Beleid

Package units

Documentatie details

Doelgroep	Afdelingen BWSD, BWK, O&A, S&B, B&O, PR en IV
Classificatie	Intern
Eigenaar	Directeur bedrijfsvoering, CIO
Geldig van tot	Ntb
Laatste review	Ntb
Auteur(s)	Henk Pierik
Status	Definitief
Versie	1.0

Wijzigingsblad

Versie	Datum	Wijziging	Auteur
1.0	26-09-2025	Definitieve versie	Henk Pierik

Inhoud

1. Inleiding 4
2. Doelstelling 4
3. Scope 4
4. Definitie en voorbeelden van Package Units 4
5. Aanleiding 5
6. Aandachtspunten 6
   6.1 Beheer: 6
   6.2 Informatieveiligheid: 6
   6.3 Bedrijfscontinuïteit: 7
   6.4 Data uitwisseling: 8
7. Visie en advies 9
   7.1 Informatieveiligheid en data uitwisseling 9
   7.2 Bedrijfscontinuïteit 9
   7.3 Advies 10
8. Conclusie 10

1. Inleiding

Dit document beschrijft het beleid rondom het gebruik van package units binnen het waterschap.

2. Doelstelling

Het doel is om een kader te bieden voor het zorgvuldig afwegen van het gebruik van package units.

3. Scope

Dit beleid is van toepassing op alle afdelingen die betrokken zijn bij de aanschaf en het beheer van package units.

4. Definitie en voorbeelden van Package Units

Onder een "package unit" verstaan we een geïntegreerd systeem die één of meerdere hardwarecomponenten, zoals bijvoorbeeld een motor, blower, voortstuwer en/of menger, gecombineerd met een eigen besturingseenheid.

Enkele voorbeelden van package units zijn warmte-krachtkoppelingen (wkk) -units), affakkel installaties, visliften, roosterreinigers, blower units, ‘intelligente pompen‘ en ‘intelligente voortstuwers’.

Ook in de software kennen we package units (black-boxes), deze black-box is een bundeling van functionaliteiten, bibliotheken, modules of software delen, welke compleet geleverd worden door een leverancier. Denk hierbij aan bijvoorbeeld de Nereda-procesbesturing van Royal Haskoning, de data gedreven sturing (Treatment System Optimization (TSO)) van Xylem.

5. Aanleiding

Momenteel is er geen duidelijke visie of beleid over het wel of niet toepassen van package units. Ook zijn er geen proces afspraken over het maken van een keuze om wel of niet voor een package unit te kiezen. Hierdoor is de kans groot dat er geen volledig integrale afweging gemaakt wordt, waarbij de risico's voor het primaire proces, de security en de ambities niet tegen elkaar worden afgewogen.

Ook zijn er zorgen over het verwachtingsmanagement; vaak zijn er geen afspraken gemaakt en vastgelegd over het beheer, de verantwoordelijkheid, de gewenste bedrijfscontinuïteit en is er mogelijk geen Service Level Agreement (SLA) bij de unit afgesproken, terwijl er wel een bepaalde verwachting leeft.

Bij de aanschaf van een package unit wordt momenteel voornamelijk gekeken naar het werktuigbouwkundige onderhoud. Echter, vaak is niet duidelijk hoe de informatieveiligheid gedurende de gehele levenscyclus van de unit is geborgd. In het document "Algemene Werktuigbouwkunde Standaard Waterketen" (doc. Zal-st-w-0005) is in hoofdstuk 2.2 beschreven aan welke (voornamelijk werktuigbouwkundige) voorwaarden een package unit moet voldoen. Het beleid voor de eisen in het kader van CSIR (BIO&IEC62443) en NIS2 is daarin niet opgenomen. Maar dat zou wel moeten.

Om een goede afweging te kunnen maken, waarbij alle aspecten worden bekeken, is dit visie, aandachtpunten en adviezen document gemaakt. Dit document beschrijft de aandachtspunten en eigenschappen voor het overwegen van een package unit en geeft een zienswijze op het gebruik ervan.
Hierin worden verschillende aandachtspunten gepresenteerd die kunnen worden meegenomen bij de afweging om een package unit aan te schaffen. Deze aandachtspunten richten zich op aspecten zoals beheer, informatieveiligheid, bedrijfscontinuïteit en data-uitwisseling.

