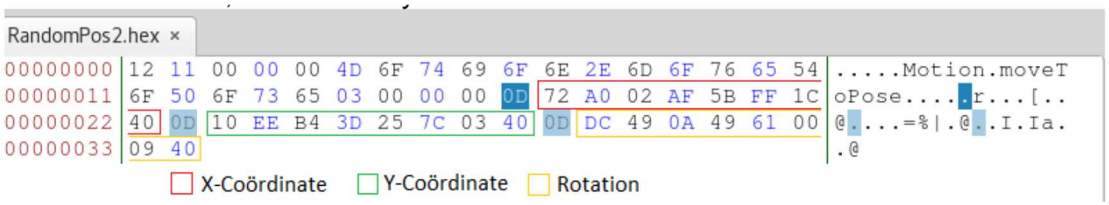
Bij het testen zijn meerdere ernstige kwetsbaarheden gevonden. Samenvattend is de AGV door onbeveiligde communicatie van buitenaf aan te sturen door een aanvaller die toegang tot het netwerk weet te verkrijgen, worden er onveilige protocollen als ftp en telnet gebruikt waardoor er toegang tot het interne systeem mogelijk was, en bevat het systeem componenten die het aanvalsoppervlak vergroten. Ook waren Denial of Service (DoS) aanvallen mogelijk.

Onbeveiligde communicatie. De communicatie tussen de fleetmanager en de AGV was volledig onbeveiligd. Er werd geen encryptie en geen authenticatie gebruikt. Hierdoor was het mogelijk om valse bestemming coördinaten te injecteren en de AGV naar willekeurige locaties te laten rijden. Onderstaande screenshot van een netwerk capture laat een niet versleuteld bericht zijn met daarin leesbaar een Motion.moveTo commando. De vervolgdata zijn vervolgens wel op een in eerste instantie onleesbare manier gecodeerd, maar niet versleuteld.



Figuur 9 **Onversleutelde aansturing van de AGV vanuit de fleetmanager software.**

Met enig giswerk bleek de aansturing te bestaan uit een x-coördinaat, y-coördinaat en een rotatie zoals in de figuur hieronder aangegeven. Dit bleken hexadecimaal weergegeven 64-bit double waardes te zijn.

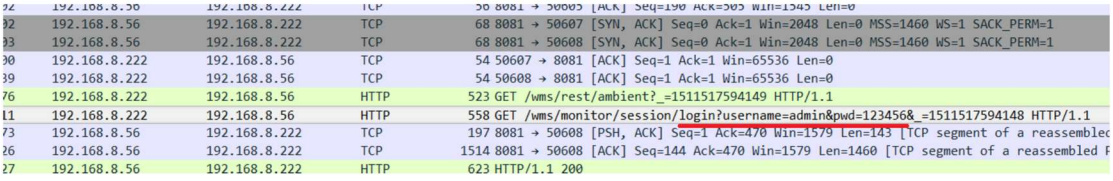


Figuur 10 **Coördinaten in AGV aansturing.**

Met behulp van eenvoudige scripts kon vervolgens de AGV naar willekeurige locaties gestuurd worden. Hiermee kan bijvoorbeeld het logistieke proces waar de AGV onderdeel van is belemmerd worden, of kan de AGV gestolen worden.

Buiten dit voorbeeld van de aansturing van de AGV zijn er ook andere commando's mogelijk om kaartinformatie aan te passen of te verwijderen, missies toe te voegen of te verwijderen, en statusinformatie door te geven.

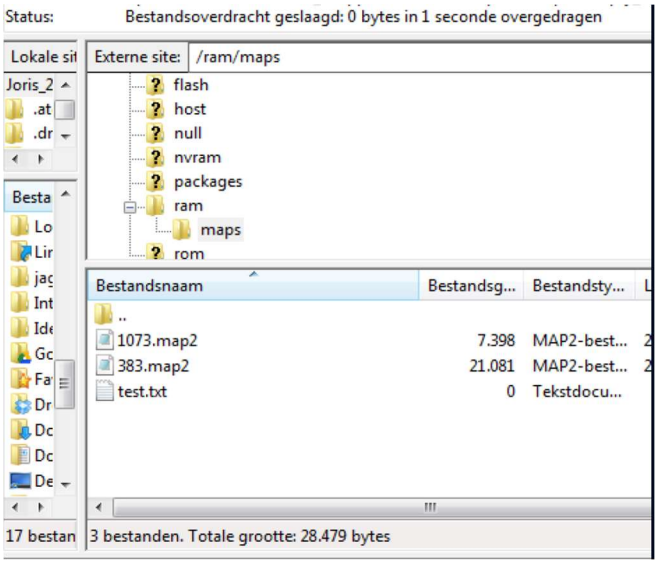
Voor toegang tot de fleet manager software was wel een wachtwoord nodig. Dit erg onveilige wachtwoord werd echter onversleuteld over het netwerk gecommuniceerd zoals te zien is in de screenshot beneden, waardoor een aanvaller op het netwerk deze af kan luisteren en vervolgens toegang tot de fleetmanager software te krijgen.



Figuur 11 **Onversleutelde authenticatie tot de fleetmanager software.**

Onveilige protocollen. Toegang tot het interne systeem is mogelijk via ssh, telnet, en ftp. Telnet en ftp staan bekend als onbeveiligde protocollen. Ook hier zijn benodigde

wachtwoorden af te luisteren en kunnen wachtwoord aanvallen worden uitgevoerd. Telnet toegang is verkregen na een wachtwoordaanval. Via deze systeemtoegang waren echter geen kwalijke vervolgstappen mogelijk. In de figuur hier onder is te zien dat na ftp-toegang toegang tot kaartbestanden is. De AGV kan hiermee dus een ander beeld van de omgeving gegeven worden.



