hetWaterschapshuis

Beschrijving functionele blokken PA-Systemen

Contact informatie:

Het Waterschapshuis

Stationsplein 89

3818 LE Amersfoort

Dhr. Henk Pierik

Datum:

02 november 2021

Versie	Datum	Beschrijving van de wijziging	Auteur
0.1	05-07-2021	Concept	RGr
0.2	09-07-2021	Feedback verwerkt Waterschapshuis overleg	RGr
0.3	14-07-2021	Feedback verwerkt consultant review	RGr
0.4	22-09-2021	Feedback verwerkt werkgroep	RGr
1.0	11-10-2021	Eindversie	SKo
1.1	02-11-2021	Feedback verwerkt, eindversie	RGr

Inhoud

1 Inleiding

Dit document geeft omschrijvingen van de functionele blokken zoals gedefinieerd in de netwerktekeningen 'Hoofdkantoor', 'Hoofdlocatie / RWZI' en 'PA-object' van de 'High-level architectuur Waterschappen' versie 0.93.

Onder Proces Automatisering (PA) valt alles wat direct of indirect ingrijpt op het besturen en regelen van het (primaire) proces.

Een functioneel blok wordt gedefinieerd als een zone waar apparaten, systemen en installaties worden opgenomen die eenzelfde primaire functie hebben. Dit werkt op een vergelijkbare wijze als zones in de IEC 62443 norm. De omschrijvingen bestaan uit:

- Het doel van het functionele blok;
- Voorbeelden van systemen in het functionele blok;
- Gekoppelde functionele blokken & conduits;
- Specifieke best practices (mits aanwezig).

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en krijgt een naam die een combinatie is tussen de namen van de functionele blokken.

Best practices worden gegeneraliseerd weergegeven per overkoepelende omgeving. Zoals DMZ, PA-omgeving, KA omgeving, etc.

Binnen dit document, wordt uitgegaan van een initieel Security Level (SL) van 2 conform de IEC 62443, deel 3-3. Hogere security levels die mogelijk van toepassing zijn in specifieke functionele blokken kunnen leiden tot aanvullende eisen welke niet in dit document benoemd zijn. De IEC 62443 is een normenkader ten behoeve van cybersecurity in Industriële Automatisering en Controle Systemen (IACS).

Er wordt gebruik gemaakt van gegeneraliseerde referenties naar de Cyber Security Implementatie Richtlijn (CSIR) 1.95. Dit wordt beschreven in een algemeen overzicht van relevante CSIR vereisten ten opzichte van de IEC 62443 3-3 Security Level 2. Dit overzicht is niet specifiek per functioneel blok gedefinieerd en geeft alleen relevante vereisten ten opzichte van IEC 62443 3-3 Security Level 2. Een overzicht hiervan is toegevoegd aan dit document als bijlage.

Wanneer er afgeweken wordt van de beschreven architectuur, dan is het van belang dit vast te leggen, te verantwoorden en goed te laten keuren door de management verantwoordelijke. Het zogenaamde 'comply or explain'.

In de bijlagen is de uitgebreide versie van het document 'Beschrijving functionele blokken PA-Systemen' toegevoegd waarbij per functioneel blok de volledige informatie terug te vinden is.

1.1 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

2 DMZ

DMZ's voorzien in communicatie tussen functionele blokken en deze communicatie verloopt via een firewall waarbij strenge controle wordt uitgeoefend op het netwerkverkeer. Het doel van een DMZ in combinatie met een firewall is om directe communicatie te voorkomen tussen verschillende functionele blokken. Hierbij is het van belang dat er in de basis geen communicatie plaatsvindt tussen functionele blokken en alleen noodzakelijke communicatie in overleg met alle belanghebbenden. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Binnen de DMZ worden patches direct toegepast zodra deze beschikbaar komen.

Er wordt niet permanent data opgeslagen in DMZ's, maar er worden alleen communicatievoorzieningen in opgenomen. Het doorgeven van informatie is wel mogelijk via de DMZ, maar directe communicatie van het ene functionele blok naar het andere functionele blok niet.

Onder communicatievoorzieningen wordt het volgende verstaan:

- Steppingstone server
- Proxyservers
- Transfer fileservers
- Updateservers

2.1 DMZ KA / PA

Het functionele blok 'DMZ KA / PA' is bestemd voor communicatie tussen de KA omgeving en PA omgeving.

Specifieke communicatievoorzieningen voor dit functionele blok:

- Steppingstone server om toegang te krijgen tot de PA omgeving (via bijvoorbeeld RDP)

2.1.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- KA – Servers & Clients
- PA – Systemen en Data
- OTA
- DMZ PA/ES

2.1.2 Aanvullende best practices (operationele werkwijze)

De verbonden OTA (Ontwikkeling, Testen en Acceptatie) dient geen onderdeel te zijn van de productieomgeving en hiermee ook geen gebruik te maken van netwerkservices zoals authenticatie, filesharing, DNS, DHCP, etc.

2.2 DMZ PA / Private WAN

Het functionele blok 'DMZ PA / Private WAN' is bestemd voor communicatie tussen de PA omgeving en PA blokken/sites verbonden met een WAN connectie.

Specifieke communicatievoorzieningen voor dit functionele blok:

- Steppingstone server om toegang te krijgen tot verschillende sites

2.2.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- Afstandsbediening
- Hoofdlocatie / RWZI PA
- PA-object
- Hoofdkantoor PA

2.3 DMZ PA / ES

Het functionele blok 'DMZ PA / ES' is bestemd voor communicatie tussen de PA omgeving en extra systemen die communicatie behoeven met de PA omgeving.

Specifieke communicatievoorzieningen voor dit functionele blok:

- Steppingstone server om toegang te krijgen tot verschillende packages

2.3.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / PA
- PA – Systemen en Data
- PA – Control
- Warmtekrachtcentrale
- Package unit

2.4 DMZ KA / Internet

Het functionele blok 'DMZ KA / Internet' is bestemd voor communicatie tussen de KA omgeving en het internet.

Specifieke communicatievoorzieningen voor dit functionele blok:

- Steppingstone server om toegang te krijgen tot de KA omgeving

2.4.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Hoofdkantoor KA
- KA – Servers & Clients
- RA (toegang op afstand)
- Hoofdlocatie / RWZI KA
- Internet

2.5 DMZ PA / Private WAN – PA-object

Het functionele blok 'DMZ PA / Private WAN' is bestemd voor communicatie tussen de PA omgeving en PA blokken/sites verbonden met een WAN connectie vanaf het oogpunt van PA-objecten.

