Informatisering

Implementatie Visie PA

Hoogheemraadschap van
Delfland

Documentnaam

GE.IN.001 Informatisering

Eigenaar en beheerder document

Documenteigenaar	
Functie: Manager PA	Naam: Casper Braamse
Documentbeheerder	
Functie: PA-adviseur	Naam: Hidde Schouten, Edwin van Velzen

Versiebeheer

Versie	Datum	Omschrijving
0.90	3-2-2025	Eerste versie, afgestemd met: Edwin van Velzen (PA-adviseur), Hidde Schouten (PA-adviseur), Guide Frese (architect), Christiaan van ’t Hoft (architect), Boris van den Berg (ISO PA), Ben Bruinink (functioneel beheerder PA), Johan Witkam (specialist PA), Iris Groenewegen (business consultant), Robin van den Assem (datage-dreven werken). Gereed voor iAdvies op 10 februari 2025.
0.91	10-2-2025	Commentaar van het iAdvies verwerkt. Gereed voor stuurgroep op 18 februari 2025.
1.0	18-2-2025	

Vaststelling en periodieke validatie

Vastgestelde versie	Datum vaststel-ling	Wie	Functie
1.0	18-2-2025	Stuurgroep PA	Stuurgroep
Volgende vali-datie	Q3 2025		
Classificatie	Intern		

Registratie

DMS-nummer: 2402548

Foto voorblad: AI

Hoogheemraadschap van Delfland

Inhoud

1 Implementatie Visie PA

Met het opstellen van de Visie PA is Hoogheemraadschap Delfland (hierna: Delfland) in 2021 gestart op standaardisatie binnen de procesautomatisering (PA). Met project Implementatie Visie PA geven wij handen en voeten aan deze standaardisatie. Dit document, informatisering, is onderdeel van deze standaard.

1.1 Doel van de PA-standaard informatisering

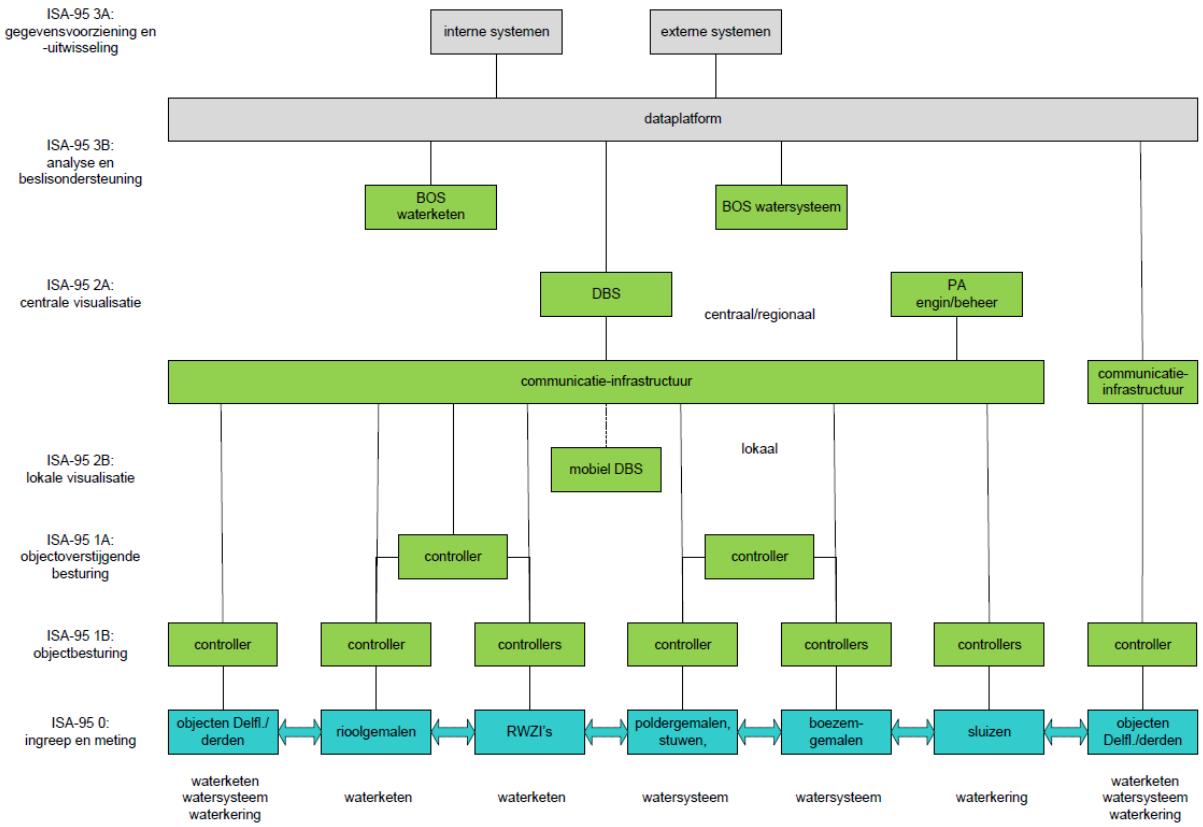
Het doel van dit document is om richtlijnen vast te stellen voor de veilige en efficiënte uitwisseling van gegevens tussen de PA-omgeving (PA) en externe systemen, zoals het kantoornetwerk of slimme oplossingen van derden. De nadruk ligt op het garanderen dat deze gegevensoverdracht plaatsvindt op een veilige, consistente en schaalbare manier. Het doel is om te zorgen voor veilige datastromen zonder unieke oplossingen voor elke koppeling te ontwikkelen, maar in plaats daarvan herbruikbare en generieke paden te creëren. De voordelen hiervoor voor Delfland zijn:

- Hiermee verlagen we de kans dat digitale dreigingen (cyber aanvallen) ons primaire proces aantasten.
- Door het vermijden van maatwerk per datakoppeling, kunnen we de oplossing beter opschalen of wijzigen zonder daarbij te afhankelijk te zijn van één marktpartij (vendor lock-in).