Figuur 12 **FTP verbinding met de AGV met de kaart bestanden zichtbaar.**

Onnodige componenten. Bij het scannen van de AGV werd ook een openstaande poort 80 gevonden. Hier waren twee webpagina's te vinden, die gehost werden door een interne webserver component. Beide webpagina's en de interne webserver blijken geen bekende functie hebben voor de AGV. Deze onnodige functionaliteit vergroot dus onnodig het aanvalsoppervlak en de kans op exploiteerbare kwetsbaarheden op de AGV, waardoor een aanvaller toegang zou kunnen krijgen tot het systeem.

Wat nader onderzoek nog uit zou moeten wijzen is of de safety systemen op de AGV gecompromitteerd zouden kunnen worden. Het gaat hierbij om bumper systemen en een licht radar (een zgn. LiDAR) die ervoor zorgen dat de AGV niet tegen objecten of mensen aan kan rijden.

Denial of Service aanval. Door een zogenaamde man-in–the-middle aanval uit voeren op het netwerk kon de communicatie tussen de fleet manager en de AGV geblokkeerd worden waardoor de AGV niet meer functioneerde zoals bedoeld.

De opbrengst van de security testen is dat er inzicht is verkregen in de security gerelateerde kwetsbaarheden van de AGV. Deze kwetsbaarheden zijn doorgegeven aan de ontwikkelaar om deze op te lossen. Als maatregel tegen onnodig openstaande poorten is de toegang tot deze poorten geblokkeerd op de wireless router die onderdeel is van de AGV. Ook zijn richtlijnen handleiding voor klanten. Hierbij is gewezen op het belang van netwerkscheiding en het gebruik van sterke wachtwoorden. Deze security test laat dus aan de ene kant zien welke zwakheden er voor kunnen komen op een AGV systeem. Het laat ook zien dat het de integrator en de klant helpt om tot een veiligere situatie te komen.

5 Bevindingen – Interviews met bedrijven

Dit hoofdstuk presenteert de bevinden van interviews die we hebben gevoerd met een aantal bedrijven rondom de cybersecurity van hun AGV. Soms is hier ook breder dan de AGV, ook naar Operationele Technologie/Smart Industry gekeken. Het doel van de interviews is om de stand van zaken rondom cybersecurity bij een groep bedrijven met verschillende rollen te inventariseren, om zo een vergelijking te kunnen maken. Er is gevraagd naar risico's, kwetsbaarheden, en maatregelen.

Voor het onderzoek zijn we geïnteresseerd in de rollen. De bedrijven kunnen worden ingedeeld naar 3 rollen, namelijk:

- component leveranciers – maken een onderdeel van een AGV, 1 bedrijf geïnterviewd. Component leverancier wordt met C aangeduid, dus C1.
- integratoren – stellen een AGV of OT-onderdeel samen, 4 bedrijven geïnterviewd. Integratoren worden met I aangeduid, dus I1, I2, I3 of I4.
- (eind)gebruiker – gebruiken het geïntegreerde systeem; 1 bedrijf geïnterviewd. Gebruiker wordt hieronder met G aangeduid, dus G1.

De interviewresultaten worden geanonimiseerd gepresenteerd. Dit omdat de meeste bedrijven niet wilden dat bedrijfsnaam gekoppeld wordt aan de uitspraken rondom security.

De interviewverslagen worden dan ook niet gepresenteerd. In alle gevallen betreft het bedrijven die een vestigingsplaats in Zuid Nederland hebben en die alle OT-producten leveren of onderhouden. De interviews zijn tussen september 2018 en april 2019 gevoerd. De geïnterviewden zijn open bevraagd. Pas achteraf is de er door de interviewer(s) een mate van relevant zijn (op schaal van 1 (relevant) tot 3 (sterk relevant) aan toegekend.

De gevoerde interviews geven het volgende overzicht van factoren die vertegenwoordigers van de bedrijven noemen als hen wordt gevraagd naar de factoren die volgens hen de security van AGVs beïnvloed.

		C1	I1	I2	I3	I4	G1
A	Niet veilig geconfigureerde systemen		3	3	1		3
B	Geen goede scheiding tussen IT en OT	3		3	1		3
C	Geen updates, geen patches, dus verouderde software	3	3	3			1
D	Geen of gebrekkige authenticatie	3	3	1			1
E	Geen beveiligde communicatie		3	3	1		1
F	Verantwoordelijkheid IT en OT	3		3	1	3	1
G	Geen monitoring				1	1	
H	Geen vulnerability scanning (patch management)				3	1	
I	Asset management – overzicht IT/OT				3		

Tabel 3 **– Factoren die security AGVs beïnvloed (interview resultaat).**

Interpretatie – De meeste geïnterviewden benadrukken de verantwoordelijkheid van IT en OT (factor F), die in het licht van minder goede scheiding tussen IT en OT (factor B) logisch lijkt. Dit betreft organisatie. De andere factoren betreffen meer technisch aspecten, zoals dat systeem niet veilig geconfigureerd wordt of dat er geen update worden gemaakt. Er is niet duidelijk één factor aan te wijzen die als dé zwakke schakel wordt gezien. Alle factoren worden daarmee geïnterpreteerd als relevant voor de security van AGVs.Verder is er niet een duidelijk onderscheid van de factoren naar de rollen (C, G of I) te maken.