Specifieke communicatievoorzieningen voor dit functionele blok:

- Steppingstone server om toegang te krijgen tot het PA-object

2.5.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control
- Hoofdlocatie / RWZI PA
- Hoofdkantoor PA

3 PA Omgeving

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussenstaat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

3.1 PA – Systemen en Data

Het functionele blok ‘PA – Systemen en Data’ is bestemd voor historian servers, domain controllers en MES servers. Het functionele blok wordt gebruikt voor controle van het proces, opslag en ondersteunende diensten.

Hieronder wordt verstaan:

- Historian servers
- Domain Controllers
- MES servers
- Fileservers
- Applicatieservers

3.1.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control
- PA – Beheer

- DMZ KA/PA
- DMZ PA/ES
- DMZ PA/Private WAN
- PA – Safety / Hoog kritisch

3.2 PA – Beheer

Het functionele blok 'PA – Beheer' is bestemd voor engineering servers en -stations. Het functionele blok wordt gebruikt voor servers en werkstations waarmee wijzigingen aangebracht kunnen worden binnen een PA omgeving.

Hieronder wordt verstaan:

- Engineering workstations
- Aankoppelvlakken voor engineering laptops
- Engineering servers

3.2.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- PA – Control
- PA – Wireless apparaten

3.3 PA – Wireless apparaten

Het functionele blok 'PA – Wireless apparaten' is bestemd voor apparaten gebruikmakend van draadloze communicatie als primair of secundair middel. Het functionele blok wordt gebruikt voor draadloze modems, draadloze sensoren en andere draadloze communicatie binnen de PA omgeving.

Hieronder wordt bijvoorbeeld verstaan:

- Wireless HART sensoren / gateways;
- 3G/4G modems (bijvoorbeeld voor primaire / secundaire communicatie of private APN);
- GSM modems (bijvoorbeeld voor alarmering);
- LoraWAN of andere LPWAN toepassingen;
- Draadloze gebouwautomatisering;
- Bluetooth;
- Wifi routers / access-points;

3.3.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Beheer
- PA – Control

3.3.2 Aanvullende best practices (operationele werkwijze)

Bij het inzetten van apparaten die wireless communicatie gebruiken of ondersteunen, dan moeten er een aantal stappen ondernomen worden:

1. Schakel wireless interfaces uit wanneer deze niet in gebruik zijn;
2. Als uitzetten niet mogelijk is, dan moet een risicoanalyse worden uitgevoerd en beheersmaatregelen worden opgesteld;
3. Indien het risico niet geaccepteerd wordt, dan moet de wireless toepassing in een eigen zone geplaatst worden, een conduit beschreven worden en moet dit getest worden.

3.4 PA – Control

Het functionele blok 'PA – Control' is bestemd voor apparaten die voorzien in controle over één of meerdere processen. Het functionele blok wordt gebruikt voor clients, workstations en servers waarmee in aansturing van processen wordt voorzien.

Hieronder wordt verstaan:

- SCADA clients en servers
- HMI's
- DCS clients en servers
- Automation servers
- Visualisatie servers
- Operator workstations

3.4.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- PA – Beheer
- PA – Wireless apparaten
- PA – IO / PLC
- PA – Safety / Hoog kritisch
- Package unit
    - Bus koppeling

- DMZ PA / ES

3.4.2 Aanvullende best practices (operationele werkwijze)

Bij het functionele blok 'PA – Control' vindt eventueel een direct koppelvlak plaats met Extra Systemen doormiddel van bijvoorbeeld een bus koppeling. Een dergelijke koppeling vindt alleen plaats wanneer een koppeling via een DMZ niet mogelijk is. Documenteer en controleer een dergelijke verbinding streng.

3.5 PA – IO / PLC

Het functionele blok 'PA – IO / PLC' is bestemd voor apparaten die voorzien in directe aansturing van een proces en daarbij een aansturing, actuator of sensor rol heeft. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren.

Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

3.5.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

3.6 PA – Safety / Hoog kritisch

Het functionele blok 'PA – Safety / Hoog kritisch' is bestemd voor apparaten die voorzien in safety van een IACS proces of voor apparaten welke een hoog kritische functionaliteit hebben voor het proces. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren met een safety / hoog kritische functionaliteit.

Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

3.6.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- PA – Control

3.7 Afstandsbediening

Het functionele blok 'Afstandsbediening' is bestemd voor apparaten die voorzien in controle over één of meerdere processen op afstand, zijnde een andere geografische locatie en/of site. Het functionele blok wordt gebruikt voor clients, workstations en servers waarmee in aansturing van processen wordt voorzien. Apparaten in dit functionele blok kunnen ook voorkomen op een 'Hoofdlocatie/RWZI' naast een 'Hoofdkantoor' locatie.

Hieronder wordt verstaan:

- SCADA clients en servers
- HMI's
- DCS clients en servers
- Automation servers
- Visualisatie servers
- Operator workstations

3.7.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / Private WAN

3.7.2 Uitwijklocatie

In situaties waar de afstandsbediening de primaire manier bediening is in de vorm van een gecentraliseerde controlekamer, dan is een uitwijklocatie een optionele redundantie om te voorzien in hogere uptime.

4 Extra systemen

Extra systemen betreffen systemen of installaties die niet onderdeel zijn van het primaire proces(sen) van het waterschap / hoogheemraadschap, maar geen KA systeem betreft. Deze systemen kunnen uiteenlopend zijn waardoor de best practice is om deze systemen in een eigen stuk netwerk te plaatsen. Hierbij wordt de communicatie van en naar de systemen streng gecontroleerd.

4.1 Warmtekrachtcentrale

Het functionele blok 'Warmtekrachtcentrale' is bestemd voor apparaten die functioneel onderdeel zijn van een warmtekrachtcentrale. Dit is een extra systeem ten opzichte van het primaire proces van waterschappen / hoogheemraadschappen en hierdoor niet noodzakelijk.

4.1.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / ES

4.2 Package unit

Het functionele blok 'Package unit' is bestemd voor apparaten die functioneel onderdeel zijn van een extra systeem. Dit is een extra systeem ten opzichte van het primaire proces van waterschappen / hoogheemraadschappen en hierdoor niet noodzakelijk.

