ProRail

ICS beveiliging ProRail

Ontsluiting en beveiliging van RailInfra assets

Eigenaar ICT – CIO Office
Auteur Thijs Wientjes

Kenmerk IBB-2.30
Versie 1.2
Datum November 2016
Bestand IBB-2.30 Ontsluiting Railinfra assets - Technische requirements v1.2

Status Definitief
Informatieclassificatie Intern

Inhoudsopgave

Versiebeheer		
Versie	Datum	Wijziging
0.5	Juli 2016	Eerste concept verstuurd binnen ProRail ter info/review.
0.51	Augustus 2016	- Onderscheid tussen levels en security zones toegevoegd; - Lokale railinfra assets opgenomen in één security zone; - Additionele requirements toegevoegd.
0.8	Augustus 2016	Review commentaren verwerkt.
0.9	Oktober 2016	Aanscherpingen Hans ven der Spek verwerkt
1.2	November 2016	- Per requirement referentie toegevoegd naar de bijbehorende BIV classificatie; - Visualisatie levels vs. security zones in requirement 1 gecorrigeerd; - Sectie 3.4 gecorrigeerd; - Naam “OBI-zone” aangepast naar “Beheerzone”; - Sectie 3.3.1 over scheiding monitoren en bedienen toegevoegd; - Requirements 1.2.4, 1.3 vervallen, en 18 aangepast n.a.v. sectie 3.3.1; - Requirement 1.2.4.1 vervallen; - Requirements 14, 17, 18 en 30 verduidelijkt; - Taalkundige aanpassingen; - Sectie 2.1. aangevuld; - Requirement 6 aangepast; - Requirement 32 gesplitst.

Distributie		
Versie	Datum	Aan
0.5	Juli 2016	Stoffel Bos, CISO
		Jaco Schoonen, Vakdeskundige AM
		IMA team infravoorzieningen
		Architectuurwerkgroep TunnelTechnische Installaties (TTI)
0.51	Augustus 2016	Marco de Heuvel
		Hans van der Spek
		Paul Ram
		Arjan Janssens
		Stoffel Bos, CISO
		Jaco Schoonen, Vakdeskundige AM
		IMA team infravoorzieningen
		Architectuurwerkgroep TunnelTechnische Installaties (TTI)
0.8	September 2016	Stoffel Bos, CISO
		Jaco Schoonen, Vakdeskundige AM
		IMA team infravoorzieningen
		Architectuurwerkgroep TunnelTechnische Installaties (TTI)
		Marco de Heuvel
		Hans van der Spek
		Paul Ram
		Arjan Janssens
		Ron Bosch
0.9	Oktober 2016	Stoffel Bosch, CISO
		Hans van der Spek
1.2	November 2016	Stoffel Bos, CISO

1 Introductie

1.1 Achtergrond

Op dit moment wordt binnen ProRail het oude Asynchronous Transfer Mode (ATM) netwerk uitgefaseerd omdat deze technologie end-of-life is. Als vervanger is hiertoe een nieuw ICT netwerk aangelegd op basis van Multi Protocol Layer Switching (MPLS) dat een meer open karakter heeft dan het oude ATM netwerk.

Naar aanleiding van de plannen van ProRail om alle railinfra assets via dit nieuwe ICT netwerk (SpoorLAN en Fides) te ontsluiten ten behoeve van centrale monitoring en bediening is begin 2016 geïdentificeerd dat binnen dit meten en sturen domein additionele meetregelen nodig zijn t.a.v. Cybersecurity.

Hiertoe zijn binnen ICT en AM diverse medewerkers meegenomen in een campagne voor security awareness op industriële control netwerken. Naar aanleiding daarvan is besloten de requirements voor het ontsluiten van de railinfra assets verder uit te werken om te identificeren welke additionele maatregelen benodigd zijn.

Dit document beschrijft de technische requirements voor veilige ontsluiting van de railinfra assets naar het ICT netwerk.

1.2 Scope

De scope van dit document richt zich tot de technische requirements aan de industrial control systems (ICS) en onderliggende infrastructuur, als aanvulling/aanscherping op het bestaande ProRail InformatieBeveiligingsBeleid (IBB).

Voor bediening en monitoring van het ICS wordt gebruik gemaakt van software oplossingen die op servers in de ProRail technische ruimtes actief zijn. Hierop zijn vanuit het bestaande IBB al diverse richtlijnen van toepassing (o.a. de server hardening richtlijnen). Dit document vervangt deze richtlijnen niet. Deze richtlijnen blijven van kracht.

Naast de technische inrichting zijn naar verwachting ook aanvullende organisatorische maatregelen benodigd, zoals onder andere:

- Awareness/training van IT en AM personeel;
- Eisen aan cybersecurity awareness/certificering van het personeel van de PCA's;
- Procedures en resources voor opvolging van gerapporteerde alerts;
- Audits van de ICS omgeving om het beveiligingsniveau te evalueren en te spiegelen aan het beveiligingsbeleid;
- Stringent wijzigingsbeleid, inclusief audits om ongeautoriseerde wijzigingen te identificeren.

Nadere beschrijving van deze maatregelen vallen buiten de scope van dit document.

1.2.1 Netwerkinfrastructuur versus systeem

De requirements zijn in principe beschreven als eisen aan het systeem. Binnen het ProRail InformatieBeveiligingsBeleid wordt op dit moment aangegeven dat binnen een netwerkdomein geen oplossingen worden geïmplementeerd voor additionele cybersecurity.

In geval van ICS systemen zijn in veel gevallen echter ook netwerkinfrastructuur-oplossingen benodigd om aan de requirements te voldoen. Deze oplossingen mogen niet per systeem gekozen worden, maar dienen te worden ingezet als collectieve nutsvoorziening binnen de ICS netwerken, en zullen worden bepaald door ICT infravoorzieningen.

1.3 Doel

Doel van dit document is het bieden van een kader met voorschriften waaraan alle ICS systemen die binnen ProRail worden geïmplementeerd moeten voldoen. De voorschriften moeten tijdens het project vertaald worden naar concrete oplossingen in een binnen het project op te leveren technisch detailontwerp.

Daarnaast dienen alle bestaande systemen ook aan dit document te worden getoetst om de veiligheid ook hier op orde te brengen.

1.4 Positionering

Dit document vormt een onderdeel van het stelsel van informatiebeveiliging bij ProRail, en biedt bovenop het generieke beveiligingsbeleid een set specifieke maatregelen voor meet & bediensystemen binnen de railinfra.

1.5 Uitgangspunten

Dit document is inhoudelijk en pragmatisch van karakter, en gebaseerd op wereldwijd erkende good practices en referentiearchitecturen voor beveiliging van ICS systemen, waaronder:

- IEC62443: Network and system security for industrial-process measurement and control
- NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security
- SANS institute: Secure Architecture for Industrial Control Systems

1.6 Leeswijzer

Hoofdstuk 2 geeft een kort overzicht van de ICS specifieke bedreigingen waartegen de Railinfra assets beschermd moeten worden.

In hoofdstuk 3 worden de generieke richtlijnen gegeven die voor alle ICS systemen van toepassing zijn.

In hoofdstuk 4 worden de requirements opgesomd, verdeeld naar de verschillende gebieden van beveiligingsmaatregelen. De requirements worden per stuk gepresenteerd in tabelvorm zoals hieronder.