Richtlijn – voor de beveiliging van AGVs zijn de volgende factoren van belang:

- **Besteedt voldoende aandacht aan:**
  - **het configureren van de AGV(s)**
  - **authenticatie van de AGV(s)**
  - **beveiliging van communicatie tussen AGV(s) en netwerk**
  - **monitoren van het gedrag en netwerkverkeer rondom de AGV(s)**
- **Zorg voor een goede scheiding tussen IT en operationele technologie, en zorg voor goede afstemming tussen beide.**

Hieronder volgen relevante details die in de interviews zijn genoemd[27].
Risico's voor de security van AGVs:

- Beinvloeden van sensoren. Wordt al grotendeels afgevangen in AGV systemen zelf door het combineren van input van sensoren en stilleggen van de AGV bij tegenstrijdigheden in waargenomen signalen. Genoemd door C1.
- Gebruik van open standaarden en toepassing van mogelijk minder geschikte technieken voor productieomgevingen. Genoemd door C1.
- Nieuwe functionaliteit waarbij productieomgevingen (op Fleet Manager niveau) direct aan cloudomgevingen (MS Azure, Amazon) worden verbonden. Genoemd door C1.
- Toename gebruik van meer mainstream OS-en als Windows binnen AGV systemen Dit in tegenstelling tot meer embedded system specifieke OS-en als Realtime Linux. Genoemd door C1.
- Dataontsluiting. Genoemd door I.

Kwetsbaarheden voor AGVs:

- Communicatie tussen Fleetmanager en AGV. Dit gebeurt of 'plain-t' direct via ethernet, of (steeds vaker) via een SSL verbinding. In de AGV zelf wordt voornamelijk gecommuniceerd direct via ethernet (eigen, niet beveiligde protocollen) en in sommige gevallen via CAN Bus. Genoemd door C1.
- Updates worden in de praktijk pas uitgevoerd wanneer dit noodzakelijk is, een niet succesvolle update kan immers verstoring van het productieproces verstoren. Hierdoor worden (security) updates in de praktijk niet of eens in de paar jaar uitgevoerd. Genoemd door C1.

Mogelijke te nemen maatregelen voor het (beter) beveiligen van AGVs :

- Soms wordt uit veiligheidsoogpunt in de AGV handmatig de kabel losgetrokken waarmee van afstand met de AGV verbonden wordt om de kans op beïnvloeding van buitenaf te verkleinen. Genoemd door C1.
- Omdat de AGV een eigen fysiek netwerk heeft, dat gekoppeld is aan het eigen netwerk van de Fleetmanager, zijn er impliciete grenzen van verantwoordelijkheid. Deze grenzen zijn niet expliciet zo met elkaar afgesproken. Genoemd door C1.
- *Security-by-obscurity* in de vorm van eigen, niet open, protocollen. Niet zozeer uitstaan uit dat oogpunt, meer uit het vergroten van de kans dat een klant opnieuw hardware van dezelfde leverancier aanschaft in plaats van hardware van verschillende leveranciers te combineren. Genoemd door C1.

[27] Deze zijn m.n. afkomstig uit interview met Component leverancier. Tijdens interviews met de andere rollen zijn minder details genoemd. Hier zou aanvullend kunnen worden gevraagd.

- Bij referentie architectuur, worden in de keuzes wat betreft OS ook security aspecten meegenomen. Genoemd door I4.
- Nieuwe protocollen openCOA, MQTT (met TLS) hebben authenticatie en encryptie mogelijkheden. Genoemd door I4.
- Bij dataontsluiting en datakoppelingen[28] wordt authenticatie en encryptie expliciet meegenomen in ontwerp en implementatie. Genoemd door I4.
- Security als eis vanuit de klant komt vooralsnog alleen van hele grote klanten. Kleinere klanten hebben veel minder security besef en stellen vaak geen security eisen en leggen de focus op performance, real-time werking, en robuustheid. Int4Awareness presentatie voor medewerkers waarin aanvalsscenario's besproken worden om bewustwording van security te verhogen. Genoemd door I4.

Maatregelen die niet als optie worden gezien voor het beveiligen AGVs:
- Maatregelen die de productie zouden kunnen verstoren/vertragen (virusscanners, IPS,...).
- Monitoring wordt niet toegepast binnen de AGV omgeving.

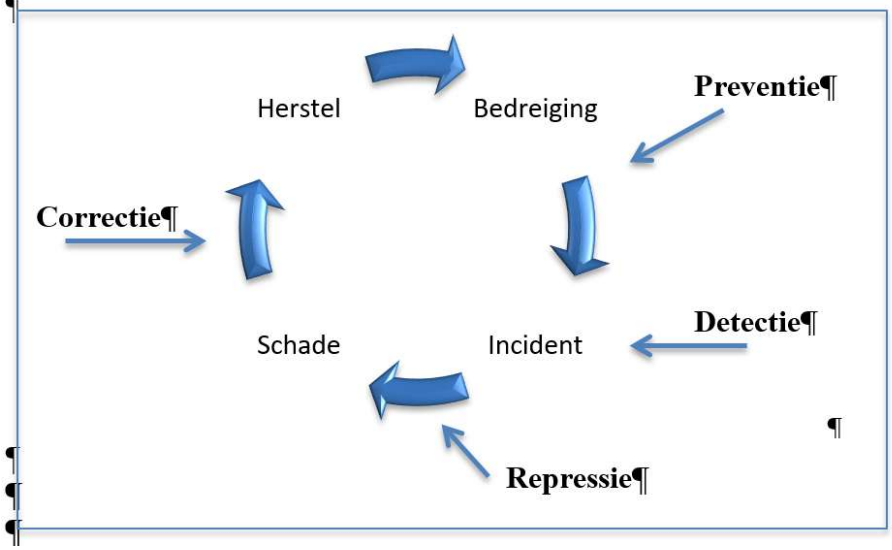
De bevindingen in de interviews zijn te koppelen aan best-practices om tot een goede aanpak van security te komen. Hiermee kunnen de in dit hoofdstuk genoemde risico's en kwetsbaarheden gemitigeerd worden en de reeds genoemde maatregelen breder worden belicht. Deze aanpak wordt in het volgende hoofdstuk besproken.

