

# Operationele Technology

## Thema architectuur

### Gemeente Utrecht



concept  
versie 0.2; 21-01-2026

# Colofon

## **Uitgave**

architect@utrecht.nl

## **In opdracht van**

Stadsbedrijven

Informatie- en Procesmanagement

## **Rapportage**

Architectuur Community

## **Opstellers**

Frans de Waal

Frank Gerwig

## Versiebeheer

| Versie | Datum      | Auteur(s)  | Wijziging                                 |
|--------|------------|------------|-------------------------------------------|
| 0.1    | 23-12-2025 | F. de Waal | Initiële versie                           |
| 0,2    | 19-01-2026 | F. Gerwig  | Purdue referentie architectuur toegevoegd |
|        |            |            |                                           |
|        |            |            |                                           |
|        |            |            |                                           |
|        |            |            |                                           |

## Kennisdelen

| Naam     | Functie                 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.94 |
|----------|-------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|
| IPM team | IPM team Stadsbedrijven | x   |     |     |     |     |     |     |     |     |      |
|          |                         |     |     |     |     |     |     |     |     |     |      |
|          |                         |     |     |     |     |     |     |     |     |     |      |
|          |                         |     |     |     |     |     |     |     |     |     |      |
|          |                         |     |     |     |     |     |     |     |     |     |      |
|          |                         |     |     |     |     |     |     |     |     |     |      |

## Verklarende woordenlijst

Zie bijlage

## Relevante Documenten

- Enterprise Utrecht Architectuur & thema architecturen Data, Integratie, Security, Common Ground
- [Gartner] diverse documenten uit repository
- [Purdue] NIS2 en Purdue model [Het Purdue Model: Een heruitvinding voor de NIS2 Normering \(silta-ict.be\)](#)
- [BIO] Baseline Informatiebeveiliging Overheid (BIO), maatregel 6.1.1.4, v1.0.4zv, 17 juni 2020.
- [HH] beveiligen Operationele Technology voor gemeenten [Beveiliging van Operationele Technologie \(OT\) door gemeenten \(dehaagsehogeschool.nl\)](#)
- [BOMM] Bommel van, S.: De volgende uitdaging van de IT-auditor: Operationele Technologie, in: de IT-auditor, editie 2-2020, 16 juni 2020.
- [TG] verminderen kwetsbaarheden en risico's IT/OT [Verminderen kwetsbaarheid en risico's IT/OT integratie in het waterdomein \(twynstragudde.nl\)](#)
- [BUUR] Buuren van, E: Wat betekent de NIS2-richtlijn voor onze decentrale overheid?, website Kenniscentrum Europa Decentraal (KED), 17 februari 2023.
- [DIGI] Operationele Technology, website digital trust center van het Ministerie van Economische Zaken en Klimaat.

- [IEC] IEC 62443-2-1, Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security Program, edition 1.0, 2010-11.
  - [IIA] The IIA's three lines model, An update of the Three Lines of Defense, Institute of Internal Auditors (IIA), juli 2020.
  - [ISO15] NEN-EN-ISO 9001:2015 (nl), kwaliteitsmanagementsystemen – eisen, ICS 03.120.10 oktober 2015.
  - [ISO22] ISO / IEC 27001:2022 (nl), Informatiebeveiliging, cybersecurity en bescherming van de privacy – managementsysteem voor informatiebeveiliging – eisen, derde editie, 2022-10.
  - [NCSC] Nationaal Cyber Security Centrum (NCSC), Wbni-melding, website NCSC, 5 maart 2023. [NCSC - Operationele Technology](#)
  - [NIB1 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Europese Raad, houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, 6 juli 2016.
  - [NOREA] Handreiking voor SOC 2 en SOC 3 op basis van ISAE3000 / Richtlijn 3000A, Nederlandse Orde van Register EDP-auditors (NOREA), december 2021.
  - [VIEL] Vielberth, M., Böhm, F., Fichtinger I., en Pernul, G.: Security Operations Center: A Systematic Study and Open Challenges, in: IEEE Access, 31 december 2020
- [PZH] Aanbevelingen uit een casestudy bij de provincie Zuid-Holland [NOREA | Cybersecurity van Operationele Techniek](#)

