Memo

Aan
Algemeen Bestuur

Kopie aan

Van	Doorkiesnummer	E-mail
J.N.J.J. Beemsterboer		
Onderwerp	**Registratienummer**	**Datum**
Cybersecurity vervanging hoofdpost procesautomatisering Watersystemen	25.1131051	12 november 2025

Aanleiding
In het CHI overleg van 15 oktober 2025 is besloten een uitvoeringskrediet ter beschikking te stelling voor het vervangen van de centrale hoofdpost procesautomatisering Watersystemen (Corsa registratie: 25.0984966). Dit is gedaan onder de voorwaarde dat er middels een notitie nadere toelichting wordt gegeven over hoe er in het project voor wordt gezorgd dat de gekozen oplossing voldoet aan de cybersecurity standaarden en -wetgeving. Ik heb de toezegging gedaan u hierover te informeren vóórdat de aanbesteding door het Waterschapshuis gepubliceerd wordt. Inmiddels zijn de voorbereidingen voor de aanbesteding in de afrondende fase en is de publicatie van de aanbesteding gepland op 12 december 2025.
Ik besef dat dit ingewikkelde materie is, maar om een goede duiding te geven ontkom ik er niet aan om hier en daar technisch jargon te gebruiken.

Uiteenzetting feiten
Het waterschap staat voor de taak om vitale waterstaatkundige objecten zoals gemalen, stuwen en meetpunten betrouwbaar en veilig te beheren. Deze objecten worden aangestuurd via procesautomatiseringssystemen die gebruik maken van Operationele Technologie (OT). Deze systemen zijn steeds vaker verbonden met IT-systemen voor data-analyse en sturingsalgoritmes, rapportages en beheer. Dit biedt kansen, maar brengt, mede ingegeven door de geopolitieke situatie, ook beveiligingsrisico's met zich mee.
Cybersecurity is daarom een essentieel onderdeel van de besluitvorming bij de keuze voor een nieuw OT-systeem, zoals de vervanging van de hoofdpost voor het huidige TMX systeem.

Procesautomatiseringssystemen vormen het hart van het operationele waterbeheer. Ze zorgen voor de monitoring, besturing en alarmering van processen die direct invloed hebben op waterveiligheid, waterkwaliteit en infrastructuur. Denk aan het automatisch openen van een sluis bij hoogwater, het aansturen van pompen bij hevige neerslag, of het verzamelen van meetgegevens voor beleidsbeslissingen. Omdat deze systemen onderdeel zijn van vitale infrastructuur, moeten ze voldoen aan strenge eisen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid.

Bij de selectie van de nieuwe hoofdpost wordt het zogenaamde Purdue-model gehanteerd. Dit model biedt een gelaagde structuur waarin OT- en IT-systemen logisch en fysiek van elkaar gescheiden zijn. De lagen variëren van niveau 0 (sensoren en actuatoren die direct het waterproces beïnvloeden) tot niveau 5 (bedrijfsapplicaties zoals e-mail en ERP-systemen). De TMX-hoofdpost

bevindt zich in de middenlagen van dit model (niveau 2/3), waar procescontrole en data-analyse plaatsvinden. Onderstations opereren op niveau 1, terwijl koppelingen met centrale ICT-omgevingen plaatsvinden via een beveiligde bufferzone (DMZ) tussen niveau 3 en 4. Deze segmentatie is essentieel om cyberrisico's te beperken en de continuïteit van waterbeheer te waarborgen. Door deze indeling wordt voorkomen dat kwetsbaarheden in kantooromgevingen direct impact hebben op vitale processen zoals sluisbediening of gemaalsturing. Daarnaast maakt het model het mogelijk om monitoring en logging per segment in te richten, zodat afwijkingen snel worden gedetecteerd en afgehandeld.
Bij het wegvallen van de communicatie vallen de systemen terug op de lokale regelingen in de onderstations (Purduelevel 0/1), zodat de kritische sturing op peilniveaus in de basis kan blijven functioneren. Hiermee blijft het systeem de primaire taken vervullen bij calamiteiten.