[28] ..Voorbeeld huidige ontwikkelingen datalake in relatie tot industry 4.0

6 Een aanpak voor robot security

Aan de hand van de hiervoor in kaart gebrachte bedreigingen en kwetsbaarheden in industriële omgevingen, zie hoofdstuk 3, kunnen we security maatregelen benoemen. We maken hierbij gebruik van standaarden rondom industriële security. Ook kunnen we leren van en vergelijken met standaarden rondom IT security. In deze sectie wordt een overzicht van typen maatregelen en maatregelen zelf gegeven vanuit hiervoor bestaande standaarden. Voor deze maatregelen wordt vervolgens een analyse en advies gegeven.
Security maatregelen kunnen worden ingedeeld naar hun werkgebied op verschillende manieren. Naar het werkgebied in de incidentcyclus: preventieve, detectieve, repressieve, en correctieve maatregelen. Naar het werkgebied in de laag van de operationele bedrijfsomgeving: fysieke maatregelen, technisch en/of operationele maatregelen, en organisatorische maatregelen. Organisatorische maatregelen worden ook wel opgedeeld in deelgebieden zoals compliance, procedureel, beleid (policy), awareness.

Wij leggen in dit onderzoek de focus op preventieve en detectieve technische maatregelen, maar benoemen ook de relevante organisatorische maatregelen. Fysieke maatregelen zoals het afsluiten van ruimtes laten we in dit onderzoek buiten beschouwing. Ook gaan we niet specifiek in op repressieve en correctieve maatregelen omdat de focus ligt op het voorkomen en het tijdig detecteren van problemen. In dit onderzoek kijken we niet alleen de operationele omgeving omdat we in de keten ook kijken naar ontwikkelaars en integrators van industriële componenten en omgevingen. De verantwoordelijkheid en mogelijkheden liggen namelijk niet alleen bij de eindgebruiker, maar ook bij de andere schakels in de keten.



Figuur 13 **Maatregelen in de incidentencyclus**[29]**.**

Relevante standaarden van security maatregelen zijn de Europese ISO 27001 standaard voor informatiebeveiliging, de wereldwijde ISA/IEC 62443 serie van standaarden voor industriële security, de Amerikaanse NIST publicatie 800-82 “Guide to Industrial Control Systems Security”, de Amerikaanse ICS-CERT Recommended

[29] Geinspireerd op figuur uit (ABN AMRO, 2016) https://insights.abnamro.nl/2016/02/industrial-internet-of-things/

Practices, de Amerikaans SANS / CIS Critical Security Controls, en de Nederlandse NCSC “Checklist beveiliging van ICS/SCADA systemen”.
Waar alle standaarden en checklists van uitgaan is een management *PDCA*-cyclus[30] waarbij risk management als basis dient voor een security programma, zoals ook al benoemd is in de in H2 benoemde richtlijnen (1) Denk in risico’s, en (2) Leg een incident response administratie aan. Belangrijk is om een securitybeleid te formuleren dat ook van toepassing is op de ICS/SCADA systemen en dat er commitment uitgesproken wordt door het senior management (zie de NCSC “Checklist beveiliging van ICS/SCADA systemen”). Er dient securitybeleid te worden uitgewerkt en ingeregeld voor patchmanagement, voor het gebruik van verwijderbare media zoals usb-sticks, en voor het gebruik van mobiele apparatuur zoals laptops en smartphones in de OT omgeving en netwerken. Een goed overzicht van hardware en software *assets* is belangrijk als een basisoverzicht voor zowel organisatorische als technische maatregelen. Ook het belang van security awareness training en een trainingsprogramma wordt in alle standaarden benadrukt.
Technische security maatregelen die standaard zijn in IT-omgevingen kunnen ook worden overwogen voor OT-omgevingen. Denk hierbij aan preventieve maatregelen zoals firewalls en netwerkscheiding, het gebruik van sterke wachtwoorden, veilige systeemconfiguratie, beveiligde communicatie. Qua detectieve maatregelen hebben we het dan over logging en monitoring en intrusion detection systemen (IDS). Een standaard IT security maatregel die niet zomaar inzetbaar is in OT omgevingen is patch-management, ofwel het zeer regelmatig updaten van software met uitgebrachte bug-fixes en nieuwe versies. Dit maakt het belang van andere maatregelen zoals netwerkscheiding en firewall filtering alleen maar groter. Wij zien dit als een geheel van richtlijnen rondom de cybersecurity van AGVs.

In de tabel 4 wordt een overzicht gegeven van security maatregelen. Deze security maatregelen komen uit de genoemde standaarden waarbij de meest typische organisatorische en technische maatregelen zijn opgenomen in de tabel. Voor een aantal van deze maatregelen geven we hieronder een toelichting over hoe deze relevant en inzetbaar zijn voor industriële security of hoe ze zich verhouden tot dezelfde maatregelen in IT-omgevingen.

[30] PDCA: plan do check act (Deming).

Maatregelen	Component leveranciers (C)	Integratoren (I)	Eindgebruikers (G),
Organisatorisch			
Riskmanagement			V
Securityprogramma met PDCA-cyclus			V
Asset Management			V
Vulnerability en Patchmanagement	V	V	V
Beleid gebruik verwijderbare media			V
Beleid gebruik mobiele apparatuur			V
Security awareness en trainingsprogramma	V	V	V
Incident response plan			V
Externe security testen en audits	V	V	V
Security by Design - Secure Development	V	V	
Technisch			
Firewalls en Netwerkscheiding		V	V
Authenticatie en gebruik van sterke wachtwoorden	V	V	V
Veilige systeemconfiguratie en system hardening	V	V	V
Logging en Monitoring	V	V	V
Intrusion Detection Systemen (IDS)			V
Brute Force beveiliging	V		
White- en blacklisting		V	V
Veilig remote beheer	V	V	V
Beveiligde netwerkcommunicatie	V	V	V

Tabel 4 – Overzicht organisatorische en technische security maatregelen.