# Inhoudsopgave

|           |                                                                                                                                                  |           |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1.</b> | <b>INLEIDING .....</b>                                                                                                                           | <b>8</b>  |
| 1.1       | DOEL VAN OT THEMA ARCHITECTUUR .....                                                                                                             | 9         |
| 1.2       | DOELGROEP DOCUMENT .....                                                                                                                         | 9         |
| 1.3       | SCOPE OT THEMA ARCHITECTUUR .....                                                                                                                | 10        |
| 1.4       | LEESWIJZER.....                                                                                                                                  | 11        |
| 1.5       | RELATIE MET ANDER GEMEENTELIJKE DOCUMENTEN.....                                                                                                  | 12        |
| <b>2.</b> | <b>CONTEXT OT BINNEN DE GEMEENTE UTRECHT .....</b>                                                                                               | <b>13</b> |
| 2.1       | DEFINITIE OT .....                                                                                                                               | 13        |
| 2.2       | ONTWIKKELINGEN DIGITALISERING IoT, IT/OT INTEGRATIE.....                                                                                         | 13        |
| 2.3       | WETTELIJKE EN NORMATIEVE KADERS.....                                                                                                             | 13        |
| 2.4       | POSITIONERING MET BETREKKING TOT DE ENTERPRISE ARCHITECTUUR UTRECHT .....                                                                        | 14        |
| 2.5       | SAMENHANG ANDERE THEMA ARCHITECTUREN .....                                                                                                       | 15        |
| <b>3.</b> | <b>ARCHITECTUURPRINCIPES OT .....</b>                                                                                                            | <b>17</b> |
| 3.1       | PURDUE REFERENTIE ARCHITECTUUR.....                                                                                                              | 17        |
| 3.2       | IMPLICATIES VAN ARCHITECTUURPRINCIPES .....                                                                                                      | 17        |
| 3.3       | KOPPELING PRINCIPES .....                                                                                                                        | 18        |
| <b>4.</b> | <b>OT-REFERENTIE ARCHITECTUUR.....</b>                                                                                                           | <b>20</b> |
| 4.1       | ARCHITECTUURPRINCIPES .....                                                                                                                      | 20        |
| 4.2       | PURDUE MODEL .....                                                                                                                               | 20        |
| 4.1       | LOGISCHE OT-ARCHITECTUUR .....                                                                                                                   | 21        |
| 4.2       | FYSIEKE OT-INFRASTRUCTUUR.....                                                                                                                   | 22        |
| 4.3       | OPERATIONELE OT-INFRASTRUCTUUR.....                                                                                                              | 22        |
| 4.4       | ZONES EN CONDUITS (IEC-62443).....                                                                                                               | 22        |
| <b>5.</b> | <b>ORGANISATIE&amp; GOVERNANCE .....</b>                                                                                                         | <b>25</b> |
| 5.1       | NIEUWE CAPABILITY “BEHEER OT” .....                                                                                                              | 25        |
| 5.2       | GEWIJZIGDE BEDRIJFSFUNCTIES.....                                                                                                                 | 26        |
| 5.3       | ROLLEN, TAKEN EN VERANTWOORDELIJKHEDEN.....                                                                                                      | 28        |
| 5.4       | RASCI-TABEL – FUNTIONEEL BEHEER OT-SYSTEMEN .....                                                                                                | 34        |
|           | BINNEN HET DOMEIN FYSIEKE LEEFOMGEVING. BEHEER VAN DE REFERENTIEARCHITECTUUR (EIGENAARSCHAP, WIJZIGINGEN, ARCHITECTUURBOARD, VERSIEBELEID) ..... | 34        |
| <b>6.</b> | <b>HOOFDPROCES LEVENSCYCLUS OT-SYSTEEM .....</b>                                                                                                 | <b>37</b> |
| 6.1       | OT-SYSTEEM ONTWERP EN REALISATIE ONDER ARCHITECTUUR.....                                                                                         | 37        |
| 6.2       | NIEUW INSTRUMENT KWETSBAARHEID- EN RISICOANALYSE OT-SYSTEEM .....                                                                                | 38        |
| 6.3       | AANSLUITVOORWAARDEN / NON-FUNCTIONALS VOOR OT-SYSTEMEN.....                                                                                      | 38        |
| 6.4       | NIEUWE WERKWIJZEN FUNCTIONEEL BEHEER OT-SYSTEEM.....                                                                                             | 39        |
| 6.5       | CYBER SECURITY MANAGEMENT SYSTEM .....                                                                                                           | 40        |
| 6.6       | CYBERSECURITY OP STRATEGISCH EN TACTISCH NIVEAU .....                                                                                            | 40        |

