PA Zones en conduitsmodel

Hoogheemraadschap Delfland

PA-roadmap

Datum	:	Selectie uit document ten behoeve van aanbesteding project WBS. Volledig document delen na gunning.
Versie	:	
Kenmerk	:	
Classificatie	:	Vertrouwelijk

Eigenaar en beheerder document

Documenteigenaar	
Functie: PA manager	Naam: -
Document beheerder	
Functie: senior beleidsadviseur	Naam: -

Versiebeheer

Versie	**Datum**	**Omschrijving**
3.0	18-2-2025	Stuurgroep PA

Vaststelling en periodieke validatie

Vastgestelde versie	**Datum vaststelling**	**Wie**	**Functie**
3.0	18-2-2025	Stuurgroep PA	Stuurgroep
Volgende validatie	1-12-2025		
Classificatie	Vertrouwelijk		

Registratie

DMS	-

Inhoud

Selectie uit document ten behoeve van aanbesteding project WBS. Volledig document delen na gunning.

1 Het zones en conduitsmodel

1.1 Inleiding

Vanuit de [PA Roadmap] is er naast een scheiding van KA en PA ook een behoefte om het PA-netwerk zo in te delen dat deze robuust is tegen diverse incidenten. Dit document geeft hieraan invulling door het netwerk in zones te verdelen. Maar deze ook te koppelen met conduits om zo de gezamenlijke werking van systemen te behouden.

1.2 Referenties

Referentie	Naam	Versie	Datum	Opsteller
[PA Roadmap]	Roadmap - Netwerkscheiding en Segmentering PA/KA	1.0	27-06-2022	KienIA
[IEC]	IEC62443			IEC

1.3 Kader vanuit de IEC62443

Vanuit de IEC62443-3-2 [IEC] norm dienen bij het opstellen van het zone en conduitsmodel de volgende eisen in acht genomen te worden:

- **ZCR3.1: Bepaal de zones en conduits**; het PA-landschap dient onderverdeeld te worden in zones en conduits op basis van een risicoafweging. Voor de groepering van assets in zones wordt een afweging gemaakt op basis van beveiligingsrisico's, kritiekheid van de assets, de operationele functie, de fysieke of logische locatie en de vereiste toegang tot de systemen. Voor Delfland kunnen we hier denken aan de groepering naar functie (waterveiligheid, waterkwaliteit), de segmentering naar zuiveringskringen en/of boezem versus poldergemalen, maar ook de systeem hiërarchie (volgens ISA88/IEC 62264-1; Purdue model) met onderscheid in Veldnetwerk, Control netwerk, Systeem/bediennetwerk etc. Daarnaast geeft de objectclassificatie een handvat voor de kritiekheid van de verschillende assets.
- **ZCR3.2: Scheidt business en PA-assets;** de KA en PA-assets worden in verschillende zones ondergebracht die logisch dan wel fysiek gescheiden zijn. Dit komt overeen met het advies om PA en KA te scheiden.
- **ZCR3.3: Scheidt safety gerelateerde assets af;** de safety gerelateerde assets moeten ondergebracht worden in een andere zone dan niet safety gerelateerd assets. Dit pleit ervoor om de autonome besturing op het laagste niveau te scheiden van de besturingssystemen op hogere niveaus en bediensystemen
- **ZCR3.4: Scheidt tijdelijk aangesloten apparatuur;** apparatuur zoals bijvoorbeeld een beheer laptop die alleen tijdelijk met het PA-netwerk wordt verbonden voor een onderhoudstaak, moet in een aparte zone worden ondergebracht.
- **ZCR3.5: Scheidt draadloze verbonden apparatuur;** apparatuur die via draadloze netwerken worden verbonden, dient in een apart zone ondergebracht te worden. Dit geldt bijvoorbeeld voor poldergemalen en peilmeetsystemen en andere meetsystemen.
- **ZCR3.6: Scheidt apparatuur verbonden via externe netwerken;** ook deze systemen moeten in een aparte zone ondergebracht te worden. Dit geldt bijvoorbeeld voor weermodellen die gebruikt worden door BOS, maar ook de secundaire gemalen van de gemeentes die gebruikt worden.

Vanuit de IEC-62443 is de volgende stap het bijpassende SL-T niveau per zone vast te stellen. Daarmee wordt bepaald welke beveiligingsmaatregelen uit de IEC-62443 van kracht zijn voor een bepaalde zone. Binnen Delfland volgen we de CSIR als normenkader voor de PA. Bij de objectclassificatie naar weerstandsniveaus zijn alle objecten toegewezen aan weerstandsniveaus 1 en 2. De maatregelen die betrekking hebben op netwerkzonering en -

segmentering zijn voor deze weerstandniveaus gelijk. Daarmee zijn de sets basismaatregelen voortkomend uit de CSIR dus voor alle netwerkzones van de PA hetzelfde.