Asset management, vulnerability- en patchmanagement. Asset management geeft een belangrijk basisoverzicht van de operationele industriële omgeving. Assets zijn de waardevolle of essentiële hard- en software componenten die je in huis hebt en de signalen en data die daarin verwerkt wordt. Voor assets kan een BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) gegeven worden als security requirements. Dit kan als basis dienen voor een secure ontwerp van de omgeving. Technisch kan het actief inventariseren en volgen van assets gebruikt worden om er voor te zorgen dat alleen geauthorizeerde devices toegang krijgen, en ongeauthorizeerde of niet gemanagede devices worden gedetecteerd of toegang wordt ontzegd. Denk hierbij aan het scannen van de relevante netwerkomgevingen: management netwerk waar scada systemen en engineering werkstations op aangesloten zijn, wifi-netwerken waarbij een koppeling naar de industriële omgeving aanwezig is. Mechanismen als whitelisting en technologie als software certificaten kan hier eventueel bij ingezet worden. Bij het scannen van netwerkomgevingen kan ook real-time of periodiek in de gaten gehouden worden of alle softwarecomponenten

up-to-date zijn. Hiervoor zijn vulnerability scanning tools beschikbaar. Ook kan hierbij gekeken worden naar onnodig openstaande poorten op aangesloten systemen. Zoals in hoofstuk 3 reeds besproken is, kan patchmanagement binnen een OT omgeving niet altijd zomaar tijdig of volledig worden uitgevoerd. Denk aan industriële opstellingen die 24/7 moeten doordraaien, en het niet beschikbaar hebben van een testomgeving om te testen of een update geen neveneffecten heeft. In testen viel ook op dat patches niet altijd verstrekt worden door ontwikkelaars van componenten en software. Dit is een zeer kwalijke zaak omdat nu eenmaal als stelregel geldt dat alle software regelmatige updates behoeft. Een aanvaller of malware kan anders te makkelijk op zoek gaan naar kwetsbaarheden en deze uitbuiten.
Ons advies is om assets in kaart te brengen, bewust met moeilijk te patchen componenten om te gaan, dit in het security en patchbeleid expliciet te maken, en bewust na te gaan of de risico's via andere maatregelen afdoende worden afgedekt. Advies aan ontwikkelaars van OT componenten en software is om voor regelmatige updates te zorgen. Bij aankoop van systemen kan dit als selectiecriterium worden gehanteerd en/of eisen rondom beschikbaar stellen van updates kunnen richting leveranciers en ontwikkelaars worden geuit. Een vaak gehoorde opmerking is dat update management niet mogelijk is omdat downtime van de OT-omgeving niet mogelijk is en er geen testversie is van een OT omgeving is om negatieve effecten van updates uit te kunnen sluiten. Als niet alle systemen geupdate kunnen worden is het belang van vulnerability management om in ieder geval overzicht te hebben van de aanwezige kwetsbaarheden. Hierbij zijn daarmee ook andere maatregelen zoals netwerkscheiding en firewall filtering, en security monitoring van groot belang. Ook adviseren wij, met het toenemende belang van security, om te onderzoeken of een gestubte teststraat (bestaande uit PLCs en software met gesimuleerde I/O) niet toch tot de mogelijkheden behoord. Met een teststraat en korte onderhoudswindows is (gedeeltelijk) updatemanagement misschien toch haalbaar.

Beleid gebruik verwijderbare media en mobiele apparatuur. Een bron van datalekken, malware en kwetsbaarheden zijn verwijderbare media en mobiel apparatuur. Deze kunnen, als hier geen beleid voor wordt gehanteerd, toegang krijgen tot de industriële omgeving zonder hier via aanwezige screening- en authenticatie mechanismen toezicht op te houden. Denk aan een smartphone op het wifi-netwerk, een engineering laptop die aangesloten wordt op een industriële netwerkomgeving, of ongecontroleerde usb-sticks die ingeprikt worden op systemen in de industriële omgeving. Ons advies is om hier een beleid voor op te stellen, na te gaan welke uitdagingen hierdoor ontstaan om deze vervolgens bewust aan te kunnen pakken.

Security testen en audits. Waar steeds meer bedrijven kiezen om hun IT-omgeving regelmatig (bijv. jaarlijks) te laten testen op security tekortkomgingen lijkt dit in OT-omgevingen nog minder gebruikelijk. Omdat hiermee nu juist de blinde vlekken, de vergeten configuraties en gemiste systemen, gevonden kunnen worden is ons advies om een jaarlijkse security test van de OT omgeving te laten uitvoeren. Zelfs een korte test door een externe partij kan de meest gevaarlijke tekortkomingen blootleggen zodat deze om te beginnen bekend zijn en vervolgens kunnen worden verbeterd.

Firewalls en netwerkscheiding, en veilig remote beheer. De OT omgeving moet vaak verbonden zijn met de IT omgeving. Met de opkomende aandacht voor datagebruik in smart industry zullen deze verbindingen verder toenemen. Het

helemaal (fysiek) scheiden van IT en OT is ook vanuit security oogpunt niet verstandig omdat er dan juist onveilig management van de omgeving kan ontstaan. Remote beheer van omgevingen moet bijvoorbeeld mogelijk zijn, maar wel op een goed beveiligde manier. De essentie van netwerkscheiding is om het ingaand en uitgaand verkeer strikt te reguleren. Dit kan via firewalls. Vaak is er weinig tot geen uitgaand verkeer vanuit een OT netwerk en is precies te definiëren welk verkeer er wel in- en uit het OT netwerk gaat. De netwerkfiltering kan dus zeer precies worden ingeregeld op type verkeer (protocol), hierbij gebruik makend van whitelists van bron- en bestemmingsadressen. Input hiervoor kan vanuit assetmanagement komen, zie het eerdere punt hierover. Ons advies is dus niet om koppelingen tussen OT en IT te voorkomen, maar om de koppelingen zo precies mogelijk in te regelen zodat het aanvalsoppervlak beperkt wordt.