1.1.1 De PA-standaard informatisering is een uitwerking van de PA-visie

De standaardisatie van de PA is een gevolg op de PA-visie. De PA-visie schrijft voor dat de PA flexibel moet zijn en bij moet dragen aan innovaties en de digitale transformatie van Delfland. Hierbij doet de PA-visie een voorzet voor de technische architectuur van de PA, zie Figuur 1. Deze architectuur bevat een centraal dataplatform. Dit is één van de onderwerpen van deze PA-standaard.

De PA-standaard informatisering beschrijft een toekomstige situatie alsof deze al werkelijkheid is. Dat is tijdens het opstellen van dit document nog niet zo. Tijdens het realiseren van de situatie zoals in deze PA-standaard beschreven, is veel samenwerking vereist tussen de verschillende afdelingen van Delfland, zoals BPA, OTI, ICT, IFM, DMA en MWA.



Figuur 1 Potentiële technische architectuur volgens onze PA-visie [kopie uit de PA-visie].

1.1.2 De PA-standaard informatisering sluit aan bij de PA-principes

Eén van de eerste stappen van de implementatie van de PA-visie was het opstellen van de PA-principes. Deze PA-principes zijn gestoeld op de PA-visie, maar ook op de 'Gezamenlijke Architectuurprincipes HHSK, HHD en HHR, werkset ter ondersteuning van projecten' v1.3 uit 2020 (van Hoogheemraadschappen Delfland, Rijnland en Schieland & de Krimpenerwaard). Het gedachtengoed van de meeste van alle twaalf PA-principes is impliciet verwerkt in deze PA-standaard. Twee PA-principes komen expliciet in deze PA-standaard en lichten we daarom uit:

- *Principe 5: Duurzaam & datagedreven - De PA draagt optimaal bij aan duurzaamheid, daartoe werken wij onder architectuur en is de PA toekomstbestendig en ondersteunt en bevordert deze het datagedreven werken.*
  Een randvoorwaarde voor datagedreven werken, is het efficiënt en effectief overdragen van procesdata en sturingsgegevens. Deze PA-standaard geeft hier richting aan.
- *Principe 10: Modulair, uniform en gestandaardiseerd - De PA is functioneel modulair, uniform en volgens courante standaarden ingericht zodat deze flexibel uitbreidbaar en aanpasbaar is, zoals op nieuwe werkwijzen en organisatie.*
  Deze PA-standaard beschrijft een gestandaardiseerde en uniforme informatisering van de PA. Met de richting die deze PA-standaard geeft, is het mogelijk om uitbreiding van de PA modulair uit te voeren.

1.2 Scope van de PA-standaard informatisering

Deze informatienorm beperkt zich tot de PA-omgeving. Dit document richt zich enkel op het faciliteren van gegevensoverdracht van en naar de PA-omgeving en niet op de bredere IT- of kantooromgevingen. Belangrijk is dat dit document geen uitspraak doet over welke data essentieel is voor specifieke functies van slimme oplossingen, maar uitsluitend de mechanismen

beschrijft voor het veilig en schaalbaar verplaatsen van data van externe systemen naar de PA-omgeving en vice versa.

Ook beschrijft dit document de implicaties op gebied van cybersecurity niet, deze worden behandeld in de richtlijnen Security en PA Systeemarchitectuur.

1.3 Leeswijzer

1.3.1 Belangrijke definities en termen

Tabel 1 benoemt sleutelbegrippen die dit document hanteert.

Tabel 1: Sleutelbegrippen in deze richtlijn.

Begrip	Beschrijving
Gegevensoverdracht	Het proces van het verplaatsen van data tussen verschillende systemen.
Historian-systeem	Een time series database (TSDB, geschikt voor opslag van tijdsreeksen) uitgebreid met tooling voor: • data-aggregatie; • validatie; • analyse en trending; • integratie (met PA-systemen zoals PLC/SCADA-systeem of een DCS); • compliance (onder andere beveiliging en audit trails).
Schaalbaarheid	De mogelijkheid om oplossingen voor gegevensoverdracht herbruikbaar te maken voor meerdere dataverbindingen, zonder dat elke koppeling maatwerk vereist.
Veiligheid	De maatregelen die worden genomen om te waarborgen dat gegevensbescherming en toegangscontrole zijn gewaarborgd, zodat externe partijen geen bedreiging vormen voor de PA-processen.

1.3.2 Perspectief van dit document

De opstellers van dit document hebben bewust gekozen een actieve schrijfstijl te hanteren. Dat betekent dat we werkwoorden als ‘zijn’ en ‘worden’ zoveel mogelijk hebben vermeden en in plaats daarvan gebruik hebben gemaakt van een actieve schrijfstijl met de eerste persoonsvorm ‘we’. ‘We’ heeft in dit document geen betrekking op een specifieke functionaris, maar geldt voor Delfland in het algemeen en de verantwoordelijken voor PA in het bijzonder.