4.2.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / ES
- PA – Control
    - Bus koppeling
- 4G Leverancier

4.3 4G leverancier

Het functionele blok '4G leverancier' is bestemd voor interfaces geleverd door de leverancier van het betreffende extra systeem. Dergelijke connecties kunnen door leveranciers opgelegd worden in contractuele / SLA / onderhoud technische afspraken. Een dergelijke connectie wordt afgeraden door de ongecontroleerde aard van de verbinding en heeft een connectie via eigen netwerk de voorkeur.

4.3.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Package unit

4.3.2 Aanvullende best practices (operationele werkwijze)

4G connecties buiten eigen beheer worden afgeraden door de ongecontroleerde aard van de verbinding. Een connectie via eigen netwerk heeft de voorkeur.

5 Internet / Private WAN

'Internet / Private WAN' betreft netwerkverbindingen die zich buiten de organisatie bevinden en niet volledig gecontroleerd zijn door de organisatie. Hierdoor dienen netwerkstromen die gebruik maken van een dergelijke externe connectie via een DMZ te verlopen waarbij strenge netwerkcontrole van toepassing is.

5.1 Publiek internet

Het functionele blok 'Publiek internet' is bestemd voor interfaces / netwerk connecties naar het publieke internet. Connecties die opgezet worden via SSL/TLS vallen onder deze definitie, met uitzondering van VPN technieken die hier gebruik van maken.

5.1.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Hoofdlocatie / RWZI KA
- DMZ KA / Internet
- Hoofdkantoor KA

5.2 Private WAN

Het functionele blok 'Private WAN' is bestemd voor interfaces / netwerk connecties naar locatie overspannende verbindingsoplossingen. Dergelijke verbindingsoplossingen kunnen bestaan uit een:

- Dark fiber verbinding
- Gedeelde fiber verbinding
- Een huurlijn
- Afgenomen MPLS dienst
- Afgenomen APN dienst
- Site-to-site VPN connectie

5.2.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Hoofdlocatie / RWZI PA
- DMZ PA / Private WAN
- Hoofdkantoor PA
- PA-object

5.3 Remote Access (RA)

Het functionele blok 'Remote Access (RA)' is bestemd voor interfaces / netwerk connecties die toegang op afstand faciliteren op persoonlijke basis / voor derden. Dergelijke connecties kunnen bestaan uit:

- VPN connecties
- Remote Access Solutions
- Thuiswerk VDI connecties

5.3.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / Internet

6 KA Omgeving

De IEC 62443 specificeert geen vereisten met betrekking tot de KA omgeving. Van belang is om een fysieke scheiding tussen KA en PA te faciliteren. Dat wil zeggen dat de KA omgeving en de PA omgeving fysiek andere hardware gebruikt. Een koppeling is mogelijk door gebruik te maken van een DMZ.

Als een fysieke scheiding niet mogelijk is, dan moet er een risico-inventarisatie uitgevoerd worden en beheersmaatregelen worden gedefinieerd om (tijdelijk) risico's te mitigeren.

6.1 KA – Beheer

Het functionele blok 'KA – Beheer' is bestemd voor beheer en onderhoudssystemen voor gebruik binnen de KA omgeving. Het functionele blok wordt gebruikt als aanduiding voor servers en werkstations waarmee wijzigingen aangebracht kunnen worden binnen aan KA omgeving.

6.1.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- KA – Servers & Clients

6.2 KA – Servers & Clients

Het functionele blok 'KA – Servers & Clients' is bestemd voor clients en servers voor gebruik binnen de KA omgeving. Het functionele blok wordt gebruikt als aanduiding voor servers, laptops, thin clients en werkstations waarmee de primaire KA processen uitgevoerd kunnen worden.

6.2.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / Internet
- DMZ KA/PA
- KA – Beheer

6.3 OTA (virtueel)

Het functionele blok 'OTA (virtueel)' is bestemd voor een gesimuleerde OTA (Ontwikkeling, Testen en Acceptatie) van de PA omgeving, als een zogenaamde 'digital twin'. Het functionele blok wordt gebruikt voor alle apparaten en virtuele machines nodig voor de virtuele OTA.

6.3.1 Conduits

Er zijn geen connecties met andere functionele blokken, zodoende zijn er geen conduits.

6.3.2 Aanvullende best practices (operationele werkwijze)

De virtuele OTA omgeving heeft geen connectie met andere netwerken waardoor eventuele afhankelijkheden, invloeden van buiten en risico's worden gemitigeerd.

7 Testomgeving

De IEC 62443 specificeert geen vereisten met betrekking tot de OTA (Ontwikkeling, Testen en Acceptatie) omgeving. Van belang is om de een fysieke scheiding tussen OTA en PA te faciliteren. Dat wil zeggen dat de OTA en de PA omgeving fysiek andere hardware gebruikt. Er zal geen directe koppeling zijn met de PA- en KA omgeving, maar toegang is wel mogelijk door gebruik te maken van een DMZ en een stepping stone server.

7.1 OTA

Het functionele blok 'OTA' is bestemd voor een OTA van de PA omgeving, ten behoeve van het testen van updates en aanpassingen in een vergelijkbare (aan de PA) omgeving. Het functionele blok wordt gebruikt voor alle apparaten en virtuele machines nodig voor de OTA.

7.1.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / PA

8 PA Omgeving – PA-object

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussenstaat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

8.1 PA – Systemen en Data

Het functionele blok 'PA – Systemen en Data' is bestemd voor historian servers, domain controllers en MES servers. Het functionele blok wordt gebruikt voor controle van het proces, opslag en ondersteunende diensten.

Hieronder wordt verstaan:

- Historian servers
- Domain Controllers
- MES servers
- Fileservers
- Applicatieservers

8.1.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

8.2 PA – Beheer

Het functionele blok 'PA – Beheer' is bestemd voor engineering servers en -stations. Het functionele blok wordt gebruikt voor servers en werkstations waarmee wijzigingen aangebracht kunnen worden binnen een PA omgeving.

Hieronder wordt verstaan:

- Engineering workstations
- Aankoppelvlakken voor engineering laptops
- Engineering servers

8.2.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

8.3 PA – Wireless apparaten

Het functionele blok 'PA – Wireless apparaten' is bestemd voor apparaten gebruikmakend van draadloze communicatie als primair of secundair middel. Het functionele blok wordt gebruikt voor draadloze modems, draadloze sensoren en andere draadloze communicatie binnen de PA omgeving.

Hieronder wordt bijvoorbeeld verstaan:

- Wireless HART sensoren / gateways;
- 3G/4G modems (bijvoorbeeld voor primaire / secundaire communicatie of private APN);
- GSM modems (bijvoorbeeld voor alarmering);
- LoraWan of andere LPWAN toepassingen;
- Draadloze gebouwautomatisering;
- Bluetooth;
- Wifi routers / access-points.