Authenticatie, gebruik van sterke wachtwoorden en veilige systeemconfiguratie. Het gebruik van sterke wachtwoorden lijkt logisch. Toch ontstaan in een operationele omgeving makkelijk onveilige wachtwoorden. Dit kan komen doordat meerdere mensen wachtwoorden van bepaalde systemen moeten weten, omdat testwachtwoorden onveilig worden gekozen en niet meer worden aangepast, en omdat default wachtwoorden niet worden aangepast na het opzetten van een nieuwe omgeving. Een wachtwoordbeleid kan hier voor zorgen waarin omgang met, en aanpassing en keuze van wachtwoorden is gedefinieerd en hierop wordt toegezien. Gebruik van wachtwoorden is onderdeel van authenticatie. Qua authenticatie blijkt een extra gevaar dat dit alleen gekoppeld wordt aan gebruikerstoegang, en niet gebruikt wordt bij applicaties of services die aansturing doen binnen de OT omgeving. Hierdoor konden in onze testen signalen geïnjecteerd worden als er eenmaal toegang tot de netwerkomgeving was. Het kunnen injecteren van signalen in een OT-omgeving is uiteraard zeer onwenselijk, dus (veilige) authenticatie moet overal gebruikt worden, niet alleen voor gebruikerstoegang.
Voor veilige systeemconfiguratie, ofwel *system hardening* is ook beleid nodig, maar met daarbij iets meer onderzoek. Voor alle hard- en software in het netwerk moet bewust worden nagegaan hoe deze veilig ingesteld kunnen worden. Hieronder valt ook het weglaten of uitzetten van onnodige functionaliteiten om het aanvalsoppervlak zo klein mogelijk te maken. Zie de gepresenteerde testresultaten waarin onnodige services op een AGV aanwezig waren die ook nog eens onveilig waren geconfigureerd.
Ons advies is hiermee om (1) system hardening mee te nemen in ieder aanpassing in de OT omgeving, (2) om na te gaan of er niet geauthentiseerde toegang is tot assets door andere componenten en software in de OT-omgeving, en (3) om te zorgen voor een wachtwoordbeleid: wie mag welke passwords weten? En een werkwijze om hierop toe te zien.

Encryptie en beveiligde netwerkcommunicatie. Encryptie, ofwel versleuteling zorgt ervoor dat data niet afgeluisterd kan worden, of berichten of signalen aangepast kunnen worden. Een voorbeeld hierbij van afluisteren is dat bij authenticatie over het netwerk zonder versleuteling de gebruikte wachtwoorden van het netwerk afgeluisterd kunnen worden zodra een aanvaller toegang tot het netwerk weet te bemachtigen. Een voorbeeld van het aanpassen is bij signalen en commando's van en naar PLC of betrokken softwarecomponenten. Als deze communicatie niet goed beveiligd is, dan kunnen de signalen en commando's onderweg worden aangepast via een man-in-the-middle aanval, wederom als een aanvaller toegang tot het netwerk heeft. Ons advies

aan leveranciers en aan integratoren is om beveiligde communicatie resp. in te bouwen en in te regelen en onveilige communicatie uit te schakelen dan wel via netwerkscheiding te blokkeren.

Logging, monitoring, en intrusion detection systemen. In IT-omgevingen is security monitoring vrij gebruikelijk. Als basisinput voor monitoring worden log-events van alle hiervoor aangewezen logbronnen gebruikt. Hieronder vallen relevante systemlogs, logging van netwerkcomponenten, en meldingen van security systemen zoals IDS. In OT-omgevingen blijkt dit minder gebruikelijk en is men voorzichtig om aanvullende componenten zoals IDS toe te voegen aan een OT-omgeving omdat men bang is de real-time performance te verstoren. De toegevoegde waarde van monitoring is echter groot, omdat hiermee onzichtbare inbreuken en een aanloop naar een verstoring veel eerder gedetecteerd kunnen worden. Het advies is dan ook om voorzichtige stappen te zetten in de richting van security monitoring en te beginnen met een eenvoudige basismonitoringsomgeving waarin met beperkte inspanning en zonder performance risico's eerste inzichten kunnen worden verworven. Het nut van monitoring kan dan ontdekt worden zonder de real-time performance aan te tasten, en de werkwijze rondom monitoring en benodigde response in geval van detecties kan dan op verantwoorde manier worden opgebouwd. Aanvallen waar bijvoorbeeld relatief eenvoudig op gemonitord kan worden zijn wachtwoordaanvallen, man in the middle aanvallen, en afwijkingen van normale afkomst en bestemming van bepaald verkeer aan de hand van whitelists.

Security management. De maatregelen en benodigde aanpak komen niet vanzelf tot stand. Security zal waarschijnlijk al op de agenda staan bij management overleggen. Mogelijkheden om dit verder vorm te geven zijn om het managementcommitment te expliciteren in een securitybeleid, een responsible disclosure policy te overwegen en een meldpunt voor security meldingen in te regelen. De opzet van een PDCA cyclus zorgt ervoor dat er planmatig met security wordt omgegaan en de aanpak in ieder geval niet aan het toeval wordt overgelaten. Om te beginnen kunnen hierin de bedreigingen, risico's en mogelijk impact worden uitgewerkt en besproken. Daarna kan een security plan worden opgesteld waarin bovengenoemde maatregelen en adviezen worden verwerkt. Het advies voor wat betreft een security management aanpak is om te beginnen met een eenvoudige cyclus en haalbare veranderingen.