2 Systeemoverzicht

2.1 Overzicht van datatypes en functies per ISA-95 niveau

Voor het opzetten van een effectieve en veilige oplossing voor het databeheer in de PA, vereist een goed begrip van de verschillende soorten data die de PA genereert en verwerkt binnen elk niveau van onze PA. Onze lagenstructuur, gebaseerd op ISA-95 (zie PA-visie) biedt een gelaagde structuur waarin elk niveau een specifieke functie heeft en eigen typen data produceert en verwerkt. Deze paragraaf beschrijft de datatypes die typisch voorkomen per ISA-95-niveau, evenals hun bewaartermijnen en de bijbehorende aggregatieniveaus.

Het doel van dit overzicht is om inzicht te geven in de aard en het gebruik van data op elk niveau, van fysieke processen tot operationeel en strategisch management. Dit kader dient als

referentiepunt voor de standaarden en richtlijnen in dit document, en helpt om de functionele eisen en beveiligingsniveaus beter te begrijpen.

Voor de volledigheid benoemt deze paragraaf ook het vierde niveau van de ISA-95 piramide. Deze valt echter buiten de scope van de PA en wordt ook niet door de PA-visie geadresseerd.

Tabel 2: Datavormen per ISA-95 niveau.

Niveau	Type data	Dataformaat	Bewaartermijn	Aggregatieniveau
Level 0	Fysieke meetgegevens	Analoge signalen (bijv. 4-20 mA), directe sensoren en actuatoren	Kortstondig (real-time verwerking, meestal niet opgeslagen)	Directe, ruwe data
Level 1	Besturingssignalen	Digitale signalen (1's en 0's), discrete IO, PLC-input/output	Zeer kort (ms tot sec) voor diagnostiek en troubleshooting	Directe meting en feedbackloops
Level 2	Procesvoeringsdata	Proceswaarden, statusinformatie (bijv. temperatuur, druk)	Korte termijn (dagen tot maanden), afhankelijk van de frequentie van de gegevens en het gebruik in rapportage)	Aggregatie op basis van trenddata en basisstatistieken
Level 3	Productie-informatie en KPI's	Productiedata, orderstatus, energiegebruik, kwaliteitsgegevens	Middellange termijn (dagen tot jaren, afhankelijk van regelgeving en optimalisatie)	Aggregatie per shift, productiebatch, KPI's berekeningen
Level 4	Operationele managementdata	Planning, voorraadniveaus, kwaliteitsstatistieken, onderhoudsstatus	Lange termijn (maanden tot jaren voor compliance en strategische planning)	Aggregatie op bedrijfsniveau: rapportages, historische data-analyse voor trends en verbeteringen

Toelichting per niveau:

- Level 0 (Technologie, fysieke processen)
  - Type Data: Directe sensorgegevens zoals analoge stroom (bijv. 4-20 mA), temperatuur, en druk die fysieke toestanden in het proces meten.
  - Bewaartermijn: Real-time, meestal niet opgeslagen.
  - Aggregatieniveau: Geen aggregatie; alleen ruwe, directe meetgegevens.
- Level 1 (Procesbesturing, objecten en objectoverstijgend sturen)
  - Type Data: Digitale input/output gegevens die de PLC of controllers aansturen, zoals 'aan/uit' en 'open/dicht' signalen.
  - Bewaartermijn: Milliseconden tot seconden, voornamelijk voor directe besturing en troubleshooting.
  - Aggregatieniveau: Minimale aggregatie; feedbacksignalen en diagnostiek kunnen getoond worden.
- Level 2 (Procesvoering, lokale of centrale bediening en monitoring)
  - Type Data: Gegevens over het proces zelf, zoals flow, temperatuur, druk, en andere procesvariabelen.
  - Bewaartermijn: Enkele dagen tot maanden, afhankelijk van de gebruiksdoelen, zoals troubleshooting of trendanalyse.
  - Aggregatieniveau: Basisaggregatie voor trending; data kunnen worden geaggregeerd in gemiddelden of maxima over korte tijdsperioden.
- Level 3 (Analyse, beslisondersteuning, gegevensvoorziening en -uitwisseling)

    - Type Data: Productie-informatie, energieverbruik, orderstatus, KPI's zoals productiviteit en efficiëntie.
    - Bewaartermijn: jaren, voor operationele optimalisatie en historische analyse.
    - Aggregatieniveau: Aggregatie per batch, shift of dag; KPI's en productiecijfers worden samengevoegd in rapportages.
- Level 4 (Bedrijfsmanagement)
    - Type Data: Strategische en operationele data zoals planningsinformatie, voorraadbeheer, kwaliteits- en onderhoudsgegevens.
    - Bewaartermijn: jaren, afhankelijk van de behoeften aan compliance en bedrijfsanalyse.
    - Aggregatieniveau: Data worden geaggregeerd tot hoge niveaus, zoals jaarlijkse rapportages, trendanalyses, en strategische besluitvorming.