Tussen de verschillende zones liggen de conduits. De datastromen/uitwisseling die plaats mag vinden over deze conduits wordt in dit zone en conduitsmodel vastgelegd.

Het zo ontstane model vormt het startpunt voor de gedetailleerde risicoanalyse. Uit deze analyse volgt of er nog aanvullende beveiligingsmaatregelen voor bepaalde zones nodig zijn. Deze aanvullende maatregelen zijn bij de betreffende zones en/of conduits aan het model toegevoegd.

1.4 Uitgangspunten en principes

Algemeen:

- Geen directe koppeling van PA met Internet/netwerken van buiten;
- PA bevat wat nodig is voor besturing van de installaties, informatie die hieruit voortkomt voor rapportages, planvorming, e.d. gebeurt in KA. Daarmee vindt ook de historische opslag in KA plaats;
- Horizontaal op basis van hiërarchie in de systeemketen, verticaal op basis van functionele clustering.

Waterketen:

- Opdeling naar zuiveringsketens;
- Bij hoge cyberdreiging eilandbedrijf van zuiveringskring mogelijk.

Watersysteem:

- Waterveiligheid zo lang mogelijk borgen, ook wanneer delen van PA niet meer bereikbaar/bruikbaar zijn;
- Aansluiten bij architectuur vernieuwing BOS;
- Clustering op basis van functies op waterveiligheid. Andere clusteringen die nodig zijn vanuit andere invalshoeken kunnen functioneel altijd gemaakt worden op bv. niveau BOS.

1.4.1 Keuzes PA roadmap leidend

De opdeling in zones en conduits die in dit document zijn beschreven zijn gebaseerd op de besluiten in [PA Roadmap]. Als er meerdere opties voor een keuze worden gepresenteerd in [PA Roadmap] gaan we er in dit document vanuit dat de geadviseerde optie gekozen wordt. Als er toch een andere keuze is gemaakt kan dat effect hebben op de uitwerking van het Zones en Conduits model en zal het ontwerp tegen de uiteindelijke keuze getoetst moeten worden.

1.4.2 Zones en de lagen uit het Purdue model

Van iedere zone wordt aangegeven tot welke laag deze behoord, aan de hand van de aanduiding L0 t/m L6. Dit is gebaseerd op het model van Purdue, zoals deze ook toegepast is bij de IEC62443.

Hierbij is het van belang om in acht te nemen dat deze gelaagdheid iets zegt over de hiërarchie en niet de clustering van zones. Over het algemeen zal een zone verbonden zijn met zones 1 laag boven en 1 laag onder de zone zelf.

Daarnaast geven de lagen ook een indicatie van welke functionele communicatie er in de zone verwacht mag worden.

De betekenis van de lagen is als volgt:

- L6: Internet
- L5: Zones op dit niveau faciliteren de communicatie tussen KA-systemen en systemen op het internet
- L4: Zones op dit niveau faciliteren de communicatie tussen KA-systemen
- L3.5: Zones op dit niveau faciliteren de communicatie tussen KA- en PA-systemen

- L2/3: Zones op dit niveau faciliteren de bediening van systemen door gebruikers
- L1: Zones op dit niveau faciliteren de communicatie tussen bediening en besturing
- L0: Zones op dit niveau faciliteren de communicatie tussen controller en sensoren en actuatoren

Als een zone zich op de grens van deze lagen bevindt of meerdere lagen omvat zullen alle relevante lagen worden aangegeven bij de zone.

1.4.3 Conduits

Een conduit maakt netwerkverkeer mogelijk tussen twee systemen die zich in verschillende zones bevinden. Denk hierbij bijvoorbeeld aan een firewall of router. Hiermee ontstaat de mogelijkheid om netwerkverkeer te filteren en enkel dat door te laten wat toegestaan en noodzakelijk is. Daarmee zijn conduits ook interessante punten in het netwerk om te monitoren door het SOC.

In dit document wordt per conduit vastgelegd met welke zones deze verbonden is. Ook zal per conduit functioneel beschreven worden welke data deze uitwisselt tussen die zones.

1.4.4 PLC’s en veldbusnetwerken

Normaliter is het niet toegestaan dat systemen aan meer dan 1 zone tegelijk verbonden zijn, toch bevat dit document een aantal systemen waarvoor dit wel het geval is.

Het betreft hier PLC’s die naast het controller netwerk ook aan het veldbusnetwerk zijn verbonden. De veldbusnetwerken zijn Profibus-netwerken die niet via netwerkapparatuur, maar via de PLC zijn verbonden. Profibus is niet gevoelig voor cyberaanvallen via het netwerk.

Het toevoegen van een conduit in deze situatie zou de situatie slechts complex in beheer maken, maar het netwerk niet veiliger. Daarom is ervoor gekozen om in dit specifieke geval te accepteren dat PLC-systemen in 2 zones tegelijk kunnen zitten.