ID	Requirement	B	I	V
		M	L	-
Rationale				

Per requirement moeten de volgende velden ingevuld worden:

- **ID**
  ID van de requirement in de vorm van een in dit document uniek volgnummer. Daar waar requirements een nadere specificatie zijn van een requirement erboven wordt dit in de nummering aangegeven.
- **Requirement**
  omschrijving van de requirement
- **Rationale**
  Omschrijving van de achterliggende reden waarom deze requirement wordt gesteld.
- **B I V**
  Hier staat aangegeven vanaf welke classificatie een requirement geldig is (Laag, Midden. Hoog):
  - Indien onder één van de B.I.V. aspecten een "-" staat dan betreft het een requirement die onafhankelijk van de classificatie moet worden ingevoerd;
  - Indien een van de B.I.V. aspecten een classificering heeft, dan geldt deze maatregel ook voor de bovenliggende niveaus. Een classificatie ´L´ betekent ook dat deze maatregel geldt voor classificatie ´M´ en ‘H’.
    - Indien meerdere specifieke niveaus zijn aangegeven, is de requirement geldig wanneer één of meer van de aspecten van het systeem een specifiek niveau heeft dat gelijk is aan of groter is dan in de requirement is gespecificeerd.
  - Indien onder één van de B.I.V. aspecten een lege cel staat dan betreft het een aspect dat niet van toepassing is voor de maatregel.

1.7 Referenties

De referenties die als bron voor dit document zijn gebruikt, zijn opgenomen in bijlage B.

2 ICS Cybersecurity

2.1 Waarom een ICS specifiek beleid?

Op dit moment bestaat een ProRail breed informatiebeveiligingsbeleid. Hierin zijn diverse vereiste maatregelen samengevat om met name de vertrouwelijkheid en beschikbaarheid van informatie te kunnen waarborgen, met een sterke focus op de capaciteiten die het systeem hiervoor moet bieden. Voor Operations Technology (OT) systemen is echter een specifieke kijk nodig, omdat hier vertrouwelijkheid minder van belang is, maar beschikbaarheid en integriteit des te belangrijker om de betrouwbaarheid en veiligheid op het Nederlandse spoorwegennet te kunnen waarborgen.

Een belangrijk aspect hierin is dat OT systemen op dit moment nog onvoldoende in staat zijn zichzelf tegen de diverse bedreigingen te beschermen, en dat deze situatie vanwege de lange lifecycle van deze systemen nog voor een lange termijn zal blijven bestaan.

Meer over IT-OT integratie wordt opgenomen in de ICT architectuur 2025.

2.2 Waartegen willen we ons beschermen?

Kortgezegd moet voorkomen worden dat delen van het spoorwegennet onveilig worden of uitvallen, ongeacht of dit door een bewuste aanval of door onzorgvuldig handelen gebeurt. Dit betekent dat bescherming geboden moet worden tegen:

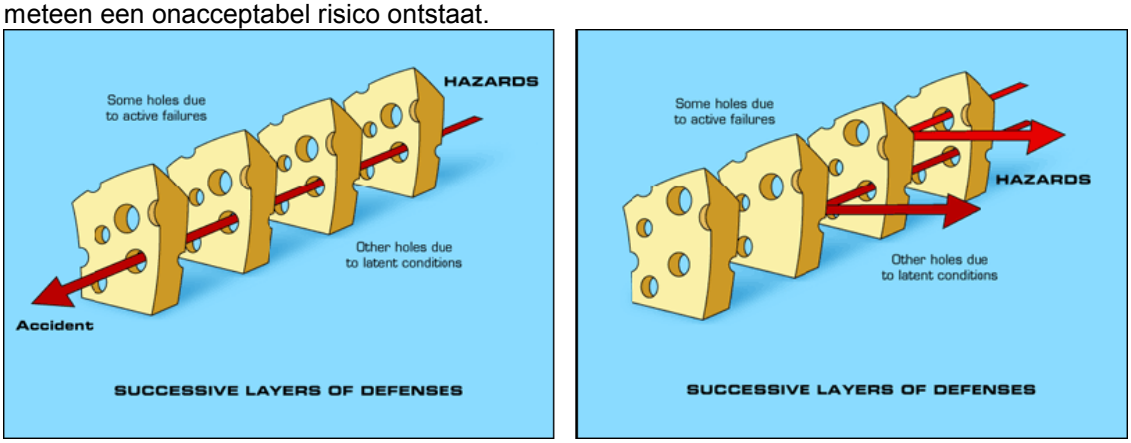
- Verlies of beperking van zicht op of controle over de systeemfunctionaliteit;
- Verlies of beperking van de beschikbare connectiviteit met de systemen;
- Ongeautoriseerde wijziging van parameters, setpoints of systeemconfiguraties;
- Beschadiging of vernietiging van apparatuur (zowel fysiek als softwarematig).

Belangrijk is hier dat ProRail fail-safe systemen heeft ingezet op het spoor, die een onveilige situatie veelal zullen voorkomen. Deze fail-safe systemen bereiken dit echter meestal door delen van de railinfrastructuur stil te leggen. Wanneer dit soort ingrijpen te vaak voorkomt zal dit grote reputatieschade tot gevolg hebben, ondanks het feit dat de fail-safe systemen goed functioneren en menselijk letsel met succes hebben voorkomen.

3 Algemene richtlijnen

3.1 Defense in depth

Voor fysieke veiligheid maakt ProRail gebruik van het Zwitserse kaas model van Reason. Dit model gaat uit van meerdere lagen van bescherming, zodat bij een issue in één laag niet meteen een onacceptabel risico ontstaat.



Figuur 1: Het Zwitserse kaas model van Reason

Dit principe van gelaagde beveiliging moet ook worden toegepast voor beveiliging van automatische systemen. Bijvoorbeeld het beschermen tegen ongeautoriseerd gebruik maken van systeemfuncties. Dit kan als eerste in de ICS software worden gerealiseerd via het instellen van de juiste autorisaties. Worden in de applicatie opzettelijk of per ongeluk ongewenste autorisaties toegekend, dan kan de functionaliteit richting de systemen in het veld op andere lagen alsnog worden geblokkeerd via restricties op systeem- of netwerkniveau.

3.2 Voorschrijven, implementeren, beheren, toetsen

Dit document stelt diverse kaders waaraan zowel ProRail als haar opdrachtnemers moeten voldoen. Dat betekent ook dat iedereen die bij de systemen waarvoor deze kaders gelden betrokken is van deze kaders op de hoogte moet worden gesteld.

Daarnaast moet getoetst worden of aan deze kaders wordt voldaan.

Dit document moet daarom bij aanbestedingen en projecten meegenomen worden. En tijdens het project moeten vakdeskundigen betrokken worden die tijdens de diverse fasen van uitvraag en implementatie op naleving van de in dit document gestelde kaders toetsen.

Daarnaast moet naleving van deze kaders tijdens de operationele fase worden opgenomen in de betreffende dienstenovereenkomsten, zodat ook tijdens de operationele levenscyclus hierop kan worden getoetst en waar nodig actie kan worden vereist.