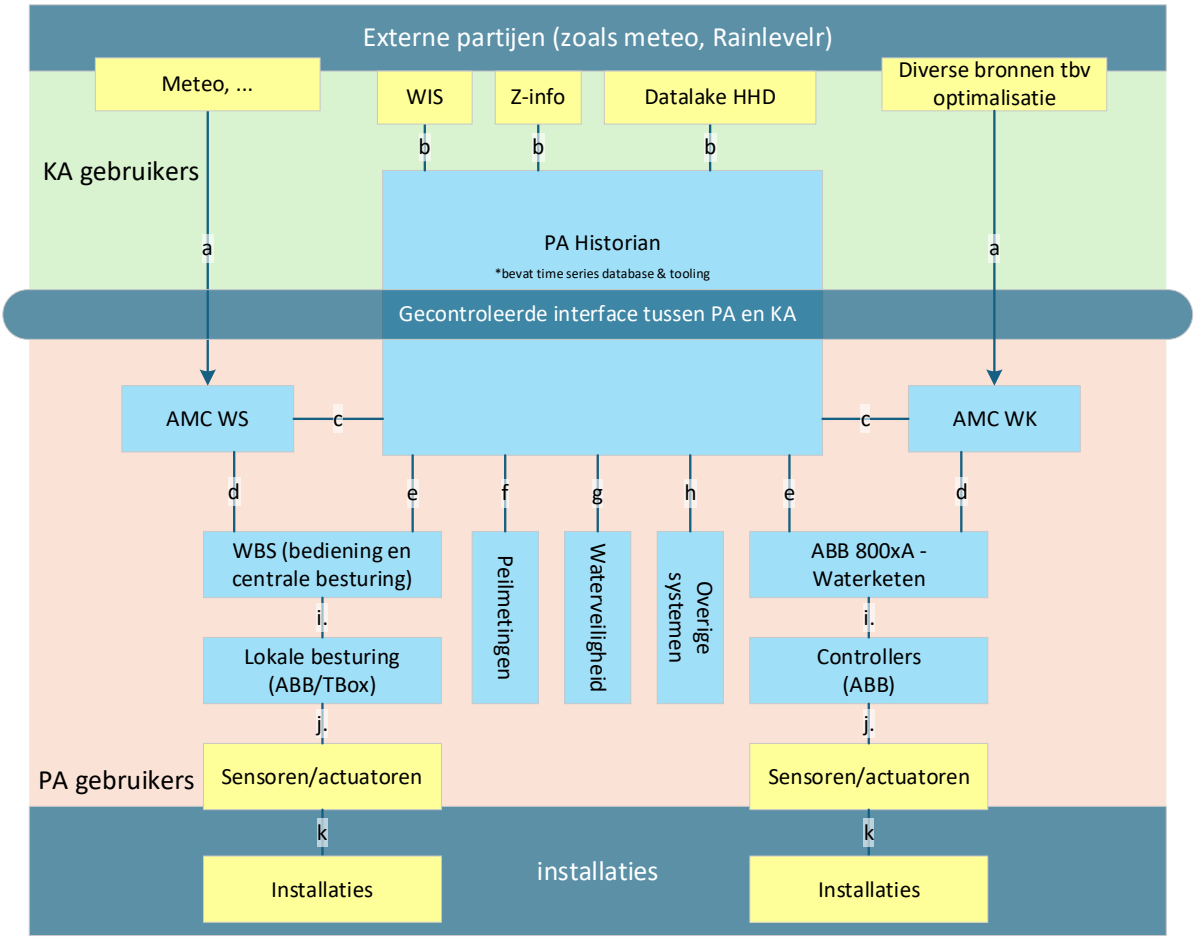
2.2 Systemen en datastromen

2.2.1 Visuele weergave van systemen en datastromen

Figuur 2 geeft een overzicht weer van de belangrijkste systemen binnen de PA-omgeving en zowel hun onderlinge relaties als koppelingen met systemen buiten de PA. Deze visualisatie dient als uitgangspunt voor de verdere beschrijving van datastromen en de rol van verschillende systemen in de architectuur.

De visuele weergave is als volgt opgebouwd:

- Het systeem heeft een gedeelte (rode achtergrond) waarvan specifiek de PA de gebruiker is. Aan de andere kant (groene achtergrond) is een gedeelte van het systeem waarvan de gebruikers KA-zijdig zijn. Hiertussen is een gecontroleerde interface welke subparagraaf 2.2.2 verder toelicht.
- Voor de blauwe blokken geldt dat de PA verantwoordelijk is voor de inrichting en het beheer. De gele blokken liggen buiten de scope van de PA. De gecontroleerde interface tussen de PA en de KA is een gedeelde verantwoordelijkheid van de PA en ICT.



Figuur 2 Overzicht van functionele koppeling tussen PA-systemen en KA.

2.2.2 Toelichting of overzichtsplaat

Figuur 2 toont functioneel hoe verschillende applicaties of systemen met elkaar communiceren. Tabel 3 beschrijft de blokken uit Figuur 2. Bij het maken van het ontwerp van deze architectuur, hebben we enkele belangrijke keuzes gemaakt om de betrouwbaarheid, veiligheid en schaalbaarheid van data-uitwisseling tussen de PA- en KA-omgevingen te waarborgen. Deze keuzes lichten we hieronder toe.