Tevens worden de visie en diverse adviezen beschreven over de keuze voor het wel of niet aanschaffen en gebruiken van een package unit. Daarnaast bevat het document een advies over een alternatief voor een package unit en staan er verschillende adviezen in met betrekking tot het maken en vastleggen van afspraken en verantwoordelijkheden bij de aanschaf van een package unit. Dit hoofdstuk kan gebruikt worden bij de eventuele uitvraag van een package unit.

6. Aandachtspunten

Om een goede afweging te maken over het wel of niet aanschaffen en gebruiken van een package unit, zijn onderstaand een aantal zaken beschreven waarover nagedacht moet worden.

De package units komen voor in verschillende vormen en (onder)delen van het proces. Afhankelijk van de belangrijkheid van de package unit in het proces, de gewenste of noodzakelijke koppeling met de besturingsinstallatie en de gewenste vorm van beheer kan gekozen worden voor het wel of niet toepassen van een package unit. Voor bijvoorbeeld een hydrofoorinstallatie, waarvan alleen de status middels een digitale ingang wordt gekoppeld aan de besturing, kan vanuit het belang voor het proces, en vanuit het cybersecurity oogpunt met minder risico's gekozen worden voor een package unit dan bijvoorbeeld voor een blower installatie, welke essentieel is voor de bedrijfsvoering en waarbij veel data van- en naar de besturing moet gaan.

De besluitvorming dient plaats te vinden op basis van risicoanalyse, SLA-onderzoek en kosten/baten-analyse. De weging van de aandachtspunten dient per geval te gebeuren door o.a. de betrokken assetmanager, de beheerder van de installatie, een specialist onderhoud, een specialist werktuigbouw, een specialist besturingstechniek en een cybersecurityspecialist. Hiervoor zal een proces opgesteld moeten worden en de overweging van de totstandkoming, met de afgewogen criteria, dient vast gelegd te worden.

6.1 Beheer:

- Ontwerp en de realisatie
  Het ontwerp en de realisatie van de package unit gebeurt door de fabrikant of leverancier van de package unit. De afdeling informatievoorziening, het team procesautomatisering is niet betrokken bij het ontwerp van deze specifieke unit en heeft geen inzicht in de gebruikte hard- en/of software en toegepaste informatieveiligheidsveiligheidsnormen. Hierdoor kan de afdeling informatievoorziening, het team procesautomatisering niet (gedelegeerd) verantwoordelijk zijn voor de PA gerelateerde (onderdelen van) de besturing van de package unit of deze units beheren. De verantwoordelijkheid en het beheer van de package unit ligt daarom bij degene die de package unit heeft aangeschaft of beheert.

- Beperkte aanpassingsmogelijkheden:
  Package units worden vaak als kant-en-klare systemen geleverd, wat betekent dat ze mogelijk beperkte flexibiliteit bieden voor aanpassingen aan specifieke behoeften en eisen van onze organisatie.

6.2 Informatieveiligheid:

- Beperkte controle over de informatieveiligheid:
  Package units hebben vaak beperkte mogelijkheden voor het implementeren van specifieke beveiligingsmaatregelen die nodig zijn voor onze organisatie. Het is ook niet altijd duidelijk wat het kennisniveau en naleving van de informatieveiligheidsprocessen en procedures van de betreffende fabrikant of leverancier is. Informatieveiligheid is een belangrijk aspect bij industriële besturingssystemen, en het gebrek aan aanpasbaarheid kan leiden tot beperkte controle over de beveiligingsmaatregelen en mogelijke kwetsbaarheden.

- Potentiële blootstelling aan kwetsbaarheden:
  Package units worden vaak ontwikkeld en getest met een algemeen gebruik in gedachten, waardoor ze mogelijk gevoelig zijn voor bekende kwetsbaarheden. Als er een beveiligingslek wordt ontdekt in een component van de package unit, kan het tijd kosten voordat de fabrikant een patch of een update beschikbaar stelt. Het is maar de vraag of de leverancier hier zicht op heeft en actief met het dichten van de lek bezig gaat. De leverancier kan moeilijk het risico van de lek voor onze organisatie inschatten. Het team procesautomatisering heeft geen zicht op de gebruikte componenten, systemen, software en mogelijke veiligheidslekken in deze systemen. Dit vergroot het risico op potentiële aanvallen en inbreuken op de informatieveiligheid.

- Naleven cyber security eisen
  Om te voldoen aan de informatieveiligheidseisen voor de procesautomatisering zijn o.a. de IEC62443 norm en de CSIR richtlijn opgesteld. Het team procesautomatisering heeft geen zicht of het product en de leverancier voldoen aan de technische-, proces- en procedure eisen uit deze norm en richtlijn. Ook kunnen we deze leveranciers niet auditen op het naleven van de prosessen en procedures.