8.3.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

8.4 PA – Control

Het functionele blok 'PA – Control' is bestemd voor apparaten die voorzien in controle over één of meerdere processen. Het functionele blok wordt gebruikt voor clients, workstations en servers waarmee in aansturing van processen wordt voorzien.

Hieronder wordt verstaan:

- SCADA clients en servers
- HMI's
- DCS clients en servers
- Automation servers
- Visualisatie servers
- Operator workstations

8.4.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / Private WAN
- PA – Beheer
- PA – Wireless apparaten
- PA – IO / PLC
- PA – Safety / Hoog kritisch
- PA – Systemen en data

8.4.2 Aanvullende best practices (operationele werkwijze)

Het functionele blok 'PA – Control' is essentieel in de opzet van een PA-object doordat er wordt voorzien in de essentiële aansturing rol.

8.5 PA – IO / PLC

Het functionele blok 'PA – IO / PLC' is bestemd voor apparaten die voorzien in directe aansturing van een proces en daarbij een aansturing, actuator of sensor rol heeft. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren.

Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

8.5.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

8.6 PA – Safety / Hoog kritisch

Het functionele blok 'PA – Safety / Hoog kritisch' is bestemd voor apparaten die voorzien in safety van een IACS proces of voor apparaten welke een hoog kritische functionaliteit hebben voor het proces. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren met een safety / hoog kritische functionaliteit.

Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

8.6.1 Conduits

De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

Bijlage A Uitgebreide beschrijving functionele blokken PA-Systemen

A.1 Inleiding

Dit document geeft omschrijvingen van de functionele blokken zoals gedefinieerd in de netwerktekeningen 'Hoofdkantoor', 'Hoofdlocatie / RWZI' en 'PA-object' van de 'High-level architectuur Waterschappen' versie 0.92. Een functioneel blok wordt gedefinieerd als een zone waar apparaten, systemen en installaties worden opgenomen die eenzelfde primaire functie hebben. Dit werkt op een vergelijkbare wijze als zones in de IEC 62443 norm. De omschrijvingen bestaan uit:

- Het doel van het functionele blok;
- Voorbeelden van systemen in het functionele blok;
- Gekoppelde functionele blokken & conduits;
- Best practices;
- CSIR referenties.

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en krijgt een naam die een combinatie is tussen de namen van de functionele blokken.

Binnen dit document, wordt uitgegaan van een initieel Security Level (SL) van 2 conform de IEC 62443, deel 3-3. Hogere security levels die mogelijk van toepassing zijn in specifieke functionele blokken kunnen leiden tot aanvullende eisen welke niet in dit document benoemd zijn. De IEC 62443 is een normenkader ten behoeve van cybersecurity in Industriële Automatisering en Controle Systemen (IACS).

Er wordt gebruik gemaakt van gegeneraliseerde referenties naar de Cyber Security Implementatie Richtlijn (CSIR) 1.95. Dit heeft uiting per beschreven functioneel blok door een overzicht te geven van relevante CSIR vereisten ten opzichte van de IEC 62443 3-3 Security Level 2. Dit overzicht is niet specifiek per functioneel blok gedefinieerd en geeft alleen relevante vereisten ten opzichte van IEC 62443 3-3 security level 2. Een overzicht hiervan is toegevoegd aan dit document als bijlage.

Wanneer er afgeweken wordt van de beschreven architectuur, dan is het van belang dit vast te leggen, te verantwoorden en goed te laten keuren door de management verantwoordelijke. Het zogenaamde 'comply or explain'.

A.2 DMZ

A.2.1 DMZ KA / PA

Het functionele blok 'DMZ KA / PA' is bestemd voor communicatie tussen de KA omgeving en PA omgeving waarbij strenge controle wordt uitgeoefend op het netwerkverkeer. Dit wil zeggen dat er niet permanent data wordt opgeslagen in het functionele blok 'DMZ KA / PA', maar er alleen communicatievoorzieningen in worden opgenomen. Het doorzetten van informatie is dus wel mogelijk via deze DMZ en directe communicatie van het ene functionele blok naar het andere functionele blok niet.

Onder communicatievoorzieningen wordt het volgende verstaan:

- Steppingstone server om toegang te krijgen tot de PA omgeving (via bijvoorbeeld RDP)
- Proxyservers
- Transfer fileservers
- Updateservers

A.2.1.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- KA – Servers & Clients
- PA – Systemen en Data
- OTA
- DMZ PA/ES

A.2.1.2 Best practices

DMZ's voorzien in communicatie tussen functionele blokken en deze communicatie verloopt via een firewall. Het doel van een DMZ in combinatie met een firewall is om directe communicatie te voorkomen tussen verschillende functionele blokken. Hierbij is het van belang dat er in de basis geen communicatie plaatsvindt tussen functionele blokken en alleen noodzakelijke communicatie in overleg met alle belanghebbenden. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Binnen de DMZ worden patches direct toegepast zodra deze beschikbaar komen.

De verbonden OTA (Ontwikkeling, Testen en Acceptatie) dient geen onderdeel te zijn van de productieomgeving en hiermee ook geen gebruik te maken van netwerkservices zoals authenticatie, filesharing, DNS, DHCP, etc.

A.2.1.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.2.2 DMZ PA / Private WAN

Het functionele blok 'DMZ PA / Private WAN' is bestemd voor communicatie tussen de PA omgeving en PA blokken/sites verbonden met een WAN connectie waarbij strenge controle wordt uitgeoefend op het netwerkverkeer. Dit wil zeggen dat er niet permanent data wordt opgeslagen in het functionele blok 'DMZ PA / Private WAN', maar er alleen communicatievoorzieningen in worden opgenomen. Het doorzetten van informatie is dus wel mogelijk via deze DMZ en directe communicatie van het ene functionele blok naar het andere functionele blok niet.

Onder communicatievoorzieningen wordt het volgende verstaan:

- Steppingstone server om toegang te krijgen tot verschillende sites
- Proxyservers
- Transfer fileservers
- Updateservers

A.2.2.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- Afstandsbediening
- Hoofdlocatie / RWZI PA
- PA-object
- Hoofdkantoor PA

A.2.2.2 Best practices

DMZ's voorzien in communicatie tussen functionele blokken en deze communicatie verloopt via een firewall. Het doel van een DMZ in combinatie met een firewall is om directe communicatie te voorkomen tussen verschillende functionele blokken. Hierbij is het van belang dat er in de basis geen communicatie plaatsvindt tussen functionele blokken en alleen noodzakelijke communicatie in overleg met alle belanghebbenden. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Binnen de DMZ worden patches direct toegepast zodra deze beschikbaar komen.