In het selectieproces wordt niet alleen aandacht besteed aan de technische aspecten maar, ook de juridische kant is stevig verankerd. Het nieuwe systeem moet voldoen aan de eisen van de Europese NIS2-richtlijn, die aanbieders van essentiële diensten verplicht tot het nemen van passende beveiligingsmaatregelen. Daarnaast is rekening gehouden met de Wet weerbaarheid kritieke entiteiten, die zich richt op het beschermen van vitale infrastructuur tegen verstoringen. Ook de Cyber Resilience Act (CRA) speelt een rol: deze stelt eisen aan veilige softwareontwikkeling, patchbeleid en incidentrespons. Deze wet- en regelgeving is niet slechts een formele verplichting, maar vormt een leidraad voor het ontwerp en de uitvoering van het nieuwe systeem.
In het Programma van Eisen (PvE) en de gunningscriteria wordt expliciet aandacht besteed aan de naleving van deze kaders. Cybersecurity wordt daardoor vanaf het begin meegenomen in het ontwerp van de nieuwe hoofdpost.

Dit principe van "Security by Design" komt o.a. tot uiting in verschillende, hieronder genoemde, onderdelen van de architectuur en het beheer:

- Het systeem maakt gebruik van versleutelde verbindingen (SSL/TLS), gescheiden webapplicaties en databases, en firewallsegmentatie om ongeautoriseerde toegang te voorkomen.
- Verouderde technologieën zoals Java en Flash zijn uitgesloten, om bekende kwetsbaarheden te vermijden.
- Toegangsbeheer is ingericht via een veilige gebruikersinterface die gebruik maakt van Multi-Factor Authenticatie (MFA) en waarin automatische sessie-locks bijdragen aan een veilige gebruikersinteractie. Gebruikersrechten zijn fijnmazig instelbaar, zodat alleen bevoegde personen toegang hebben tot kritieke functies.
- Monitoring en logging zijn conform internationale standaarden ingericht. Logboeken worden versleuteld opgeslagen, zijn traceerbaar en worden minimaal vijf jaar bewaard. Integratie met Security Information and Event Management (SIEM) en Security Operations Center (SOC) maakt het mogelijk om afwijkingen snel te detecteren en te analyseren.
- Patchmanagement en kwetsbaarhedenscans maken het mogelijk om snel te reageren op nieuwe dreigingen. Er is een beleid voor coordinated vulnerability disclosure en gratis beveiligingsupdates, zodat het systeem actueel en veilig blijft.
- Back-up en herstel zijn robuust geregeld: gegevens worden off-site versleuteld opgeslagen en kunnen binnen vier uur worden hersteld.
- Het systeem is geschikt om te kunnen worden ingezet in verschillende redundancy concepten, zoals hot/cold stand-by, fysiek gescheiden van de productieomgeving, zodat bij calamiteiten snel kan worden overgeschakeld.
- Incidentrespons is geborgd via duidelijke procedures voor escalatie en calamiteiten. In geval van verstoring is binnen vier uur een rudimentair werkend systeem beschikbaar, zodat de vitale functies van het waterbeheer niet stilvallen.

Conclusie
De selectiecriteria zoals in de aanbesteding gehanteerd voor de nieuwe hoofdpost systeem zijn niet alleen technisch beschreven, maar ook strategisch verantwoord. Door het toepassen van het Purdue-model, het naleven van actuele wetgeving en het implementeren van best practices op het gebied van cybersecurity, is de weerbaarheid van het systeem structureel geborgd. Dit biedt het bestuur de zekerheid dat het nieuwe OT-systeem niet alleen functioneel sterk is, maar ook veilig, robuust en toekomstbestendig.

Met vriendelijke groet,

J.N.J.J. Beemsterboer
Portefeuillehouder Integraal waterbeheer (landelijk gebied)