3.3 Isolatie, separatie

In het landelijke ProRail netwerk zijn diverse ICS systemen actief. Deze systemen bevinden zich verspreid over het land. Om te voorkomen dat door opzet of door onzorgvuldig handelen verstoringen ontstaan of verstoringen zich uitbreiden, is het belangrijk dat systemen en personen die geen interactie met elkaar hoeven te hebben, van elkaar worden gescheiden op systeemniveau. Samengevat zijn er 3 zaken die te allen tijde voorkomen moeten worden:

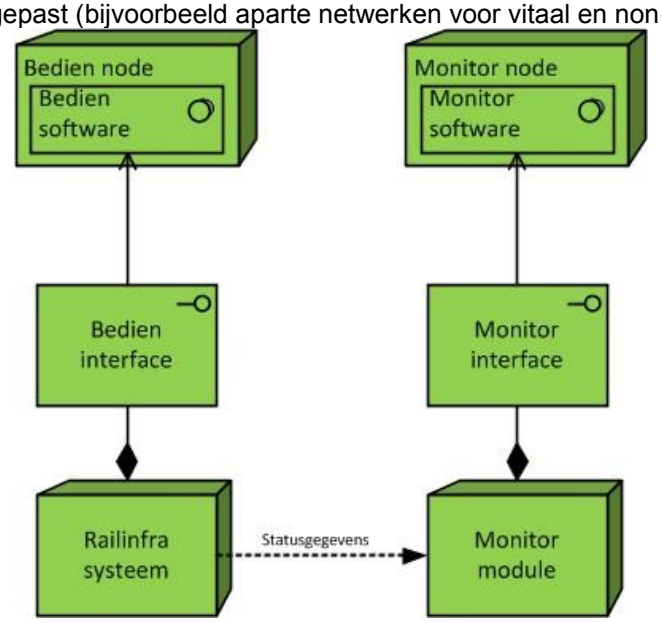
- We moeten voorkomen dat lokale problemen onnodige invloed hebben op assets op andere delen van het landelijke ProRail netwerk;
- We moeten voorkomen dat personen netwerktoegang hebben tot systemen waarvoor zij geen rol vervullen;
- We moeten voorkomen dat systemen netwerktoegang hebben tot systemen waarmee geen interactie nodig is;

- We moeten voorkomen dat onbevoegde personen fysiek toegang hebben tot systemen;
- We moeten detecteren dat onbevoegde personen toegang hebben verkregen of proberen te krijgen tot systemen.

3.3.1 Monitoren versus bedienen

Een bijzonder geval van separatie is de strikte scheiding tussen het monitoren van een systeem en het bedienen van een systeem. De monitoring functie heeft vaak lagere eisen t.a.v. beschikbaarheid en wordt aan een grotere groep mensen beschikbaar gesteld. Dit terwijl de bedienfunctie vaak als vitaal wordt beschouwd, en aan een veel kleinere groep mensen ter beschikking wordt gesteld. Van deze personen worden vaak ook hogere kwalificaties vereist.

In de toekomst zal de scheiding tussen het vitale en non-vitale deel ook in de infrastructuur strikter worden toegepast (bijvoorbeeld aparte netwerken voor vitaal en non-vitaal verkeer).



Figuur 2: Scheiding tussen monitoren en bedienen binnen het systeem

Om die reden moet elk systeem zo ontworpen zijn, dat binnen het systeem deze scheiding al is aangebracht, en dat het systeem hiervoor niet volledig leunt op beveiligingsdiensten vanuit de infrastructuur.

3.4 BIV codering voor kritieke railinfra assets

Voor ICS systemen en de gegevens daarbinnen is het vaak lastig om een BIV (Beschikbaarheid, Integriteit, Vertrouwelijkheid) codering mee te geven voor de gebruikte data. Vaak worden meetgegevens op een sensor bijvoorbeeld niet gezien als te classificeren data. Echter in de praktijk betreft het hier gegevens die door een systeem gebruikt worden om automatisch railinfra assets aan- of bij te sturen. Het is dus erg belangrijk dat deze gegevens beschikbaar en correct zijn. Voor systemen waarvoor geen BIV classificatie is vastgesteld zijn alle requirements in dit document geldig.

Voor systemen waarvoor wel een BIV classificatie is vastgesteld kan aan de hand van de BIV classificatie in de tabel (zie ook de leeswijzer in sectie 1.6) worden bepaald of de requirement in kwestie van toepassing is.

Ook voor veel systemen met lagere eisen zijn veel requirements van kracht. Dit omdat alle systemen moeten voldoen aan de generieke eisen van isolatie en separatie zoals belicht in de sectie 3.3 hierboven.

3.5 Comply or explain

Het kan zijn dat een systeem niet aan alle gestelde requirements kan voldoen, of dat er gegronde redenen zijn dat een systeem aan een aantal van deze requirements niet hoeft te voldoen.

Voor elke requirement uit hoofdstuk 4 die voor systemen met een BIV codering gelijk aan of hoger dan in de requirement is gesteld niet zou gelden, moet per systeem en per requirement worden aangetoond dat de rationale niet valide is, en dat niet voldoen aan de requirement in kwestie geen negatieve invloed kan hebben op andere systemen binnen hetzelfde netwerkdomein.

In dat geval moet de reden per requirement worden geformuleerd en aan de chief information security officer (CISO) worden voorgelegd, zodat hij (samen met vakinhoudelijk specialisten) kan bepalen of de voordelen die deze afwijking oplevert groot genoeg zijn om de bijbehorende extra risico's te accepteren.

3.6 Pak eerst de basis aan

Voor veel bestaande systemen zal gelden dat ze niet kunnen voldoen aan veel van de gestelde eisen in dit document. Het is echter niet reëel om te vereisen dat alle onderdelen vervroegd vervangen moeten worden. Voor de bestaande systemen moet worden uitgegaan van de maatregelen die wel geïmplementeerd kunnen worden om de resterende periode binnen de lifecycle te kunnen overbruggen. Hierin dienen dan de volgende 5 basis functionaliteiten voor cybersecurity terug te komen:

- Voorbereiden, bijvoorbeeld door:
  - Goede wijzigingsprocedures
  - Een correct overzicht van de aanwezige assets
  - Opleiding van personeel (security awareness, of certificering)
- Voorkomen, bijvoorbeeld door:
  - Patching
  - Logische toegangscontrole
  - Netwerk zonering
- Detecteren, bijvoorbeeld door:
  - Logging / IDS
  - Anti-malware
- Opvolging
  - Incident response
  - Containment via netwerk zonering
- Recovery
  - Correct werkende backup/restore
  - uitwijkvoorzieningen

Er zal een nieuw document worden opgesteld om hier in meer detail op in te gaan.

3.7 Safety

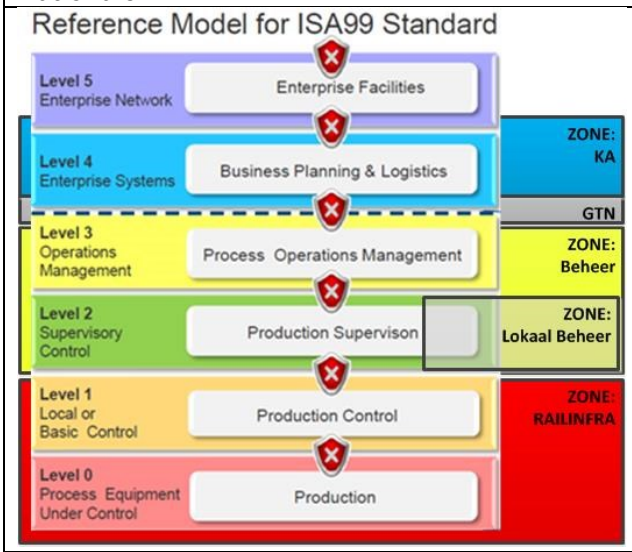
Veel van de ProRail safety systemen zijn ontworpen om in een separaat en gesloten netwerk te functioneren (conform Cenelec EN50159, cat. 1). Hierdoor zijn onvoldoende mitigerende maatregelen geïmplementeerd die wel te verwachten zijn voor een systeem dat op een groter netwerk wordt aangesloten. Vanuit een centrale operatie kunnen systemen uitgeschakeld worden, maar om de veiligheid van mensen te kunnen garanderen moet een lokale uitschakeling voor systemen die een levensbedreigende situatie (bijvoorbeeld hoog/middenspanning) kunnen vormen altijd aanwezig zijn. Hier geldt:

- Safety instrumented systems vallen onder een aparte safety zone, die fysiek volledig gescheiden is van de overige netwerkzones, en nooit op FIDES of ander WAN aangesloten zal worden.
- Indien noodzakelijk kan gebruik gemaakt worden van fysieke safety interlocks.