A.2.2.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.2.3 DMZ PA / ES

Het functionele blok 'DMZ PA / ES' is bestemd voor communicatie tussen de PA omgeving en extra systemen die communicatie behoeven met de PA omgeving waarbij strenge controle wordt uitgeoefend op het netwerkverkeer. Dit wil zeggen dat er niet permanent data wordt opgeslagen in het functionele blok 'DMZ PA / ES', maar er alleen communicatievoorzieningen in worden opgenomen. Het doorzetten van informatie is dus wel mogelijk via deze DMZ en directe communicatie van het ene functionele blok naar het andere functionele blok niet.

Onder communicatievoorzieningen wordt het volgende verstaan:

- Steppingstone server om toegang te krijgen tot verschillende packages
- Proxyservers
- Transfer fileservers
- Updateservers

A.2.3.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / PA
- PA – Systemen en Data
- PA – Control
- Warmtekrachtcentrale
- Package unit

A.2.3.2 Best practices

DMZ's voorzien in communicatie tussen functionele blokken en deze communicatie verloopt via een firewall. Het doel van een DMZ in combinatie met een firewall is om directe communicatie te voorkomen tussen verschillende functionele blokken. Hierbij is het van belang dat er in de basis geen communicatie plaatsvindt tussen functionele blokken en alleen noodzakelijke communicatie in overleg met alle belanghebbenden. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Binnen de DMZ worden patches direct toegepast zodra deze beschikbaar komen.

A.2.3.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.2.4 DMZ KA / Internet

Het functionele blok 'DMZ KA / Internet' is bestemd voor communicatie tussen de KA omgeving en het internet waarbij strenge controle wordt uitgeoefend op het netwerkverkeer. Dit wil zeggen dat er niet permanent data wordt opgeslagen in het functionele blok 'DMZ KA / Internet', maar er alleen communicatievoorzieningen in worden opgenomen. Het doorzetten van informatie is dus wel mogelijk via deze DMZ en directe communicatie van het ene functionele blok naar het andere functionele blok niet.

Onder communicatievoorzieningen wordt het volgende verstaan:

- Steppingstone server om toegang te krijgen tot de KA omgeving
- Proxyservers
- Transfer fileservers
- Updateservers

A.2.4.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Hoofdkantoor KA
- KA – Servers & Clients
- RA (toegang op afstand)
- Hoofdlocatie / RWZI KA
- Internet

A.2.4.2 Best practices

DMZ's voorzien in communicatie tussen functionele blokken en deze communicatie verloopt via een firewall. Het doel van een DMZ in combinatie met een firewall is om directe communicatie te voorkomen tussen verschillende functionele blokken. Hierbij is het van belang dat er in de basis geen communicatie plaatsvindt tussen functionele blokken en alleen noodzakelijke communicatie in overleg met alle belanghebbenden. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Binnen de DMZ worden patches direct toegepast zodra deze beschikbaar komen.

A.2.4.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.2.5 DMZ PA / Private WAN – PA-object

Het functionele blok 'DMZ PA / Private WAN' is bestemd voor communicatie tussen de PA omgeving en PA blokken/sites verbonden met een WAN connectie vanaf het oogpunt van PA-objecten waarbij strenge controle wordt uitgeoefend op het netwerkverkeer. Dit wil zeggen dat er niet permanent data wordt opgeslagen in het functionele blok 'DMZ PA / Private-WAN', maar er alleen communicatievoorzieningen in worden opgenomen. Het doorzetten van informatie is dus wel mogelijk via deze DMZ en directe communicatie van het ene functionele blok naar het andere functionele blok niet.

Onder communicatievoorzieningen wordt het volgende verstaan:

- Steppingstone server om toegang te krijgen tot het PA-object
- Proxyservers
- Transfer fileservers
- Updateservers

A.2.5.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control
- Hoofdlocatie / RWZI PA
- Hoofdkantoor PA

A.2.5.2 Best practices

DMZ's voorzien in communicatie tussen functionele blokken en deze communicatie verloopt via een firewall. Het doel van een DMZ in combinatie met een firewall is om directe communicatie te voorkomen tussen verschillende functionele blokken. Hierbij is het van belang dat er in de basis geen communicatie plaatsvindt tussen functionele blokken en alleen noodzakelijke communicatie in overleg met alle belanghebbenden. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Binnen de DMZ worden patches direct toegepast zodra deze beschikbaar komen.

A.2.5.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.3 PA Omgeving

A.3.1 PA – Systemen en Data

Het functionele blok 'PA – Systemen en Data' is bestemd voor historian servers, domain controllers en MES servers. Het functionele blok wordt gebruikt voor controle van het proces, opslag en ondersteunende diensten.

Hieronder wordt verstaan:

- Historian servers
- Domain Controllers
- MES servers
- Fileservers
- Applicatieservers

A.3.1.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control
- PA – Beheer
- DMZ KA/PA
- DMZ PA/ES
- DMZ PA/Private WAN
- PA – Safety / Hoog kritisch

A.3.1.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.3.1.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.3.2 PA – Beheer

Het functionele blok 'PA – Beheer' is bestemd voor engineering servers en -stations. Het functionele blok wordt gebruikt voor servers en werkstations waarmee wijzigingen aangebracht kunnen worden binnen een PA omgeving.

Hieronder wordt verstaan:

- Engineering workstations
- Aankoppelvlakken voor engineering laptops
- Engineering servers

A.3.2.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- PA – Control
- PA – Wireless apparaten

A.3.2.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.3.2.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.3.3 PA – Wireless apparaten

Het functionele blok 'PA – Wireless apparaten' is bestemd voor apparaten gebruikmakend van draadloze communicatie als primair of secundair middel. Het functionele blok wordt gebruikt voor draadloze modems, draadloze sensoren en andere draadloze communicatie binnen de PA omgeving.