- **Alle procesdata verzamelen we in een time-series database**
  De PA-historian speelt een centrale rol in de architectuur. De PA-historian bestaat onder andere uit een time-series database (TSDB). Alle procesdata komt op de PA-historian binnen en slaan we op in een TSDB. Vanuit de PA-historian distribueren we data naar andere applicaties binnen de PA-omgeving. Ook datastromen naar buiten de PA verlopen via de PA-historian. Deze technologie biedt ondersteuning voor hoge snelheid, schaalbaarheid en het opslaan van tijdgebaseerde gegevens. Dit centrale punt biedt overzicht, uniformiteit en maakt het beheer van datastromen eenvoudiger.
- **Advanced monitoring & control (AMC) aan de PA-kant van het koppelvlak tussen PA en KA**
  De AMC-systemen zijn aan de PA-kant van het koppelvlak gepositioneerd. Hier vallen het huidige en eventueel toekomstige beslissingsondersteunende systemen (BOS) onder. Dit ontwerp zorgt ervoor dat deze systemen rechtstreeks toegang hebben tot procesdata zonder tussenkomst van KA-systemen. Hierdoor blijft essentiële procesinformatie snel en accuraat beschikbaar voor besluitvorming en optimalisatie, ook als de PA in het zogeheten eilandbedrijf gaat.
- **Datastromen tussen AMC en PA-systemen**

AMC-systemen ontvangen data via de PA-historian. Afhankelijk van de inrichting van de PA-historian is het ook mogelijk om via de AMC-systemen commando's naar PA-systemen te sturen. Wanneer lage latentie of specifieke functionaliteit vereist is, gebruiken we een directe koppeling (bijvoorbeeld OPC-UA) tussen het AMC-systeem en de onderliggende PA-systemen.

- **De PA-historian is dé betrouwbare bron van PA-data voor zowel de PA- als de KA-omgeving.**
  We richten de PA-historian zo in dat deze veilig, betrouwbaar en schaalbaar blijft. Dit houdt in dat de PA-historian cybersecure is en bestand tegen bijvoorbeeld overvraging vanuit de KA. De technische invulling (zoals een mogelijke scheiding tussen een PA-deel en een KA-deel) bepalen we tijdens de implementatie, waarbij we leveranciers actief betrekken om mee te denken. Bij PA-eilandbedrijf bufferen we de data in de PA-historian, zodat de KA opnieuw toegang krijgt zodra het eilandbedrijf eindigt.
- **Gecontroleerde interface tussen PA en KA**
  De gecontroleerde interface faciliteert een veilige en betrouwbare datastroom tussen de PA- en KA-omgevingen. Deze interface bevat een hub-functie die de PA-historian ontsluit voor zowel de PA- als de KA-systemen. Voor het integreren van externe gegevens, zoals meteogegevens, zetten we proxy's in. Deze proxy's leveren de data gecontroleerd aan de AMC-systemen, waarbij ze de integriteit en veiligheid van de systemen behouden.

Tabel 3 Systemen uit het overzicht en hun beschrijving.

ISA-95 Niveau	Systeem	Omschrijving
Level 0	Installaties	Fysieke infrastructuur, zoals pompen, gemalen, kleppen, en andere technische installaties.
Level 0	Sensoren en actuatoren	Sensoren meten procesvariabelen (zoals debiet en niveaus), actuatoren sturen fysieke processen aan (zoals kleppen en pompen).
Level 1	Lokale besturing (ABB/TBox)	Decentrale controllers voor het aansturen van waterinstallaties binnen een specifiek gebied.
Level 1	Controllers waterketen (ABB)	Besturingssystemen die processen in de waterzuivering en afvoerketen regelen.
Level 2	Waterbediensysteem (SCADA)	Centraal systeem voor de bediening en monitoring van waterprocessen, inclusief visualisatie en bediening op afstand.
Level 2	ABB 800xA	Specifiek platform voor procesbesturing en monitoring in de waterketen.
Level 1	Peilmetingen (IoT)	Datalogger peilmetingen; waterstanden opslaan en beschikbaar stellen voor draadloze verzending
Level 1-2	Waterveiligheidssystemen	Systemen gericht op het bewaken van waterveiligheid, zoals dijken waterkeringen.
Level 1-2	Overige systemen	Overige systemen; besturingen en SCADA-systemen van overige installaties zoals gemeentegemalen.
Level 3	PA-Historian	Opslag van procesdata vanuit de PA-omgeving, bedoeld voor analyse, rapportage en data-uitwisseling met andere systemen vanuit zowel de PA- als de KA-omgeving.
Level 3	AMC WS	Advanced monitoring & control systemen voor het watersysteem, gebruikt voor tactisch advies,

ISA-95 Niveau	Systeem	Omschrijving
		tactische sturing, optimalisatie en monitoring. Het huidige BOS (beslissingsondersteunend systeem) valt in deze categorie.
Level 3	AMC WK	Advanced monitoring & control systemen voor de waterketen, gebruikt voor tactisch advies, tactische sturing, optimalisatie en monitoring.
Level 3-4	Gecontroleerde interfacing	Beveiligde verbinding voor data-uitwisseling tussen de procesautomatisering (PA) en kantoorautomatisering (KA).
Level 4	WIS (Water Informatie Systeem)	Centraal informatiesysteem voor het beheren en delen van watergerelateerde data binnen de organisatie.
Level 4	Z-info	Specifiek systeem voor het uitwisselen van informatie over waterstanden en -kwaliteit met interne en externe stakeholders.
Level 4	Datalake HHD	Centrale opslag voor organisatiebrede data, waarin waterdata wordt geïntegreerd met andere bedrijfsgegevens.
Level 5	Meteogegevens en internetbronnen	Externe gegevens (zoals weersinformatie) die via KA beschikbaar worden gesteld voor gebruik in AMC WS.
Level 5	Diverse bronnen tbv optimalisatie	Externe gegevens (zoals optimalisatie-algoritmes) die via de KA beschikbaar worden gesteld voor gebruik in AMC WK.