4 Requirements

4.1 Separatie, perimeter, traffic

ID	Requirement	B	I	V
1.	Railinfra-asset locaties die niet met elkaar hoeven te communiceren, moeten op netwerkniveau van elkaar worden gescheiden.	-	-	-
Rationale				
De Railinfra assets bevinden zich verspreid over het land, vaak op onbemande locaties. Met deze maatregel wordt voorkomen dat op ongeoorloofde manier of per vergissing stuurcommando's naar railinfra assets worden gestuurd. Bovendien wordt zo gezorgd dat problemen in een level niet meteen effect hebben op de andere levels.				

ID	Requirement	B	I	V
1.1.	Railinfra assets worden ingedeeld in levels en security zones conform de ISA99 / IEC62443 standaarden	-	-	-
Rationale				
	Het ISA99 / IEC62443 model is een referentiearchitectuur voor het beveiligen van ICS netwerken en –systemen. Deze keuze past binnen het ProRail beleid om gebruik te maken va internationaal erkende standaarden. De centrale beheer zone bevat hier levels 2 en 3, de Railinfra zone bevat de lokale assets in levels 0 en 1. In voorkomende gevallen zal er nog sprake zijn van een lokale beheerzone met daarin level 2 bedien-apparatuur.			

ID	Requirement	B	I	V
1.1.1.	De systemen die van het ProRail ICS netwerk gebruik maken moeten op het niveau van netwerkcommunicatie van elkaar gescheiden zijn.	-	-	-
Rationale				
Een scheiding op alleen applicatie-autorisatie niveau is niet voldoende. Dit voldoet niet aan het meerlaagse (gatenkaas)model, en biedt geen bescherming in geval van aangetaste systemen. De scheiding primair op het niveau van contractpartij/systeemeigenaarschap, zodat toegang tot systeem X, met eigenaar A nooit kan leiden tot toegang tot systeem Y, met eigenaar B.				

ID	Requirement	B	I	V
1.2.	Communicatie tussen de security zones moet worden gefaciliteerd via één gecontroleerd pad (conduit) per zoneovergang.	-	-	-
Rationale				
Dit is conform de ISA99 / IEC62443 standaard, en reduceert de complexiteit in de communicatie tussen de levels.				

ID	Requirement	B	I	V
1.2.1.	Een communicatiepad is alleen toegestaan tussen twee aangrenzende zones.	-	-	-
Rationale				
Dit is conform de ISA99 / IEC62443 standaard good practice. De voorkeur is om dit ook tussen tussen elk level te hebben, maar om praktische redenen mag hier van worden afgeweken.				

ID	Requirement	B	I	V
1.2.2.	In een communicatiepad tussen securityzones wordt noodzakelijke communicatie beperkt toegelaten op basis van: Source, Destination, Protocol en Poort.	-	-	-
Rationale				
Dit is conform de ISA99 / IEC62443 standaard good practice.				

ID	Requirement	B	I	V
1.2.3.	Bij overgang naar een nieuwe security zone is een nieuwe autorisatie nodig voor toegang tot de nieuwe netwerkzone.	-	-	-
Rationale				
Dit is conform de ISA99 / IEC62443 standaard good practice.				

ID	Requirement	B	I	V
1.2.4.	**<VERVALLEN>**			
Rationale				
Vervallen: OSI laag 7 inspectie wordt onderdeel van logging, detectie en opvolging, niet meer van preventie of als onderdeel van de zonegrens controle. Hiermee bereiken we dat controle over monitoren of bedienen bij de systeemeigenaar blijft, en niet ook deels bij infrastructurbeheer.				

ID	Requirement	B	I	V
1.2.5.	Multicast verkeer is alleen toegestaan binnen een broadcastdomein, niet bij zone- of subnet-overgangen.	-	-	-
Rationale				
Veel industriële protocollen maken gebruik van multicast, maar dit speelt zich vooral op lokaal niveau af. Multicast toestaan tussen verschillende zones maakt de netwerkconfiguratie onnodig complex.				

ID	Requirement	B	I	V
1.3.	Indien op locatie een lokale beheer MMI wordt gekoppeld, dient deze in een eigen lokale security zone te worden geplaatst.	**M**	**M**	
Rationale				
Standaard keuze voor ProRail is om alle bedien MMI's centraal te plaatsen, en voor lokale noodbediening waar nodig alleen een brandweerpaneel met beperkte hard-wired functionaliteit te gebruiken. Indien toch een beheer MMI met uitgebreide functionaliteit ingezet wordt moeten voor deze dezelfde restricties gelden als voor de beheer MMI's vanuit de Beheerzone.				

ID	Requirement	B	I	V
1.3.1.	Voor communicatie tussen de lokale beheer zone en de Beheerzone wordt noodzakelijke communicatie beperkt toegelaten op basis van: Source, Destination, Protocol en Poort.	**-**	**-**	**-**
Rationale				
De lokale MMI zal naar verwachting met centrale systemen moeten communiceren voor zaken als synchronisatie van SCADA gegevens en gebruikersauthenticatie.				

ID	Requirement	B	I	V
1.3.2.	Voor communicatie tussen de lokale beheer zone en de Railinfra-zone wordt noodzakelijke communicatie beperkt toegelaten op basis van: Source, Destination, Protocol en Poort.	**M**	**M**	
Rationale				
Standaard keuze voor ProRail is om alle beheer MMI's centraal; te plaatsen, en voor lokale noodbediening waar nodig alleen een brandweerpaneel met beperkte hard-wired functionaliteit te gebruiken. Indien toch een beheer MMI met uitgebreide functionaliteit ingezet wordt moeten voor deze dezelfde regels/restricties gelden als voor de beheer MMI's vanuit de Beheerzone.				

ID	Requirement	B	I	V
1.3.3.	**<VERVALLEN>**			
Rationale				
Vervallen: OSI laag 7 inspectie wordt onderdeel van logging, detectie en opvolging, niet meer van preventie of als onderdeel van de zonegrens controle. Hiermee bereiken we dat controle over monitoren of bedienen bij de systeemeigenaar blijft, en niet ook deels bij infrastructurbeheer.				

ID	Requirement	B	I	V
2.	Voor monitoring en sturing van de infra assets vanuit De Beheerzone mag alleen gebruik gemaakt worden van de volgende standaarden/protocollen: • SNMP v3 • IEC 60870-5-104 • IEC 62351 • OPC UA • HTTPS • SSH	-	-	-
Rationale				
SNMP v3 bevat een authenticatiemechanisme voor veilige monitoring. Oudere versies hebben dit niet en mogen dus niet worden gebruikt. IEC 60870-5-104 is het huidige gebruikte SCADA protocol binnen ProRail, en ook binnen Europa het meest gebruikt. IEC 62351 is een aanvulling op IEC 60870, met extra security maatregelen. OPC UA is ook een specificatie die een veilige communicatie tussen ICS componenten beschrijft, en extra monitoring functies biedt. Deze twee laatste zijn echter nog weinig in gebruik. Door op deze 4 standaarden te standaardiseren wordt onnodige complexiteit in traffic management vermeden.			