Hieronder wordt verstaan:

- Wireless HART sensoren / gateways
- 3G/4G modems (bijvoorbeeld voor primaire / secundaire communicatie of private APN)
- GSM modems (bijvoorbeeld voor alarmering)
- LoraWan of andere LPWAN toepassingen
- Draadloze gebouwautomatisering
- Wifi routers / access-points

A.3.3.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Beheer
- PA – Control

A.3.3.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall. Gebruik voor het operationeel toepassen de volgende stappen:

1. Schakel wireless interfaces uit wanneer deze niet in gebruik zijn;
2. Als uitzetten niet mogelijk is, dan moet een risicoanalyse worden uitgevoerd en beheersmaatregelen worden opgesteld;
3. Indien het risico niet geaccepteerd wordt, dan moet de wireless in een eigen zone geplaatst worden, een conduit beschreven worden en moet dit getest worden.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.3.3.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.3.4 PA – Control

Het functionele blok 'PA – Control' is bestemd voor apparaten die voorzien in controle over één of meerdere processen. Het functionele blok wordt gebruikt voor clients, workstations en servers waarmee in aansturing van processen wordt voorzien.

Hieronder wordt verstaan:

- SCADA clients en servers
- HMI's
- DCS clients en servers
- Automation servers
- Visualisatie servers
- Operator workstations

A.3.4.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- PA – Beheer
- PA – Wireless apparaten
- PA – IO / PLC
- PA – Safety / Hoog kritisch
- Package unit
  - Bus koppeling
- DMZ PA / ES

A.3.4.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Bij het functionele blok 'PA – Control' vindt eventueel een direct koppelvlak plaats met Extra Systemen doormiddel van bijvoorbeeld een bus koppeling. Een dergelijke koppeling vindt alleen plaats wanneer een koppeling via een DMZ niet mogelijk is. Documenteer en controleer een dergelijke verbinding streng.

A.3.4.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.3.5 PA – IO / PLC

Het functionele blok 'PA – IO / PLC' is bestemd voor apparaten die voorzien in directe aansturing van een proces en daarbij een aansturing, actuator of sensor rol heeft. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren.

Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

A.3.5.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

A.3.5.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.3.5.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.3.6 PA – Safety / Hoog kritisch

Het functionele blok 'PA – Safety / Hoog kritisch' is bestemd voor apparaten die voorzien in safety van een IACS proces of voor apparaten welke een hoog kritische functionaliteit hebben voor het proces. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren met een safety / hoog kritische functionaliteit.

Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

A.3.6.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Systemen en Data
- PA – Control

A.3.6.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.3.6.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.3.7 Afstandsbediening

Het functionele blok 'Afstandsbediening' is bestemd voor apparaten die voorzien in controle over één of meerdere processen op afstand, zijnde een andere geografische locatie en/of site. Het functionele blok wordt gebruikt voor clients, workstations en servers waarmee in aansturing van processen wordt voorzien. Apparaten in dit functionele blok kunnen ook voorkomen op een 'Hoofdlocatie/RWZI' naast een 'Hoofdkantoor' locatie.

Hieronder wordt verstaan:

- SCADA clients en servers
- HMI's
- DCS clients en servers
- Automation servers
- Visualisatie servers
- Operator workstations

A.3.7.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / Private WAN

A.3.7.2 Uitwijklocatie

In situaties waar de afstandsbediening de primaire manier bediening is in de vorm van een gecentraliseerde controlekamer, dan is een uitwijklocatie een optionele redundantie om te voorzien in hogere uptime.

A.3.7.3 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.3.7.4 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.4 Extra systemen

A.4.1 Warmtekrachtcentrale

Het functionele blok 'Warmtekrachtcentrale' is bestemd voor apparaten die functioneel onderdeel zijn van een warmtekrachtcentrale. Dit is een extra systeem ten opzichte van het primaire proces van waterschappen / hoogheemraadschappen en hierdoor niet noodzakelijk.

A.4.1.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / ES

A.4.1.2 Best practices

Extra systemen betreffen systemen of installaties die niet onderdeel zijn van het primaire proces(sen) van het waterschap / hoogheemraadschap, maar geen KA systeem betreft. Deze systemen kunnen uiteenlopend zijn waardoor de best practice is om deze systemen in een eigen stuk netwerk te plaatsen. Hierbij wordt de communicatie van en naar de systemen streng gecontroleerd.

A.4.1.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.4.2 Package unit

Het functionele blok 'Package unit' is bestemd voor apparaten die functioneel onderdeel zijn van een extra systeem. Dit is een extra systeem ten opzichte van het primaire proces van waterschappen / hoogheemraadschappen en hierdoor niet noodzakelijk.

A.4.2.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / ES
- PA – Control
  - Bus koppeling
- 4G Leverancier

A.4.2.2 Best practices

Extra systemen betreffen systemen of installaties die niet onderdeel zijn van het primaire proces(sen) van het waterschap / hoogheemraadschap, maar geen KA systeem betreft. Deze systemen kunnen uiteenlopend zijn waardoor de best practice is om deze systemen in een eigen stuk netwerk te plaatsen. Hierbij wordt de communicatie van en naar de systemen streng gecontroleerd.

A.4.2.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.4.3 4G leverancier

Het functionele blok '4G leverancier' is bestemd voor interfaces geleverd door de leverancier van het betreffende extra systeem. Dergelijke connecties kunnen door leveranciers opgelegd worden in contractuele / SLA / onderhoud technische afspraken. Een dergelijke connectie wordt afgeraden door de ongecontroleerde aard van de verbinding en heeft een connectie via eigen netwerk de voorkeur.

A.4.3.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Package unit

A.4.3.2 Best practices

Extra systemen betreffen systemen of installaties die niet onderdeel zijn van het primaire proces(sen) van het waterschap / hoogheemraadschap, maar geen KA systeem betreft. Deze systemen kunnen uiteenlopend zijn waardoor de best practice is om deze systemen in een eigen stuk netwerk te plaatsen. Hierbij wordt de communicatie van en naar de systemen streng gecontroleerd.

4G connecties buiten eigen beheer worden afgeraden door de ongecontroleerde aard van de verbinding en heeft een connectie via eigen netwerk de voorkeur.

A.4.3.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.5 Internet / Private WAN

A.5.1 Publiek internet

Het functionele blok 'Publiek internet' is bestemd voor interfaces / netwerk connecties naar het publieke internet. Connecties die opgezet worden via SSL/TLS vallen onder deze definitie, met uitzondering van VPN technieken die hier gebruik van maken.

A.5.1.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Hoofdlocatie / RWZI KA
- DMZ KA / Internet
- Hoofdkantoor KA

A.5.1.2 Best practices

'Internet / Private WAN' betreft netwerkverbindingen die zich buiten de organisatie bevinden en niet volledig gecontroleerd zijn door de organisatie. Hierdoor dienen netwerkstromen die gebruik maken van een dergelijke externe connectie via een DMZ te verlopen waarbij strenge netwerkcontrole van toepassing is.