|           |                                                                    |           |
|-----------|--------------------------------------------------------------------|-----------|
| 6.7       | ORGANISEER HET BEHEER VAN DE OT STRUCTUREEL .....                  | 40        |
| 6.8       | PREVENTIEF BEHEER OM CYBERSECURITY INCIDENTEN TE VOORKOMEN .....   | 40        |
| 6.9       | RICHT BUSINESS CONTINUÏTEIT MANAGEMENT .....                       | 40        |
| <b>7.</b> | <b>NIEUWE ARCHITECTUUR BOUWBLOKKEN (ABB'S) .....</b>               | <b>41</b> |
| 7.1       | GEBRUIK ARCHITECTUUR BOUWBLOKKEN ANDERE THEMA ARCHITECTUREN .....  | 43        |
| 7.2       | BESCHRIJVING VAN ARCHITECTUUR BOUWBLOKKEN .....                    | 44        |
| <b>8.</b> | <b>ARCHITECTUUR PATRONEN .....</b>                                 | <b>47</b> |
| 8.7       | PRINCIPES VOOR IT-OT-ARCHITECTUUR BINNEN DE GEMEENTE UTRECHT ..... | 47        |
|           | <i>Scheiding van domeinen</i> .....                                | 47        |
|           | <i>Standaardisatie van bouwblokken</i> .....                       | 47        |
|           | <i>Security by design</i> .....                                    | 47        |
|           | <i>Herbruikbaarheid</i> .....                                      | 47        |
| 8.8       | STRUCTUUR VAN ARCHITECTUURBOUWBLOKKEN .....                        | 48        |
| 1.        | <i>Identificatie</i> .....                                         | 48        |
| 2.        | <i>Archimate-representatie</i> .....                               | 48        |
| 3.        | <i>Functionele beschrijving</i> .....                              | 48        |
| 4.        | <i>Security &amp; compliance aspecten</i> .....                    | 48        |
| 5.        | <i>Integratie aspecten</i> .....                                   | 48        |
| 8.9       | BOUWBLOKKEN VOOR IT-OT-INTEGRATIE VOLGENS HET PURDUE-MODEL .....   | 49        |
| 1.        | <i>OT-bouwblokken (Purdue-levels 0-3)</i> .....                    | 49        |
| 2.        | <i>DMZ-bouwblokken (Purdue-levels 3.5)</i> .....                   | 49        |
| 3.        | <i>IT-bouwblokken (Purdue levels 4-5)</i> .....                    | 49        |
| 8.4       | MODELLEREN VAN IT-OT-INTEGRATIE IN ARCHIMATE .....                 | 50        |
| 8.5       | GOVERNANCE EN BEHEER IN DE EA-REPOSITORY .....                     | 50        |
| 8.1       | GEBRUIK VAN ARCHITECTUURBLOKKEN .....                              | 51        |
| <b>9.</b> | <b>BIJLAGEN .....</b>                                              | <b>52</b> |

# Management samenvatting

## Operationele Technologie Thema Architectuur

### Gemeente Utrecht

De Gemeente Utrecht werkt aan een veilige, bereikbare en toekomstbestendige stad. kritieke infrastructuur zoals bruggen, sluizen, gemalen en gebouwen speelt hierin een essentiële rol. Deze infrastructuur wordt aangestuurd door Operationele Technologie (OT), en is direct van invloed op de publieke veiligheid, bereikbaarheid van de stad en continuïteit van de dienstverlening. Tegelijkertijd zet Utrecht sterk in op digitalisering en data gedreven werken, waarbij de behoefte groeit om data uit deze infrastructuur beter te benutten.