ID	Requirement	B	I	V
3.	De communicatie tussen de Beheerzone en Railinfra-zone moet zijn voorzien van wederzijdse authenticatie.		H	
Rationale				
Zodat alleen vanuit het OBI gestuurd kan worden, en geen man-in-the-middle aanvallen mogelijk zijn op dit communicatiepad.				

ID	Requirement	B	I	V
4.	De conduit rol voor overgangen tussen de KA en Beheerzone en tussen de OBI en Railinfrazone mag niet worden vervuld door devices/software die onderdeel zijn van het operationele systeem (Zoals bijvoorbeeld SCADA PC's).	-	-	-
Rationale				
Operationele systeemdevices hebben vaak beperkingen waar het gaat om het kunnen patchen, en hebben security alleen als secundaire prioriteit.				

ID	Requirement	B	I	V
5.	De netwerktechnologie tussen de beheer- en railinfrazone moet beperkingen kunnen opleggen aan te gebruiken bandbreedte en het aantal connecties.	M		
Rationale				
Hiermee wordt voorkomen dat teveel netwerkverkeer naar de devices gaat, wat effectief een DoS tot gevolg zal hebben.				

ID	Requirement	B	I	V
6.	De railinfra assets in de railinfrazone moeten in staat zijn autonoom een veilige toestand te handhaven en/of realiseren in geval van verlies van connectiviteit met level 2 of 3.	M	M	
Rationale				
Zo kan indien mogelijk de netwerktechnologie van updates worden voorzien, onafhankelijk van de railinfra componenten. Dat wil zeggen: er is geen wederzijdse lock-in voor het plannen van downtime.				

4.2 Netwerktoegang

ID	Requirement	B	I	V
7.	Alle lokale Ethernetaansluitingen moeten worden gerealiseerd conform het ontwerpvoorschrift SpoorLAN.	-	-	-
Rationale				
Om het netwerk veilig te houden moet het altijd eenvoudig en beheersbaar blijven. Dit realiseert ProRail ICT door dit te standaardiseren zoals vastgelegd in genoemd ontwerpvoorschrift.				

ID	Requirement	B	I	V
8.	De lokale ethernetswitches moeten geconfigureerd zijn om ongeautoriseerde netwerktoegang te voorkomen.	M	M	
Rationale				
Om ongeautoriseerde toegang tot de assets buiten de gecontroleerde datapaden om te voorkomen. De minimale bescherming moet zijn tegen ongeautoriseerde draadloze toegangspunten.				

ID	Requirement	B	I	V
9.	Het gebruik van draadloze communicatie voor railinfra assets is standaard niet toegestaan.	M	M	
Rationale				

Draadloze netwerken zijn kwetsbaar voor extra bedreigingen, die zeer lastig zijn tegen te gaan:
• In een draadloos netwerk is geen strikte controle over de fysieke grenzen van het communicatiemedium. Netwerkcommunicatie kan zo opgevangen worden buiten de ruimte waar de apparatuur is geplaatst;
• Draadloze apparaten kijken continu waar de beste connectie met een netwerk beschikbaar is. Met een malafide access point kunnen de draadloze assets misleid worden om hiermee connectie te maken waarmee:
  o ongeoorloofde toegang bereikt kan worden;
  o De assets niet meer op het ProRail netwerk beschikbaar zijn.
• Radiosignalen zijn gevoelig voor verstoring, waardoor een denial of service relatief eenvoudig is uit te voeren.				

ID	Requirement	B	I	V
10.	Daar waar draadloze verbinding de enige optie is mag deze alleen worden ingezet wanneer dit voor ProRail voordelen oplevert die opwegen tegen de bijbehorende risico's, en pas na toestemming van de security officer.	-	-	-
Rationale				
Bij voorkeur dus niet. Maar er zijn scenario's denkbaar waar een draadloze koppeling onontkoombaar is. Die onontkoombaarheid moet dan echter wel via een business case worden aangetoond.				

ID	Requirement	B	I	V
11.	Daar waar draadloze verbinding de enige optie is moet deze voldoende beveiligd zijn tegen ongeautoriseerde toegang.	-	-	-
Rationale				
De business voordelen kunnen groter zijn dan de risico's. Maar dat is vaak alleen zo wanneer de risico's zoveel mogelijk worden gemitigeerd.				

ID	Requirement	B	I	V
11.1.	Draadloze verbindingen zijn altijd voorzien van sterke versleuteling (AES of beter) met individuele sleutels per aangesloten eindpunt.	-	-	-
Rationale				
Lagere niveaus van versleuteling zijn aantoonbaar eenvoudig te kraken. Vaak binnen enkele minuten of zelfs seconden.				

ID	Requirement	B	I	V
11.2.	Draadloze verbindingen zijn altijd voorzien van een willekeurig gegenereerde lange complexe toegangscode.	-	-	-
Rationale				
Lagere niveaus van versleuteling zijn aantoonbaar eenvoudig te kraken. Vaak binnen enkele minuten of zelfs seconden. Het gebruik van standaard toegangssleutels maakt het zelfs nog eenvoudiger.				

ID	Requirement	B	I	V
11.3.	De netwerknaam moet worden aangepast, zodat geen referentie beschikbaar is naar merk/type van de apparatuur of de functie van het netwerk	-	-	-
Rationale				
Hoe minder informatie wordt gegeven aan kwaadwillenden hoe beter. Dat houdt ook in: geen informatie verstrekken over de interessantheid van het netwerk.				

ID	Requirement	B	I	V
11.4.	De access point moet zowel logisch als fysiek niet zichtbaar zijn voor ongeautoriseerde apparaten en/of personen.	-	-	-
Rationale				
Om te voorkomen dat de aandacht wordt gewekt van “toevallige voorbijgangers” die nog geen gerichte scan aan het uitvoeren zijn. Een voorbeeld is de optie om de Service Set IDentifier (SSID) van het netwerk niet uit te zenden.				

ID	Requirement	B	I	V
11.5.	Beperk waar mogelijk de reikwijdte van het signaal tot alleen de strikt noodzakelijke dekking.	-	-	-
Rationale				
Om te voorkomen dat de aandacht wordt gewekt van “toevallige voorbijgangers” die nog geen gerichte scan aan het uitvoeren zijn. Dit kan onder andere gerealiseerd worden via richtantennes.				

ID	Requirement	B	I	V
11.6.	De draadloze eindpunten moeten worden geïsoleerd in een eigen security zone, geïsoleerd van de bedrade railinfra zone.	M	M	
Rationale				
Om te zorgen dat na een eventuele ongeautoriseerde toegang de draadloze apparaten als hop richting de rest van de railinfra zone gebruikt kan worden.				

ID	Requirement	B	I	V
11.6.1.	Voor communicatie tussen de lokale wireless zone en de beheerzone wordt noodzakelijke communicatie beperkt toegelaten op basis van: Source, Destination, Protocol en Poort.	-	-	-
Rationale				
Vanuit het OBI kan dan beperkt informatie uitgelezen worden, maar wel alleen door geautoriseerde systemen.				

ID	Requirement	B	I	V
11.7.	De draadloze eindpunten mogen alleen gebruikt worden voor monitoring en analyse, niet voor bediening of wijziging.	-	-	-
Rationale				
Draadloze systemen in omgevingen met deze langdurige lifecycles worden door ProRail op dit moment als te kwetsbaar beschouwd om bediening toe te staan.				

4.3 Fysieke beveiliging

ID	Requirement	B	I	V
12.	Fysieke toegang tot alle componenten in levels 0 en 1 moet zijn beveiligd conform de geldende ProRail security richtlijnen voor technische ruimtes.	-	-	-
Rationale				
Lokaal op deze devices is beveiliging niet of nauwelijks mogelijk. D.m.v. fysieke toegangsbeveiliging kan ongeoorloofde toegang bemoeilijkt worden.				