Tabel 4 beschrijft alle dataverbindingen uit Figuur 2. De eerste kolom refereert naar de letter die ook op de afbeelding te zien is. Voor dit overzicht gelden de volgende toelichtingen.

- Niet kritiek in het kader van reactietijd betekent dat de verbinding geen strikte eisen stelt aan hoe snel er data wordt uitgewisseld. Vertraging heeft geen negatieve impact op de werking van het systeem of op de gebruiker.
- ACL staat voor acces control list. Het is een lijst met regels die bepaalt welke gebruikers of systemen toegang hebben tot een specifiek systeem (PA-historian bijvoorbeeld) en welke acties te mogen uitvoeren.
- Real-time betekent een betrouwbare responsetijd. Dat is dus niet hetzelfde als 'heel snel' en kan, afhankelijk van de toepassing, over meerdere minuten gaan.
- De invulling zoals voorgesteld in Tabel 4 kent veel raakvlakken met het 'PA zones- en conduitsmodel' van Delfland, omdat we hier ook met segmentering te maken hebben. We hebben gepoogd geen licht te laten schijnen tussen de opzet in Tabel 4 en het 'PA zones- en conduitsmodel' van Delfland. Mocht dit wel het geval zijn, dan is (de huidige versie van) het 'zones en conduitsmodel' leidend.

Tabel 4 De verbindingen tussen de verschillende systemen.

ID	Betrokken Systemen	Doel van de verbinding	Beveiliging en bescherming	Type Verkeer	Reactietijd
a	Externe gegevens ↔ AMC-systeem	Externe gegevens (bijv. meteo, optimalisatie) beschikbaar stellen aan het AMC-systeem.	Proxy's in de gecontroleerde interface; beperkt tot specifieke datastromen en protocollen.	HTTP(S), REST API, KAFKA gateway	Enkele minuten / uren
b	KA-systeem ↔ PA-historian	KA-systemen (zoals WIS, datalake) voorzien van PA-data via de PA-historian.	Verkeer vindt uitsluitend plaats in de KA-omgeving. ACL's en toegang tot PA-historian gereguleerd.	SQL, OPC-UA, REST API, KAFKA gateway	Niet kritisch (batch)
c	AMC ↔ PA-historian	Verstrekken van procesdata aan AMC-systeem voor beslissingsondersteuning en/of optimalisatie.	Interne firewall binnen PA; ACL's beperken toegang tot relevante datasets.	OPC-UA, SQL	Enkele seconden
d	AMC ↔ PA-systeem (bijv. ABB800xA, WBS)	AMC geeft sturingsadviezen aan PA-systemen (optioneel).	Interne firewall binnen PA; alleen specifieke commando's/protocollen toegestaan.	OPC-UA, Modbus TCP	Kritiek (real-time)
e	PA-historian ↔ PA-systeem (bijv. ABB800xA, WBS)	Verzamelen procesdata uit PA-systemen in de PA-historian.	Interne firewall binnen PA; toegang van systemen tot PA-historian beperkt tot specifieke poorten/protocollen.	Historian-specifieke protocollen, OPC-UA	Enkele seconden
f	PA-historian ↔ Peilmetingen (IoT)	Verzamelen van waterpeildata uit IoT-sensoren voor opslag en analyse.	Beveiliging door segmentatie van IoT-apparaten, proxy's; encryptie van data-invoer naar PA-historian.	MQTT, HTTPS	Enkele seconden
g	PA-historian ↔ Waterveiligheid	Beheer en analyse van waterveiligheidsdata uit objecten zoals sluizen en gemalen.	Firewall binnen PA; voorbereid op segmentatie van toekomstige systemen.	Historian-specifieke protocollen, OPC-UA	Enkele seconden
h	PA-historian ↔ Overige systemen	Integratie van gegevens uit bijvoorbeeld Flygt-gemalen in de waterketen.	Interne firewall binnen PA; alleen datastromen uit specifieke systemen toegestaan.	Historian-specifieke protocollen, OPC-UA	Enkele seconden
i	PA-systeem (ABB800Xa, WBS) ↔ Lokale besturing	Besturing van lokale installaties vanuit WBS of ABB800xA.	Interne firewall tussen SCADA/DCS en PLC's; gebruik van veilige verbindingen en protocollen.	Modbus TCP, OPC-UA	Kritiek (real-time)
j	Lokale besturing/controllers ↔ Sensoren/Actuatoren	Real-time aansturing van apparatuur door PLC's/controllers.	Geïsoleerde verbindingen binnen installaties; geen directe toegang van buitenaf.	Analoge/digitale signalen	Sub-seconden (real-time)
k	Sensoren/Actuatoren ↔ Installaties	Signalen van apparatuur naar sensoren/actuatoren voor procesmonitoring en besturing.	Fysiek geïsoleerd; gebruik van robuuste bekabeling (bijv. 4-20 mA voor analoge signalen).	Analoge/digitale signalen	Sub-seconden (real-time)

3 Gegevensoverdracht

Voor gegevensoverdracht leunen we binnen de PA vooral op organisatiebrede richtlijnen en standaarden. Ook voor de PA kennen we verbijzonderingen; deze zijn opgenomen in de PA-standaard cybersecurity. En aantal kenmerken van de gegevensoverdracht gelden specifiek voor de informatisering en benoemen we daarom in dit hoofdstuk.