6.3 Bedrijfscontinuïteit:

- Afhankelijkheid
  Met package units wordt een afhankelijkheidsrelatie gecreëerd met de leverancier. Als er problemen voordoen of er behoefte is aan technische ondersteuning, is het waterschap volledig afhankelijk van de leverancier of fabrikant. Dit kan de reactietijd en de flexibiliteit bij het beheer van het systeem beperken. Ook is het de vraag of die leverancier in een service level argemeent (SLA) een continuïteit/ beschikbaarheid 24x7x365 SLA kan bieden. Als de leverancier een 24x7x365 SLA kan bieden, dan dient het waterschap hier ook op ingericht te zijn, zodat adequaat gereageerd kan worden op bijvoorbeeld het verzoek voor (digitale) toegang voor beheer (op afstand) van de leverancier.
  De kennis van de package unit is aanwezig bij de leverancier of fabrikant. Op het moment dat de leverancier of fabrikant er niet meer is, is het maar de vraag wie de package unit kan aanpassen, kan updaten of kan onderhouden. Hierdoor kan de bedrijfscontinuïteit van een package unit een probleem zijn.

- Eigenaarschap
  Het waterschap is (en blijft) eigenaar van de package unit, en draagt daarmee de volledige (eind)verantwoordelijkheid voor de continuïteit van het geheel. Om de continuïteit te borgen dient het waterschap de mogelijkheid te hebben om pentesten te kunnen (en mogen) doen. Ook dient het waterschap van de leverancier de rapportages t.a.v. de testen- en uitgevoerde maatregelen om de continuïteit te borgen, te ontvangen.

6.4 Data uitwisseling:

- Uitdagingen en beperking in gegevensuitwisseling
  De package units kunnen niet volledig geïntegreerd worden met onze eigen automatiseringssystemen. Dit bemoeilijkt en beperkt de uitwisseling van gegevens en de communicatie tussen verschillende systemen. De beperking van de data uitwisseling kan het operationele proces nadelig beïnvloeden. De beperking wordt o.a. veroorzaakt omdat we geen 'vreemden onderdelen"/ package units opnemen in het netwerk met de procesautomatisering. Vanwege het ontbreken van een netwerk koppeling dient de informatie-uitwisseling te gebeuren via fysieke digitale- en analoge in- en uitgangssignalen.

De aandachtspunten beheer, de informatieveiligheid, de bedrijfscontinuïteit en data-uitwisseling dienen per proces en installatie(deel) door de betrokken personen afgewogen moeten worden, om de juiste keuze te maken voor het wel of niet aanschaffen van een package unit. De keuze welke leidt tot de besluitvorming dient vast gelegd te worden.

7. Visie en advies

De onderstaande adviezen zijn opgesteld op basis van de bovenstaande aandachtspunten.

7.1 Informatieveiligheid en data uitwisseling

- Verwachtingen, afspraken en verantwoordelijkheid
  Indien een package unit aangeschaft wordt, dienen de verwachtingen, afspraken en verantwoordelijkheid t.a.v. de zaken voor de informatieveiligheid en mogelijke data uitwisseling beoordeelt, beschreven en vastgelegd te worden. Ook moeten de eventuele rest risico's benoemd en geaccepteerd worden. Daarnaast dient, indien gewenst, een SLA met de leverancier afgesproken te worden. Deze zaken dienen in een overeenkomst met de leverancier vastgelegd te worden.

- Informatieveiligheidsafspraken
  Indien een package unit aangeschaft wordt, moeten er afspraken gemaakt en vast gelegd worden over de informatieveiligheid. Denk hierbij aan afspraken over pentesten, het up-to-date houden van de besturing van de package uit, het verhelpen van de optredende kwetsbaarheden en veiligheidslekken in het besturingssysteem.

- Afspraken verificatie van informatieveiligheidseisen
  Indien een package unit aangeschaft wordt, moeten de door te voeren eisen en activiteiten vanuit de BIO, IEC62443, CSIR en NIS2 vastgelegd worden. Ook dienen er afspraken gemaakt te worden over hoe deze eisen aangetoond worden.