ID	Requirement	B	I	V
13.	Alle reserveonderdelen moeten voordat ze worden ingezet worden gecontroleerd op fysieke afwijkingen van de standaardconfiguratie	-	-	-
Rationale				
Als tegenmaatregel tegen acties zoals deze gedemonstreerd zijn in het project PLCpwn (http://www.digitalbond.com/blog/2014/02/03/s4x14-video-stephen-hilt-on-plcpwn/), waarbij een PLC fysiek is aangepast om zo het beschermde ICS netwerk direct vanaf internet toegankelijk te maken.				

4.4 Authenticatie & Autorisatie

ID	Requirement	B	I	V
14.	Elke gebruiker en/of device dient zich te authentiseren om gebruik te kunnen maken van services voor sturen en/of monitoren van de devices.	M	M	
Rationale				
Om ongeoorloofde toegang te voorkomen.				

ID	Requirement	B	I	V
14.1.	Bij toegang vanuit een zone naar een service in een andere zone dient een nieuwe authenticatie op die service plaats te vinden.	M	M	
Rationale				
Dit is conform ISA99 / IEC62443, en in lijn met de interne connectie standaarden bij netwerkdomein-overgangen.				

ID	Requirement	B	I	V
14.2.	Alle standaard gebruiker/wachtwoord combinaties moeten worden gewijzigd voordat de componenten in gebruik worden genomen. Dit geldt ook voor eventuele testfases.	-	-	-
Rationale				
Om eenvoudige toegang via overal bekende gegevens te voorkomen. En ook om te voorkomen dat tijdens testen / commissioning ongewenste zaken kunnen worden geïntroduceerd die tijdens productie bruikbaar kunnen zijn voor hackers.				

ID	Requirement	B	I	V
15.	Transport en opslag van accountgegevens is altijd versleuteld.		M	
Rationale				
Dit is conform ISA99 / IEC62443, en conform ProRail informatiebeveiligingsbeleid.				

ID	Requirement	B	I	V
16.	Waar mogelijk moet door de devices/services gebruik gemaakt worden van gescheiden autorisaties. Deze scheiding is minimaal tussen alleen lezen en beheertoegang.	M	M	
Rationale				
Om te voorkomen dat iedereen die succesvol authentiseert volledige rechten heeft over een component.				

ID	Requirement	B	I	V
17.	Het inloggen met beheerrechten is alleen toegestaan voor het uitvoeren van de specifieke beheertaken waarvoor de rechten zijn toegekend, niet voor dagelijkse operationele taken.	**M**	**M**	
Rationale				
Hiermee wordt voorkomen dat het uitvoeren van ongewenste code in een normale gebruikerssessie onnodig op beheerrechten kan meeliften. Bovendien kan zo via audit logs worden vastgesteld welke gebruiker de verhoogde rechten heeft aangeroepen. Methodes om dit te realiseren zijn het gebruik van separate beheeraccounts die alleen via een account control mechanisme (bijvoorbeeld Windows User Account Control of SUDO) kunnen worden aangeroepen.				

ID	Requirement	B	I	V
18.	Voor het monitoren en voor het bedienen van de assets moet gebruik gemaakt worden van gescheiden autorisaties op meerdere niveaus (Scheiden van SCADA hosts, separate users/groepen op zowel backend als lokaal asset niveau).	**M**	**M**	
Rationale				
Dit is conform ISA99 / IEC62443 defense in depth strategie. Hiermee worden gevolgen van een hack of configuratiefout op 1 niveau beperkt. Zie ook sectie 3.1 en 3.3.1 in dit document. Bijvoorbeeld: een gebruiker die per ongeluk teveel rechten krijgt, maar gebruik maakt van een read-only SCADA server zal op een ander niveau alsnog de noodzakelijke beperkingen opgelegd krijgen. Zie ook sectie 3.3.1 van dit document.				

ID	Requirement	B	I	V
18.1.	Het systeem moet zo geïmplementeerd zijn dat toegang tot de services voor monitoren en de services voor bedienen via volledig gescheiden netwerkpaden kan worden aangeboden.	**M**	**M**	
Rationale				
Hiermee kunnen de toegangsniveau's monitoren en bedienen ook worden afgedwongen binnen het netwerk door op deze toegangspaden te filteren.				

ID	Requirement	B	I	V
18.2.	De service voor monitoren mag nooit toegang hebben tot vitale bedienfuncties binnen het systeem.	**M**	**M**	
Rationale				
Om te voorkomen dat toegang tot de monitorfunctie als achterdeur wordt gebruikt.				

4.5 Hardening

ID	Requirement	B	I	V
19.	Op alle systeemcomponenten mogen alleen die services geactiveerd zijn die noodzakelijk zijn voor regulier functioneren. Alle overige services moeten worden uitgeschakeld.	**-**	**-**	**-**
Rationale				
Om het aanvalsplatform zo klein mogelijk te houden. Bovendien: een service die niet wordt gebruikt wordt in de praktijk ook niet onderhouden of gemonitord.				

ID	Requirement	B	I	V
20.	Als services voor beheertoegang op componenten zijn toegestaan: SSH, HTTPS, FTPS, SFTP (SCP).	**-**	**-**	**-**
Rationale				
Open standaarden die zijn voorzien van authenticatie en encryptie.				

ID	Requirement	B	I	V
20.1.	Per beheerfunctionaliteit mag slechts één service actief zijn op een eindpunt.	-	-	-
Rationale				
Het aanvalsplatform dient altijd zo klein mogelijk te worden gehouden. Wanneer een eindpunt via https te beheren is, is het onnodig om voor dezelfde functies bijvoorbeeld ook een SSH service aan te bieden.				

ID	Requirement	B	I	V
21.	Hardware interfaces die niet noodzakelijk zijn voor dagelijks functioneren/onderhoud moeten zijn uitgeschakeld, waar mogelijk mechanisch geblokkeerd: • Ethernet interfaces • Seriële/bus interfaces • Draadloze interfaces (WLAN, Bluetooth, etc.) • USB, Firewire en gelijkwaardig.	M	M	
Rationale				
Om ongewenste infecties/toegang via deze interfaces te voorkomen. Met name malware die specifiek op ICS systemen gericht is maakt veelvuldig gebruik van propagatie via deze interfaces om eventuele air-gaps te kunnen overbruggen.				

ID	Requirement	B	I	V
21.1.	Daar waar hardware interfaces niet gedeactiveerd kunnen worden, zijn alle boot- en autostart mechanismen op deze interfaces uitgeschakeld.	M	M	
Rationale				
Om ongewenste infecties/toegang via deze interfaces te voorkomen. Met name malware die specifiek op ICS systemen gericht is maakt veelvuldig gebruik van propagatie via deze interfaces om eventuele air-gaps te kunnen overbruggen.				

ID	Requirement	B	I	V
21.2.	Daar waar externe media als USB sticks noodzakelijk zijn, dient altijd gebruik gemaakt te worden van dedicated media voor deze functie.	M	M	
Rationale				
Bijvoorbeeld niet een USB stick die ook buiten de vertrouwde omgevingen is ingezet, omdat dit laatste extra kans geeft op malware infecties.				

ID	Requirement	B	I	V
21.3.	Daar waar externe media als USB sticks noodzakelijk zijn, dienen deze altijd voor gebruik gescand te worden op malware op een aparte PC.	M	M	
Rationale				
Als extra maatregel tegen malware infecties.				