3.1 Veilige mechanismen voor gegevensoverdracht

Het veilig overdragen van gegevens tussen de PA-omgeving en externe systemen is cruciaal om onze primaire processen te beschermen. Deze paragraaf zet de belangrijkste mechanismen voor veilige gegevensoverdracht uiteen.

3.1.1 Encryptie

Om de vertrouwelijkheid van gegevens te waarborgen, versleutelen we alle gegevens die tussen de PA en externe systemen worden uitgewisseld. Dit voorkomt dat onbevoegden gevoelige informatie kunnen inzien of manipuleren tijdens de overdracht. Encryptie moet altijd worden toegepast, zowel bij gegevensoverdracht (in transit) als bij opslag (at rest).

3.1.2 Authenticatie en autorisatie

Voordat een systeem of gebruiker gegevens kan verzenden of ontvangen, moet eerst worden gecontroleerd of deze partij geauthentiseerd is. Authenticatie zorgt ervoor dat alleen bekende en vertrouwde entiteiten toegang krijgen. Na authenticatie kennen we autorisatie toe om te bepalen welke specifieke gegevens een gebruiker of systeem mag inzien of wijzigen. We beperken hiermee strikt de toegang tot bevoegde entiteiten.

3.1.3 Aansluiting op netwerkscheiding en zonestructuur

Netwerkscheiding houdt in dat we de PA-omgeving strikt gescheiden houden van de kantoorautomatiseringsomgeving (KA) en externe netwerken. Deze scheiding zorgt ervoor dat kritische procesautomatiseringssystemen niet direct toegankelijk zijn vanuit minder beveiligde omgevingen, waardoor we de veiligheid van onze primaire processen kunnen garanderen. Dit doen we door netwerken op te splitsen in verschillende beveiligingszones, waarbij elke zone specifieke toegangsregels heeft die bepalen hoe gegevens kunnen stromen tussen systemen.

We hebben al een document opgesteld waarin we de netwerkscheiding tussen PA en KA beschrijven, inclusief een zone- en conduitsmodel dat de lagen van onze automatisering verduidelijkt. Dit model vormt de basis voor hoe we gegevens veilig tussen de verschillende lagen en netwerken laten bewegen. In dit document sluiten we aan op dat bestaande model en gebruiken we de goedgekeurde verbindingen en toegangsmechanismen. Zo zorgen we ervoor dat de gegevensoverdracht binnen de vastgestelde zones en conduits plaatsvindt, waarbij de veiligheid en integriteit van onze netwerkscheiding altijd behouden blijft.

3.2 Toegestane applicaties voor gegevensoverdracht

Een veilige en betrouwbare gegevensoverdracht tussen de PA-omgeving en externe systemen betekent ook dat we applicaties gebruiken die aan functionele en beveiligingseisen voldoen. Bij implementatie van deze PA-standaard dienen we een lijst op te stellen met applicaties die hieraan voldoen.

3.3 Goedgekeurde protocollen en beveiligingsmaatregelen

Bij de implementatie van deze PA-standaard stellen we ook een lijst op met goedgekeurde protocollen en beveiligingsmaatregelen voor de verbindingen tussen de PA-systemen en van

de PA-systemen naar de externe (niet-PA) systemen. De kolom “type verkeer” uit Tabel 4 op pagina 12 dient hiervoor als uitgangspunt.

3.4 Monitoring en loggen van gegevens toegang

De PA-standaard security stelt dat we gebruikersgegevens (audittrail) loggen. Vanwege de technische aard van een time-series database is het niet gezegd dat deze data ook daar (dus in de PA-historian) opgeslagen moet worden. Tijdens de implementatie van deze PA-standaard zullen we hier een afweging in moeten maken. Daarnaast verzamelt de data historian zijn eigen logdata, die beschikbaar wordt gesteld aan het Security Operations Center (SoC) voor monitoring en analyse.

4 Gegevensopslag en bewaring

Binnen de PA-omgeving maken we onderscheid tussen de gegevens die direct in de PA-systemen (level 2) worden opgeslagen en de gegevens die in de PA-historian worden beheerd. Met deze opzet blijft de lokale opslag in PA-systemen gericht op operationele stabiliteit, terwijl de centrale PA-historian zorgt voor schaalbaarheid, analyse en integratie met andere systemen.

4.1 Gegevensopslag in PA-systemen (level 2)

PA-systemen, zoals DCS, SCADA of PLC's, slaan voornamelijk procesvoeringsdata op die essentieel is voor de directe besturing en monitoring van installaties. Deze gegevens slaan we meestal in de hardware van de systemen zelf, zoals DCS, SCADA of PLC’s, op. Dit minimaliseert afhankelijkheden en waarborgt een robuuste werking wanneer verbindingen met centrale systemen wegvallen. We hebben het hier over gegevens, zoals:

- Real-time meet- en statusgegevens: Direct gebruikt voor processturing en visualisatie.
- Alarmering en gebeurtenissenlog: Data die nodig is voor het herkennen en oplossen van storingen.
- Tijdelijke opslag: Gegevens die kortstondig worden vastgehouden voor bepaalde regeldoeleinden of voor het maken van trends op de PA-systemen.