7.2 Bedrijfscontinuïteit

- Bescherming van broncode en ontwerp documentatie
  Indien een package unit aangeschaft wordt, waarvan het voortbestaan belangrijk is voor de procesvoering, is het advies om een Escrow-overeenkomst[1] af te sluiten met de leverancier en een Escow-agent. Met deze regeling kan het waterschap op het moment dat een leverancier niet meer kan leveren door bijvoorbeeld een faillissement, het stoppen met een product, of door het niet voldoen aan leveringsverplichtingen, beschikking over o.a. de broncode. Ook is het belangrijk dat geregeld wordt dat onder die omstandigheden de functionele beschrijving en andere ontwerpdocumenten beschikbaar komen voor het waterschap.

- Voorkomen van kinderziektes
  Indien een package unit aangeschaft wordt, moet er een keuze gemaakt worden in de aan te schaffen versie van de technische oplossing. Om kinderziektes te voorkomen en geen proeftuin te zijn van de leverancier, is het aan te raden om een N-1 versie aan te schaffen. (Hierbij staat "N" voor de huidige versie, "N-1" verwijst naar de vorige versie. (N-1 verwijst naar de versie die één iteraties terug is van de huidige versie.)

[1] Een Broncode of Software Escrow is een overeenkomst waarin een softwareleverancier of -distributeur en waterschap overeenkomen dat de leverancier de broncode van een softwareproduct via een escrow agent deponeert voor het waterschap. Hiermee zorg je dat de softwareproducten die zij ontwikkeld hebben of aanbieden, veiliggesteld worden door de escrow agent.

- Continuïteitsborging door leveranciers
  Indien een package unit aangeschaft wordt, is het advies om de leverancier rapportages te laten aanleveren t.a.v. de testen- en uitgevoerde maatregelen om de continuïteit te borgen.

7.3 Advies

- Overwegingen voor gebruik van package units
  Vanwege de beschreven punten t.a.v. het beheer, de informatieveiligheid, bedrijfscontinuïteit en de data uitwisseling is het advies om geen gebruik te maken van package units. Tenzij er aandachtspunten of zwaarwegende redenen zijn om toch package units aan te schaffen.
  Om de aandachtspunten goed, en met de juiste betrokkenen te wegen, is het nodig om o.a. de positie, afhankelijkheden, de belangrijkheid van de unit in het proces en eventuele alternatieven te kennen.
  Daarnaast dient een risicoanalyse gemaakt te worden t.a.v. de uitval van de unit of procesdeel. Ook een mogelijke Service Level Agreement (SLA) op de unit en organisatie dient onderzocht te worden. Daarnaast dienen de aandachtspunten t.a.v. de informatieveiligheid en mogelijke data uitwisseling beoordeelt te worden. Tevens dient het gewenste beheer van de gehele unit en een kosten/baten analyse meegenomen te worden.
  Indien er wel voor een package unit wordt gekozen, maak dan afspraken over onder andere de informatieveiligheid, Escrow, versiebeheer en continuïteitsborging

- Alternatief voor package unit
  Als alternatief voor een package unit kan de beoogde leverancier van de package unit gevraagd worden om een (deel) installatie zonder besturing te leveren, aangevuld met de functionele beschrijving en/of het technisch ontwerp. Met deze beschrijving kan het team procesautomatisering ervoor zorgen dat deze functionaliteit in de door hen beheerd systeem wordt geprogrammeerd. Hiermee wordt dit een onderdeel van de reguliere besturing van het waterschap welke het team procesautomatisering beheert en zij voor verantwoordelijk zijn.

8. Conclusie

Het beleid biedt ruimte voor maatwerk en stimuleert toekomstgerichte keuzes en is bedoeld om per situatie een integrale afweging te maken over het wel of niet toepassen van een package unit, waarbij risico's voor het primaire proces, security en ambities expliciet tegen elkaar worden afwegen. Het is dus geen verbod, maar een kader voor zorgvuldige en weloverwogen besluitvorming, gedragen door meerdere belanghebbenden. Het beleid biedt ruimte voor maatwerk en staat de stap naar de toekomst niet in de weg, mits deze voldoen aan de randvoorwaarden voor veiligheid, beheer en continuïteit.

Het advies is om geen gebruik te maken van package units vanwege zorgen over het beheer, de informatieveiligheid, de bedrijfscontinuïteit en de data-uitwisseling, tenzij er belangrijke redenen zijn om dit toch te doen.
Indien er wel gekozen wordt om een package unit in te zetten, dan is het advies om de bovenstaande aandachtpunten met de leverancier af te stemmen en vast te leggen.