ID	Requirement	B	I	V
22.	Alle firmware in de devices moet zijn voorzien van een cryptografisch gegenereerde digitale handtekening.	M	M	
Rationale				
Om de gecertificeerde firmware te kunnen onderscheiden van kwaadaardige firmware.				

ID	Requirement	B	I	V
22.1.	Tijdens elke opstartprocedure moeten deze handtekeningen worden gecontroleerd voordat alle firmware wordt geladen en de functionaliteit wordt geactiveerd.	M	M	
Rationale				
Om te zorgen dat kwaadaardige firmware nooit tot functioneel niveau kan opstarten.				

ID	Requirement	B	I	V
23.	Op systeemcomponenten moeten waar mogelijk extra maatregelen actief zijn (naast de reeds benoemde authenticatie- en autorisatie eisen) om ongeoorloofde aanpassingen in de configuratie te voorkomen, bijvoorbeeld: • Anti-malware • Application Whitelisting • Host-based firewall/IDS	-	-	-
Rationale				
Zodat ook op bedien PC's e.d. die niet altijd de meest recente updates hebben kan worden voorkomen dat kwaadaardige code uitgevoerd wordt. M.n. application whitelisting is zeer geschikt voor de zeer statische ICS omgevingen.				

4.6 Patching

ID	Requirement	B	I	V
24.	Op alle gebruikte operating systemen en software, zowel Linux/Windows als leverancier specifiek (incl. PLC firmware), moet beleid van toepassing zijn om ze waar nodig van patches en updates te voorzien.	-	-	-
Rationale				
Dit is conform ISA99 / IEC62443, en conform ProRail informatiebeveiligingsbeleid. Ook al weten we dat de frequentie van patches lager zal zijn, en het implementatieproces een stuk complexer. Ook op deze systemen is patching wel degelijk noodzakelijk.				

ID	Requirement	B	I	V
24.1.	De leverancier moet ProRail informeren over gevonden kwetsbaarheden die van invloed kunnen zijn op het correct en veilig functioneren van (een van de) gebruikte systemen.	-	-	-
Rationale				
Zodat ProRail niet alle CERT meldingen van alle gebruikte software en devices hoeft uit te pluizen. De leverancier is veelal sowieso al verantwoordelijk voor het correct blijven functioneren van het systeem. Dat maakt het patchen van kwetsbaarheden ook zijn belang.				

ID	Requirement	B	I	V
24.2.	Na testen en certificeren van de beschikbare patches moeten deze in samenwerking met ProRail op de betreffende componenten worden geïnstalleerd.	-	-	-
Rationale				
Dit is conform ISA99 / IEC62443, en conform ProRail informatiebeveiligingsbeleid.				

ID	Requirement	B	I	V
24.3.	Waar mogelijk moeten de componenten zo ingericht zijn dat installatie van Patches en updates kan plaatsvinden met minimale downtijd.	**M**		
Rationale				
We moeten naar een situatie toe waar het patchen minder impact heeft, en daardoor in de toekomst sneller kan worden uitgevoerd. Het minimaliseren van de downtijd geldt zowel voor de installatie zelf als voor de eventuele rollback.				

ID	Requirement	B	I	V
24.4.	Voor implementatie van patches dient een geborgde wijzigingsprocedure beschikbaar te zijn specifiek voor het ICS systeem.	-	-	-
Rationale				
Voor ICS patching gelden speciale spelregels, waardoor standaard IT procedures niet kunnen worden toegepast. Deze specifieke wijzigingsprocedure moet samen met de leverancier worden opgesteld.				

4.7 Logging en alerting

ID	Requirement	B	I	V
25.	Alle systeemcomponenten moeten faciliteiten hebben om het operationele gedrag te loggen t.b.v. analyse.	-	-	-
Rationale				
Door direct bij inbedrijfname van de assets in de mogelijkheid tot logging te voorzien wordt het inrichten van alert opvolging door ProRail in de nabije toekomst mogelijk zonder dat daarvoor op dat moment onoverkomelijke investeringen nodig zullen zijn.				

ID	Requirement	B	I	V
25.1.	Deze logging moet kunnen worden doorgestuurd naar een centraal systeem.		M	
Rationale				
Door direct bij inbedrijfname van de assets in de mogelijkheid tot logging te voorzien wordt het inrichten van alert opvolging door ProRail in de nabije toekomst mogelijk zonder dat daarvoor op dat moment onoverkomelijke investeringen nodig zullen zijn.				

ID	Requirement	B	I	V
26.	Alle systeemcomponenten moeten faciliteiten hebben om alle uitgevoerde configuratiewerkzaamheden en pogingen daartoe te kunnen loggen in een centraal systeem t.b.v. analyse.		M	
Rationale				
Door direct bij inbedrijfname van de assets in de mogelijkheid tot logging te voorzien wordt het inrichten van alert opvolging door ProRail in de nabije toekomst mogelijk zonder dat daarvoor op dat moment onoverkomelijke investeringen nodig zullen zijn.				

ID	Requirement	B	I	V
26.1.	Deze logdata bevat minimaal: - Ip adressen (in geval van toegang via ethernet) - Protocol/poort info - Datum en tijd (met timestamp in UTC formaat) - Gebruikersnamen - Gebruikte wijze van toegang (SSH, HTTPS, serieel etc)		M	
Rationale				
Deze info is relevant om een analyse te kunnen doen na een eventueel incident.				

ID	Requirement	B	I	V
27.	Voor deze logdata moet lokaal een buffer beschikbaar zijn voor het geval het centrale systeem tijdelijk niet beschikbaar is. Deze buffer mag na 24 uur overschreven worden.	M	M	
Rationale				
Zodat Logdata bij korte verstoringen in centraal systeem of verbinding niet verloren gaat.				

ID	Requirement	B	I	V
28.	Ethernet netwerkverkeer moet worden gemonitord en gelogd	-	-	-
Rationale				
Door direct bij inbedrijfname van de assets in de mogelijkheid tot logging te voorzien wordt het inrichten van alert opvolging door ProRail in de nabije toekomst mogelijk zonder dat daarvoor op dat moment onoverkomelijke investeringen nodig zullen zijn.				

ID	Requirement	B	I	V
29.	Ongewoon en ongewenst netwerkgedrag in en tussen de levels 1, 2 en 3 moet worden gedetecteerd en gemeld (Intrusion Detection).	-	-	-
Rationale				
Omdat dit ICS specifieke verkeer veelal niet overweg kan met de additionele latency van actieve filtering (intrusion prevention), en preventie ook effectief het bedienen beïnvloedt buiten de macht van de systeemeigenaar, is detectie en opvolging is het noodzakelijke alternatief. NB: In level 1 en 0 wordt veelal Bustechnologie gebruikt, waarvoor dit niet mogelijk en dus ook niet vereist is.				

ID	Requirement	B	I	V
29.1.	De analyse van dit verkeer vindt plaats tot op OSI laag 7.	M	M	
Rationale				
In geval van hogere beschikbaarheidseisen moeten ook afwijkende meet- en stuurcommando's van en naar de apparatuur worden gedetecteerd. Hiervoor is OSI laag 7 inspectie noodzakelijk, omdat deze commando's in dit deel van de netwerkpakketten worden verpakt.				

ID	Requirement	B	I	V
30.	Alle componenten synchroniseren hun tijd met een gedeelde, nauwkeurige tijdbron.	-	-	-
Rationale				
Om de loggegevens van verschillende assets met elkaar te kunnen matchen op basis van de timestamps is vereist dat overal dezelfde tijd wordt gebruikt.				

ID	Requirement	B	I	V
30.1.	Deze tijdbron moet in een hiërarchie onder de ProRail NTP server zijn opgenomen.	-	-	-
Rationale				
Om de loggegevens van verschillende assets met elkaar te kunnen matchen op basis van de timestamps is vereist dat overal dezelfde tijd wordt gebruikt.				