A.5.1.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.5.2 Private WAN

Het functionele blok 'Private WAN' is bestemd voor interfaces / netwerk connecties naar locatie overspannende verbindingsoplossingen. Dergelijke verbindingsoplossingen kunnen bestaan uit een:

- Dark fiber verbinding
- Gedeelde fiber verbinding
- Een huurlijn
- Afgenomen MPLS dienst
- Afgenomen APN dienst
- Site-to-site VPN connectie

A.5.2.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- Hoofdlocatie / RWZI PA
- DMZ PA / Private WAN
- Hoofdkantoor PA
- PA-object

A.5.2.2 Best practices

'Internet / Private WAN' betreft netwerkverbindingen die zich buiten de organisatie bevinden en niet volledig gecontroleerd zijn door de organisatie. Hierdoor dienen netwerkstromen die gebruik maken van een dergelijke externe connectie via een DMZ te verlopen waarbij strenge netwerkcontrole van toepassing is.

A.5.2.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.5.3 Remote Access (RA)

Het functionele blok 'Remote Access (RA)' is bestemd voor interfaces / netwerk connecties die toegang op afstand faciliteren op persoonlijke basis / voor derden. Dergelijke connecties kunnen bestaan uit:

- VPN connecties
- Remote Access Solutions
- Thuiswerk VDI connecties

A.5.3.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / Internet

A.5.3.2 Best practices

'Internet / Private WAN' betreft netwerkverbindingen die zich buiten de organisatie bevinden en niet volledig gecontroleerd zijn door de organisatie. Hierdoor dienen netwerkstromen die gebruik maken van een dergelijke externe connectie via een DMZ te verlopen waarbij strenge netwerkcontrole van toepassing is.

A.5.3.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.6 KA Omgeving

A.6.1 KA – Beheer

Het functionele blok 'KA – Beheer' is bestemd voor beheer en onderhoudssystemen voor gebruik binnen de KA omgeving. Het functionele blok wordt gebruikt als aanduiding voor servers en werkstations waarmee wijzigingen aangebracht kunnen worden binnen aan KA omgeving.

A.6.1.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- KA – Servers & Clients

A.6.1.2 Best practices

De IEC 62443 specificeert geen vereisten met betrekking tot de KA omgeving. Van belang is om een fysieke scheiding tussen KA en PA te faciliteren. Dat wil zeggen dat de KA omgeving en de PA omgeving fysiek andere hardware gebruikt. Een koppeling is mogelijk door gebruik te maken van een DMZ. Als een fysieke scheiding wordt beschouwd als te duur of niet haalbaar op korte termijn, dan moet er een risico-inventarisatie uitgevoerd worden. Hiermee worden beheersmaatregelen gedefinieerd die (tijdelijk) de risico's mitigeren.

A.6.1.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.6.2 KA – Servers & Clients

Het functionele blok 'KA – Servers & Clients' is bestemd voor clients en servers voor gebruik binnen de KA omgeving. Het functionele blok wordt gebruikt als aanduiding voor servers, laptops, thin clients en werkstations waarmee de primaire KA processen uitgevoerd kunnen worden.

A.6.2.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / Internet
- DMZ KA/PA
- KA – Beheer

A.6.2.2 Best practices

De IEC 62443 specificeert geen vereisten met betrekking tot de KA omgeving. Van belang is om een fysieke scheiding tussen KA en PA te faciliteren. Dat wil zeggen dat de KA omgeving en de PA omgeving fysiek andere hardware gebruikt. Een koppeling is mogelijk door gebruik te maken van een DMZ.

A.6.2.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.6.3 OTA (virtueel)

Het functionele blok 'OTA (virtueel)' is bestemd voor een gesimuleerde OTA (Ontwikkeling, Testen en Acceptatie) van de PA omgeving, als een zogenaamde 'digital twin'. Het functionele blok wordt gebruikt voor alle apparaten en virtuele machines nodig voor de virtuele OTA.

A.6.3.1 Conduits

Er zijn geen connecties met andere functionele blokken, zodoende zijn er geen conduits.

A.6.3.2 Best practices

De IEC 62443 specificeert geen vereisten met betrekking tot de KA omgeving. Van belang is om een fysieke scheiding tussen KA en PA te faciliteren. Dat wil zeggen dat de KA omgeving en de PA omgeving fysiek andere hardware gebruikt. Een koppeling is mogelijk door gebruik te maken van een DMZ.

De virtuele OTA omgeving heeft geen connectie met andere netwerken waardoor eventuele afhankelijkheden, invloeden van buiten en risico's worden gemitigeerd.

A.6.3.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.7 Testomgeving

A.7.1 OTA

Het functionele blok 'OTA' is bestemd voor een OTA (Ontwikkeling, Testen en Acceptatie) van de PA omgeving, ten behoeve van het testen van updates en aanpassingen in een vergelijkbare (aan de PA) omgeving. Het functionele blok wordt gebruikt voor alle apparaten en virtuele machines nodig voor de OTA.

A.7.1.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ KA / PA

A.7.1.2 Best practices

De IEC 62443 specificeert geen vereisten met betrekking tot de OTA omgeving. Van belang is om de een fysieke scheiding tussen OTA en PA te faciliteren. Dat wil zeggen dat de OTA en de PA omgeving fysiek andere hardware gebruikt. Er zal geen directe koppeling zijn met de PA- en KA omgeving, maar toegang is wel mogelijk door gebruik te maken van een DMZ en een stepping stone server.

A.7.1.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.8 PA Omgeving – PA-object

A.8.1 PA – Systemen en Data

Het functionele blok 'PA – Systemen en Data' is bestemd voor historian servers, domain controllers en MES servers. Het functionele blok wordt gebruikt voor controle van het proces, opslag en ondersteunende diensten.

Hieronder wordt verstaan:

- Historian servers
- Domain Controllers
- MES servers
- Fileservers
- Applicatieservers

A.8.1.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

A.8.1.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.8.1.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.8.2 PA – Beheer

Het functionele blok 'PA – Beheer' is bestemd voor engineering servers en -stations. Het functionele blok wordt gebruikt voor servers en werkstations waarmee wijzigingen aangebracht kunnen worden binnen een PA omgeving.