Security by Design. Tijdens de ontwikkeling expliciet aandacht geven aan security; in de analyse, in het ontwerp, tijdens de implementatie en bij het testen. Bij de systemen waar we de security van getest hebben was hier geen sprake van. In volwassen softwareontwikkeling wordt dit steeds meer een standaard manier van werken, al zijn er nog geen algemeen geaccepteerde keurmerken die dit naar buiten toe kunnen laten zien. Ook wordt er vaak over Privacy-by-Design gesproken, waarbij de privacy waarborgen expliciet wordt onderzocht en meegenomen in de ontwikkeling. Ons advies aan ontwikkelaars en integrators is om security-by-design in te voeren in de ontwikkelprocessen waarbij in ieder geval in het ontwerp security bedreigingen en maatregelen worden meegenomen. Deze kunnen dan vervolgens in de implementatie worden doorgevoerd aan de hand van best practices en checklists en in testen worden gevalideerd. Ons advies aan afnemers is om security-by-design als standaardeis te hanteren en secure coding technieken toe te passen bij ingekochte systemen en de resultaten uit vulnerability scanning, monitoring en security testen terug te communiceren naar leveranciers en integrators, en hierbij dan om een

oplossing te vragen. Hierbij lopen we wel weer tegen eventuele beperkingen in update management aan, maar het zal in ieder geval nieuwe systemen ten goede komen.

7 Oproep – Vrijheid in gebondenheid

In dit onderzoek hebben we geprobeerd een beeld te schetsen van de security uitdagingen rondom zgn. Automated Guideded Vehicles (AGVs). Dit zijn mobiele robots die in de logistiek, zorg en productie gebruikt worden om goederen indoor te transporteren. AGVs worden al regelmatig gebruikt door Nederlandse bedrijven. We verwachten dat dit nog op grotere schaal gaat gebeuren. De toepassing van AGVs hebben we geplaatst in de context van de ontwikkelingen rondom slimmere machines, de Smart Industry, ook wel aangeduid als Industrie4.0. Daarmee gaat het over Industriële Automatisering, wat in security termen operationele technologie (OT) is.

We hebben een aantal richtlijnen opgesteld voor het veilige (secure) gebruik van AGVs:

1. Leg een incident response team, plan en administratie aan. Door middel van een CSIRT team kan je snel reageren op verstoringen en weet je hoe te handelen volgens het draaiboek. Het vastleggen van welke aanvallen er hebben plaatsgevonden en deze delen met betrokkenen vergroot de toegevoegde waarde van de lessons learned.
2. Denk in risico's – bepaal mogelijke bedreigingen en de impact er van. Voor een dergelijk risk-assessment regelmatig uit. Bepaal daarbij per bedreiging kans (P) en impact (I) en stel daarbij contingenties en mitigaties op.
3. Laat security jaarlijks testen om tijdig ontstane kwetsbaarheden te ontdekken.
4. Zorg voor een goede scheiding tussen IT en operationele technologie, en zorg voor goede afstemming tussen beide.
5. Zie security als een proces, richt een PDCA cyclus in op management niveau.
6. Let op de volgende factoren bij het beveiligen van AGVs (deze zijn genoemd in de interviews, hoofdstuk 5, en verder verwoord in hoofdstuk 6:
    a. Authenticatie en gebruik van sterke wachtwoorden,
    b. Veilige systeemconfiguratie en system hardening.
    c. Logging en Monitoring.
    d. Intrusion Detection Systemen (IDS).
    e. Brute Force beveiliging.
    f. White- en blacklisting, met een voorkeur voor whitelisting[31].
    g. Veilig remote beheer.
    h. Beveiligde netwerkcommunicatie.

Omdat AGVs, en breder: systemen in de Smart Industry, verbonden systemen (connected devices) zijn die door meerdere partijen gebouwd, geïntegreerd en gebruikt worden, en die ook naar elkaar communiceren, denken wij dat meerdere partijen verantwoordelijk zijn voor het de cybersecurity van AGVs in de smart industry? Op basis van de door ons gehouden interviews, zie hoofdstuk 5, zien we dat verschillende rollen (component leverancier, integrator en gebruiker) oog hebben voor security. De interviews laten ook zien dat bovengenoemde factoren, zie bovenstaande richtlijn 6, ook niet op een van de onderkende rollen is terug te voeren. We zien dat ook terug in de casus van hoofdstuk 4, waar de security test laat zien welke zwakheden er voor kunnen komen op een AGV systeem en dat de integrator de eindgebruiker helpt om tot een veiligere situatie te komen.

[31] Blacklisting is mogelijk risicovoller.

Met andere woorden: de rollen zijn alle vrij en functioneren los van elkaar, maar dienen wel met elkaar rekening te houden en elkaar te helpen. Ze zijn wel aan elkaar gebonden.

Tenslotte een korte opmerking over vervolg onderzoek: toepasbaarheid van het communicatieprotocol OPC-UA voor AGVs te onderzoeken. OPC wordt als secure geclassificeerd, maar implementatie / afleidingen ervan hoeven dat niet te zijn. Wat betekent dat voor AGVs? In plaats van AGVs kunnen we dit breder trekken, naar connected devices, IoT.

8 Verantwoording

Dit artikel/rapport is het resultaat van een studie die is uitgevoerd in het kader van het KIEM Cybersecurity van robots in de smart industry project [32]. Het project is uitgevoerd door de auteurs van het rapport: Casper Schellekens, Ron Mélotte, Tom Broumels, Lake Lakeman en Teade Punter.

In onze onderzoeksmethodologie zijn de stappen uit ontwerpgericht onderzoek gevolgd. Hiervoor zijn we begonnen met een probleemstelling. Deze is afkomstig uit een algemene notie dat er een security probleem is met AGVs. De bedrijven Probotics (Henk Kiela) en SigmaKontrol (Lucien Kouwenhoven) hebben deze aanvraag van het lectoraat High Tech Embedded Software van Fontys ICT ondersteund.

In de uitwerking is een case study in de vorm van een penetration test door Fontys ICT-studenten semester 4 van de Cybersecurity bij een bedrijf uitgevoerd , zie hoofdstuk 4.

In het verlengde van deze case study zijn interviews met diverse bedrijven gevoerd, zie hoofdstuk 5. Ook is er veel literatuuronderzoek uitgevoerd, zie bijvoorbeeld hoofdstukken 2 en 6 voor met name standaards en overzichten. Verder is met Egbert-Jan Sol en Jules Vos (TNO) overlegd rondom cyber security op het gebied van het koppelen van security en het industriële automatiseringsdomein, zie hoofdstuk 3.