4.8 Recovery en continuïteit

ID	Requirement	B	I	V
31.	Een Backup- en recovery proces dient te zijn ingericht voor alle door het systeem gebruikte • OS- en firmware installatie images; • Applicatie installatiebestanden; • Configuratiebestanden.	-	-	-
Rationale				
Bij onherstelbare uitval van een systeemcomponent moet zo snel mogelijk een vervangend onderdeel ingezet kunnen worden, die van dezelfde functionele configuratie is voorzien.				

ID	Requirement	B	I	V
31.1.	Deze procedure wordt minimaal één maal per jaar getest.	M		
Rationale				
Hiermee wordt vastgesteld dat een recovery daadwerkelijk mogelijk is.				

ID	Requirement	B	I	V
31.1.1.	Voor deze tests is een representatieve testomgeving beschikbaar.	M		
Rationale				
In productie testen is veelal niet mogelijk. Daar waar het qua configuratie zou kunnen wordt een omgeving vaak vanwege andere prioriteiten niet vrijgegeven met uitstel en uiteindelijk afstel van de test tot gevolg. Die situatie moet te allen tijde voorkomen worden.				

ID	Requirement	B	I	V
31.2.	Deze procedure voorziet in: • Recovery van componenten tot volledig functioneel niveau in de huidige versie; • Recovery van componenten tot volledig functioneel niveau in een vorige versie (roll-back); • Recovery van componentconfiguratie na upgrade naar een nieuwe versie.	-	-	-
Rationale				
Recovery van componenten die stuk zijn gegaan of die na een upgrade niet goed functioneren is een algemene good practice. Bij upgrades van SCADA/PCD software systemen is vaak een backup bestand van de originele PLC basisconfiguraties benodigd. Deze staan vaak in kleine files (*.tpy en dergelijke) waarin bijvoorbeeld de algemene adressering is opgenomen. Upgrade projecten zijn in het verleden ver uit tijd en budget gelopen of zelfs gestrand doordat van deze files geen kopie beschikbaar was.				

4.9 Documentatie

ID	Requirement	B	I	V
32.	Van de geïmplementeerde oplossing is actuele as built documentatie beschikbaar, met daarin opgenomen minimaal: • Fysieke en logische constructieschema's; • Overzicht van de verwachte netwerkverkeersstromen.	-	-	-
Rationale				
Om de totale keten te kunnen beheren en beveiligen is als eerste vereist dat bekend is wat precies beveiligd moet worden. Zo kan het actuele netwerkverkeer of de aanwezigheid van apparatuur in het netwerk altijd getoetst worden aan de situatie zoals hij volgens het ontwerp zou moeten zijn. Dit wordt vaak aangeduid met de term "situational awareness".				

ID	Requirement	B	I	V
33.	Van de geïmplementeerde oplossing is actuele as built documentatie beschikbaar, met daarin opgenomen minimaal: • Installatie- en Configuratielogs van alle software en hardware componenten; • Vastlegging van alle assets in een configuratiedatabase.	M	M	-
Rationale				
Bij onherstelbare uitval van een systeemcomponent moet zo snel mogelijk een vervangend onderdeel ingezet kunnen worden, die van dezelfde functionele configuratie is voorzien. Werkt de recovery procedure om een of andere reden niet, is een handmatige rebuild de laatste optie. Hiervoor is de documentatie van de configuratie benodigd.				

5 Bijlage A – Begrippen en afkortingen

Begrip/afkorting	Definitie / betekenis
Application whitelisting	Een IT beheermaatregel ter voorkoming van het starten van ongeautoriseerde softwareprocessen door een lijst op te leggen van een set geautoriseerde processen en elke afwijking daarvan te blokkeren.
CERT	Computer Emergency Response Team. Een groep experts die beveiligingsincidenten of –kwetsbaarheden identificeert, afhandelt en veelal communiceert naar overige belanghebbenden.
Conduit	Een gecontroleerd pad voor toegang tussen twee beveiligingsniveaus of –zones.
Fides	Het ProRail wide area network.
FTPS	File Transfer Protocol Secure. Een uitbreiding op standard FTP met als doel een veilige uitwisseling van gegevens.
HTTPS	HyperText Transfer Protocol Secure. Een uitbreiding op standard HTTP met als doel een veilige uitwisseling van gegevens
ICS	Industrial Control System. De verzamelnaam voor alle typen veld- en ICT hard- en software die wordt gebruikt voor meten en besturing van industriële systemen.
IDS	Intrusion Detection System. Systeem voor automatische detective van ongeautoriseerde toegangspogingen.
IEC 60870-5-104	Communicatiestandaard voor het sturen van besturingscommando's tussen ICS systemen, vooral gericht op systemen voor energievoorziening.
IEC 62351	Een uitbreiding op IEC60870-5-104, met als doel een veilige uitwisseling van gegevens.
ISA99 / IEC62443	Referentiearchitectuur voor system- en netwerkbeveiliging in industriële automatisering.
OBI	Operationeel Besturingscentrum Infra.
OPC UA	Ole for Process Control – Unified Architecture (of Open Platform Communications - Unified Architecture). Industriële standard voor machine-to-machine communicatie en interoperabiliteit.
OT	Operations Technology
PCD	Process Control Domain. Veel gebruikte term voor ICS systemen die industriële processen beheren.
PLC	Programmable Logic Controller. Een digitale computer die wordt gebruikt voor het automatiseren van industriële elektromechanische processen.
SCADA	Supervisory control and data acquisition. Een veelgebruikte term voor ICS systemen die worden ingezet voor monitoren en besturen op afstand.
SFTP / SCP	Secure File Transfer Protocol / Secure Copy Protocol. Protocol voor bestandsoverdracht dat gebruik maakt van SSH, inclusief de mechanismen voor authenticatie en versleuteling met als doel een veilige uitwisseling van gegevens.
Situational awareness	Het kritieke bewustzijn van een systeemomgeving voor beslissers in de operatie van De perceptie van omgevingselementen van een systeem, het begrijpen van de betekenis van die elementen en hun samenhang en het kunnen voorspellen van de statuswijziging nadat een of meerdere variabelen in die omgeving gewijzigd wordt.
SNMP	Simple Network Management Protocol
SpoorLAN	De ProRail standaard voor lokale communicatie netwerken.
SSH	Secure Shell. Een cryptografisch netwerkprotocol voor veilige aansturing van netwerkdiensten via onvertrouwde netwerken.
SUDO	"Super User DO". Een functie op UNIX-type operating systemen om gebruikers toe te staan een proces uit te voeren met de beveiliging privileges van een andere gebruiker.
User Account Control	Een functie op Windows systemen waarmee een gebruiker aan een softwareproces eerst expliciet toestemming moet geven (door het geven van een akkoord, of door het aanbieden van credentials voor een secundaire account) voor het gebruik van verhoogde beveiliging privileges.
WLAN	Wireless LAN. Een draadloos lokaal network.
WPA2	Wi-Fi Protected Access II. Een methode voor het beveiligen van draadloze netwerken door middel van netwerktoegangscontrole en gegevensbescherming via versleuteling.

6 Bijlage B – Referenties

Titel	Link
Richtlijn security technische ruimtes	ProRail RLN00289-6-V001
OVS SpoorLAN	ProRail OVS00217-V003
NIST SP 800-82 R2	NIST.SP.800-82r2
SANS secure architecture for ICS	SANS secure architecture for industrial control systems
ICT Architectuur 2025	<nog te publiceren>