Het doel van gegevensopslag op dit niveau is snelheid en operationele betrouwbaarheid, met minimale opslagcapaciteit gericht op actuele behoeften.

4.2 Gegevensopslag in de PA-historian

De PA-historian fungeert als centrale bron voor lange-termijnopslag en analyse van PA-data. Hier slaan we gegevens op die niet alleen relevant zijn voor de PA-omgeving, maar ook beschikbaar moeten zijn voor andere systemen, zoals KA of externe analysetools. Dit omvat:

- Historische meet- en procesgegevens: Gebruikt voor trendanalyses, optimalisatie, en rapportages.
- Samengevoegde en gevalideerde gegevens: Voor betrouwbare besluitvorming en kwaliteitsbewaking.
- Gegevens van externe bronnen: Zoals meteogegevens of optimalisatiemodellen, mits relevant voor PA.

De PA-historian biedt een schaalbare oplossing voor het opslaan van grote hoeveelheden data en waarborgt dat data veilig en gecontroleerd beschikbaar is voor zowel PA- als KA-systemen via de daarvoor gedefinieerde interface.

5 Gegevensvalidatie op verschillende niveaus

Gegevensvalidatie is essentieel om de kwaliteit en betrouwbaarheid van PA-data te waarborgen, zowel binnen de PA-omgeving als bij uitwisseling met andere systemen. Voor de validatie van data geldt het volgende principe:

We valideren data zo laag mogelijk in de informatiehiërarchie.

Door controles zo dicht mogelijk bij de bron uit te voeren, verhogen we de betrouwbaarheid van data in alle bovenliggende systemen en de systemen die daar weer gebruik van maken. Het principe van de gelaagde validatie betekent het volgende:

- **Op sensorniveau en in PLC's (level 1):** Controleert data direct bij het ontstaan, bijvoorbeeld door waarden te valideren op technische plausibiliteit, zoals controle op signalen tussen 4 en 20 mA.
- **In PA-systemen (level 2):** Vindt aanvullende validatie plaats, zoals het combineren van signalen en het herkennen van conflicterende gegevens.
- **In de PA-historian:** Validatie richt zich op complexere analyses, zoals het detecteren van afwijkingen (outliers) met behulp van machine learning of statistische methoden. Deze afwijkingen worden gelabeld, zodat ze herkenbaar blijven in rapportages en analyses.
- **Bij uitwisseling met verschillende systemen:** Bij overdracht van data van verschillende systemen (bijvoorbeeld van de PA-historian naar het WIS) controleren we op de gegevens voldoen aan de gestelde eisen op volledigheid, tijdstempelconsistentie en afgesproken formats.

6 Gegevensaggregatie

Gegevensaggregatie helpt om ruwe data uit de PA-omgeving te vertalen naar bruikbare informatie voor analyses, rapportages en beslissingsondersteuning. Daarnaast rubriceer je de hoeveelheid data door deze te aggregeren, wat de belastbaarheid van de opslag ten goede komt. Gegevensaggregatie valt daarmee uit in twee definities:

- Het comprimeren van data binnen één bron.
- Het bijeenbrengen van data en er één waarheid van maken.

Gegevensaggregatie gebeurt, net als bij gegevensvalidatie, stapsgewijs op verschillende niveaus binnen de systeemhiërarchie, afgestemd op de behoefte en het detailniveau van gebruikers.

We voeren data-aggregatie uit op het niveau dat logisch past bij de complexiteit van de benodigde informatie. Het principe van gelaagde aggregatie betekent het volgende:

- **In PLC's en PA-systemen (level 1 en 2)** voeren we eenvoudige aggregaties uit, zoals gemiddelde waarden, sommaties of maximale/minimale meetwaarden over korte intervallen. Deze basisaggregaties ondersteunen directe procesvoering en lokale visualisaties. Er vindt hier meestal geen samenvoeging van data uit meerdere bronnen plaats.
- **In de PA-historian** gebruiken we meer geavanceerde aggregaties, zoals tijdgebaseerde (bijv. minuut-, uur- of daggemiddelden) en procesgebaseerde samenvattingen. Afhankelijk van de mogelijkheden van het platform kan aggregatie ook plaatsvinden op basis van afwijkingen of trends, bijvoorbeeld door alleen data op te slaan wanneer een signaal sterk verandert of een vooraf gedefinieerde drempelwaarde wordt overschreden. Dit maakt efficiënter gebruik van opslag en helpt bij het signaleren van

relevante gebeurtenissen.
Ook kan de PA-historian data uit meerdere bronnen binnen de PA-omgeving samenvoegen. Dit resulteert in een geïntegreerd overzicht van procesdata

- **In AMC-systemen** gebruiken we geaggregeerde data uit de PA-historian en verrijken deze eventueel met externe gegevens (bijv. weersinformatie) om strategische analyses en tactische sturing mogelijk te maken.

Bij aggregatie houden we rekening met de behoeften van de eindgebruiker. Data voor operationeel gebruik vereist hoge frequentie en detail, terwijl managementinformatie doorgaans geaggregeerd en overzichtelijk moet zijn.

Met een gelaagde aanpak, afgestemd op de inrichting en de mogelijkheden van systemen zoals de PA-historian, zorgen we ervoor dat data op elk niveau aansluit bij de functie en het doel, zonder onnodige belasting van systemen of gebruikers.