Hieronder wordt verstaan:

- Engineering workstations
- Aankoppelvlakken voor engineering laptops
- Engineering servers

A.8.2.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

A.8.2.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.8.2.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.8.3 PA – Wireless apparaten

Het functionele blok 'PA – Wireless apparaten' is bestemd voor apparaten gebruikmakend van draadloze communicatie als primair of secundair middel. Het functionele blok wordt gebruikt voor draadloze modems, draadloze sensoren en andere draadloze communicatie binnen de PA omgeving.

Hieronder wordt verstaan:

- Wireless HART sensoren / gateways
- 3G/4G modems (bijvoorbeeld voor primaire / secundaire communicatie of private APN)
- GSM modems (bijvoorbeeld voor alarmering)
- LoraWan of andere LPWAN toepassingen
- Draadloze gebouwautomatisering
- Wifi routers / access-points

A.8.3.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

A.8.3.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall. Gebruik voor het operationeel toepassen de volgende stappen:

1. Schakel wireless interfaces uit wanneer deze niet in gebruik zijn;
2. Als uitzetten niet mogelijk is, dan moet een risicoanalyse worden uitgevoerd en beheersmaatregelen worden opgesteld;
3. Indien het risico niet geaccepteerd wordt, dan moet de wireless toepassing in een eigen zone geplaatst worden, een conduit beschreven worden en moet dit getest worden.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.8.3.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.8.4 PA – Control

Het functionele blok 'PA – Control' is bestemd voor apparaten die voorzien in controle over één of meerdere processen. Het functionele blok wordt gebruikt voor clients, workstations en servers waarmee in aansturing van processen wordt voorzien.

Hieronder wordt verstaan:

- SCADA clients en servers
- HMI's
- DCS clients en servers
- Automation servers
- Visualisatie servers
- Operator workstations

A.8.4.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- DMZ PA / Private WAN
- PA – Beheer
- PA – Wireless apparaten
- PA – IO / PLC
- PA – Safety / Hoog kritisch
- PA – Systemen en data

A.8.4.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

Het functionele blok 'PA – Control' is essentieel in de opzet van een PA-object doordat er wordt voorzien in de essentiële aansturing rol.

A.8.4.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.8.5 PA – IO / PLC

Het functionele blok 'PA – IO / PLC' is bestemd voor apparaten die voorzien in directe aansturing van een proces en daarbij een aansturing, actuator of sensor rol heeft. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren. Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

A.8.5.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

A.8.5.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.8.5.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1

A.8.6 PA – Safety / Hoog kritisch

Het functionele blok 'PA – Safety / Hoog kritisch' is bestemd voor apparaten die voorzien in safety van een IACS proces of voor apparaten welke een hoog kritische functionaliteit hebben voor het proces. Het functionele blok wordt gebruikt voor controllers, PLC's, actuatoren en sensoren met een safety / hoog kritische functionaliteit.

Hieronder wordt verstaan:

- PLC's
- Controllers
- Sensoren
- Actuatoren

A.8.6.1 Conduits

Een conduit wordt gedefinieerd als de communicatie tussen twee functionele blokken en daarom krijgt een conduit een naam die een combinatie is tussen de namen van de functionele blokken. De voorgestelde conduits zijn gelijk aan de connecties met de volgende functionele blokken (mits aanwezig):

- PA – Control

A.8.6.2 Best practices

De PA omgeving voorziet in aansturing, onderhoud, beheer en data opslag van technische proces(sen) bij bedrijven waar IACS een centrale rol vervuld in de primaire bedrijfsvoering. Het is van belang onderscheid te maken in functionaliteit bij het inrichten van een PA omgeving, zo wordt onderscheid gemaakt in **aansturing**, **beheer** en **safety**.

Aansturing wordt verder onderverdeeld in aansturing & data verzameling (PA – Systemen en Data), controle over één of meerdere processen (PA – Control) en de uitvoerende/meet elementen (PA – IO / PLC).

Beheer heeft een enkel toegewijd blok (PA – Beheer).

Safety gerelateerde assets worden gescheiden van de rest van de PA omgeving gezien de vaak hoog kritische waarde voor de veiligheid van het proces (PA – Safety / Hoog kritisch). Bij voorkeur gebeurt dit door middel van een fysieke scheiding, waarbij een (eenrichting) terugkoppeling naar het IACS gewenst is ten behoeve van de safety systemen status.

Aanvullend worden alle apparaten gebruikmakend van draadloze communicatie als primair of secundair middel gescheiden van de rest van PA omgeving assets (PA – Wireless apparaten). Dat wil zeggen dat er een boundary apparaat tussen staat waarmee communicatie beperkt kan worden tot het noodzakelijke. Dit kan op basis van een gateway waar communicatie mee gecontroleerd kan worden of een firewall.

Scheid waar het IACS het toelaat de verschillende functionaliteiten logisch of fysiek van elkaar met een firewall als intermediair waarbij alleen noodzakelijke communicatie wordt toegestaan. Dat wil zeggen op basis van adres & poort combinatie en dat de communicatie wordt gedocumenteerd en geaccordeerd door de verantwoordelijke persoon.

A.8.6.3 CSIR referenties

De volgende vereisten vanuit de CSIR zijn relevant voor IEC 62443 3-3 Security Level 2:

- Logische toegang: LP2, LP3, LP4, LP6, LP7, LP8, LP10, LP11, LP12, LP14, LT1, LT2, LT3, LT4, LT5, LT6, LT7, LT9, LT10, LT11, LT12, LT14, LT15, LT16
- Beveiligingsincidenten en incident response plan: IP7, IP8, IT1, IT2, IT3, IT4, IT5
- Netwerkkoppelingen en cryptografie: NP1, NP2, NP3, NP4, NP5, NP7, NP8, NP9, NT1, NT2, NT3, NT4, CP1, CP2, CP3, CP4, CT1, CT2
- Bescherming tegen kwetsbaarheden: AP1, AP2, AP3, AP4, AP5, AT1, AT2, AT3, AT4, HP1, HP2, HP3, HP4, HT1, HT3, HT4, HT5, PP1, PP2, PP3, PP4, PP5, PP6, PT1
- Logging en monitoring: MP1, MP3, MP5, MP6, MP7, MP8, MP9, MP12, MT1, MT2, MT3, MT4, MT5, MT6, MT7, MT8, MT9, MT10, MT13, MT14, MT15, MT16, MT17, MT18, MT19
- Bewustwording en training: TMe11, TMe12, TMe13, TMe14, TMe15, TMe18, TMe23
- Gecontroleerd wijzigen: WP2, WP7, WT2
- Beheer en onderhoud: OP7, OP11, OP12, OT3, OT4
- Back-ups: BP1, BP3, BP4, BT1