[32] .. https://www.nwo.nl/onderzoek-en-resultaten/onderzoeksprojecten/i/08/32008.html

9 Referenties

- Bruijne, M. de, Eeten, M. van, Gañán, C.H., Pieters, W. (2017), *Towards a new cyber threat actor typology.* Delft University of Technology. Online beschikbaar: https://www.wodc.nl/onderzoeksdatabase/2740-categorisering-en-motieven-cyberactoren.aspx Geraadpleegd op 2 juli 2019.
- ENISA (2018), Good Practices for Security of Internet of Things in the context of Smart Manufacturing
  Online beschikbaar: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot Geraadpleegd op 2 july 2019.
- Holland Robotics (2018), Kansen voor de Nederlandse robotica (Position paper). Online beschikbaar: https://www.vraagenaanbod.nl/download/Holland%20Robotics%20Position%20Paper.pdf Geraadpleegd op 21 augustus 2018.
- ISA / IEC 62443, The International Society of Automation,Online beschikbaar: https://www.isa.org Geraadpleegd op 2 july 2019.
- ISO27001, International Organization for Standardization. Online beschikbaar: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en Geraadpleegd op 2 july 2019.
- Kaspersky (2018a), Threat landscape for industrial automation systems. H2 2018. Online beschikbaar: https://ics-cert.kaspersky.com/media/KL_ICS_CERT_H2_2018_REPORT_EN.pdf. Geraadpleegd op 30 mei 2019.
- Kaspersky (2018b), The State of Industrial Cybersecurity 2018. Online beschikbaar: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf. Geraadpleegd op 30 mei 2019.
- Lee, E., S. Seshia (2015), *Introduction to Embedded Systems – A Cyber-Physical Systems Approach*. Berkeley: LeeSeshia.org. ISBN 978-1-312-42740-2.
- NCSC (2018). Towards a new cyber threat actor typology. Online beschikbaar: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html. Geraadpleegd op 28 juni 2019.
- NCSC-checklist beveiliging ICS/SCADA-systemen: https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-checklist-beveiliging-ics-scada-systemen.html
- NCSC (2018). Cyber Security Assessment Netherlands 2018. https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2018/1/cyber_security_assessment_netherlands_2018.pdf
- NIST 800-82: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- Sparc (2016), Robotics 2020 Multi Annual Roadmap for Robotics in Europe. European Horizon. Online beschikbaar: https://www.eu-robotics.net/cms/upload/topic_groups/H2020_Robotics_Multi-Annual_Roadmap_ICT-2017B.pdf. Geraadpleegd op 24 augustus 2018.
- Staggs, E., Cyber-Security attacks. Online beschikbaar: https://www.honeywellprocess.com/library/marketing/presentations/Cyber-Security-Article-Kevin-Staggs.pdf Geraadpleegd op 30 mei 2019.
- Wonham, W.M., (2010). Supervisory control of discrete-event systems – lecture notes Univerity of Toronto, Online beschikbaar: http://www.se.wtb.tue.nl/_media/wonham/wonham_scdes2010.pdf. Geraadpleegd op 9 mei 2019.

10 Begrippenlijst

Het domein van de cyber security en industriële automatisering bevat veel begrippen die worden afgekort. Onderstaande lijst geeft een zo compleet mogelijk overzicht.

AGV	Autonomous Guided Vehicle – een autonome (mobiele) robot die vaak gebruikt wordt om goederen te vervoeren.
aanvalsoppervlak	Het totaal aan ingangspunten van een omgeving waar een aanvaller kan proberen data te injecteren of bemachtigen. Een security principe is om het aanvalsoppervlak zo klein mogelijk te houden.
authenticatie	Authenticatie is het nagaan of een bewijs van identiteit van een gebruiker, computer of applicatie overeenkomt met vooraf vastgelegde echtheidskenmerken.
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid
CERT	Computer Emergency Respons Team
CPS	Cyber Physical System
CSAN	Cyber Security Assessment Netherlands
CSIRT	Computer Security Incident Respons Team
DCS	Distributed Control System
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
FHICT	Fontys Hogeschool ICT
IA	Industriële automatisering
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IPC	Industriële PC
IT	Informatie Technologie
IoT	Internet of Things (IIoT - Industrial Internet of Things)
KA	Kantoorautomatisering
Man-in-middle attack	Afgekort MITM, is een man-in-het-midden aanval waarbij een gebruiker tussen de afzender en de ontvanger van informatie terechtkomt en alle informatie die daarbij wordt verzonden afluisterd.
MKB	Midden- en klein bedrijf
NCSC	Nationaal Centrum Cyber Security
Notpetya	Ransomware afkomstig van de Petya familie die ontdekt is in 2016
OPC-UA	Open Platform Communications - Unified Architecture
OT	Operationele Technologie. De hard- en software die zijn bedoeld voor het detecteren of veroorzaken van wijzigingen in fysieke processen door directe bewaking en / of regeling van fysieke apparaten zoals kleppen, pompen, enz.
Pentest	Penetration test
PLC	Programmable Logic Controller
PLM	Production Logistic Management
Ransomware	Malafide software die computer kan gijzelen, door middel van encryptie.
SCADA	Supervisory Control and Data Acquistion
S7COMM	Een (onbeveiligd) protocol waarvan een Siemens PLC gebruik maakt om te communiceren met andere apparaten
Smart Industry	Nederlandse aanduiding voor Industrie 4.0; https://www.smartindustry.nl/

System hardening	Beveiliging van systeem verhogen
Stuxnet	Een schadelijk computerprogramma wat gebruikt is voor een aanval op een kerncentrale in Iran.
wifi cracking attack	Het kraken van de beveiliging van een wifi verbinding