Dit document beschrijft de generieke referentiearchitectuur voor IT en OT binnen de gemeente Utrecht. De architectuur biedt een samenhangend kader om OT en IT op een verantwoorde manier met elkaar te verbinden. Daarbij staat veilig en betrouwbaar functioneren van de primaire procesbesturing altijd voorop, terwijl gecontroleerde ontsluiting van data mogelijk wordt gemaakt voor monitoring, analyse en sturing.

Het Purdue model vormt de basis voor deze architectuur en informatieverwerking (IT), toepassing van dit model is noodzakelijk omdat het een duidelijke scheiding aanbrengt tussen procesbesturing (OT) en informatieverwerking (IT), en tegelijkertijd vastlegt hoe deze domeinen veilig met elkaar kunnen samenwerken. Hiermee wordt voorkomen dat digitalisering en datagebruik ten koste gaan van de veiligheid en beschikbaarheid van kritieke infrastructuur. Het Purdue model ondersteunt bovendien de naleving van regelgeving zoals NIS2 en normen als IEC-62443.

De Operationele Technologie Thema Architectuur draagt bij aan:

- **Veiligheid:** door het beschermen van kritieke OT-systemen en het beheersen van cyberrisico's
- **Bereikbaarheid:** door het verhogen van beschikbaarheid en voorspelbaarheid van infrastructurele assets.
- **Digitalisering:** door OT-data gecontroleerd beschikbaar te maken voor analyse en data gedreven besluitvorming.

Dit document vormt daarbij een richtinggevend kader voor beleid, projecten en investeringen en ondersteunt de realisatie van de strategische doelen van de gemeente Utrecht,

# 1. Inleiding

Operationele Technology (OT) zijn industriële controlesystemen die belangrijke processen aansturen, zoals het bedienen van sluizen en bruggen, verkeersregelininstallaties, tunnels en toegangsbeveiliging. Dit zijn processen die continu beschikbaarheid moeten zijn 24 uur per dag en 7 dagen in de week. De OT moet voorkomen dat kritische processen hinder ondervinden of stilvallen. Het aantal OT-apparaten groeit als gevolg van de digitalisering van de procesautomatisering. En steeds vaker worden deze OT-apparaten verbonden met het internet, waardoor er efficiënter gewerkt kan worden en betere kwaliteit van dienstverlening geboden wordt. IT en OT moeten naadloos integreren, data uitwisselen voor de aansturing, monitoring van de processen en voor correctie en preventief onderhoud. Er zijn ook risico's met inzet van OT en IT in de kritische processen. Bijvoorbeeld kunnen ze een interessant doelwit zijn voor hackers, waardoor er voor de integratie tussen IT en OT zich naast beheer en efficiënte ook aandacht moet zijn voor de beveiliging ervan.

De wettelijke taken, de maatschappelijke verantwoordelijkheid van gemeenten en nieuwe wet- en regelgeving, zoals de 'Network and Information Security' (NIS)<sup>2</sup> geïmplementeerd in Wbni (op 16 januari 2023 in werking getreden) en herziening van de Wet beveiliging netwerk- en informatiesystemen (Wbni), vragen van gemeenten om wendbaar én zorgvuldig te opereren. In deze turbulente context is het essentieel dat we als gemeente Utrecht niet willekeurig, of versnipperd, OT-inrichten, verbeteren en beheren, maar dat we werken vanuit een gedeeld kader.

De gemeente realiseert met OT in de fysieke assets in de stad publieke waarde, bijvoorbeeld:

- waterbeheer in de stad – aansturing door OT van pompen en sluizen met gemalen en rioleringsstelsel
- verkeersmanagement op gemeentelijke wegen met centraal bediende OT in de verkeersregelininstallaties
- centrale bediening middels OT van openbare verlichting voor de verkeersveiligheid
- monitoring en bediening middels OT in de Stadsbaantunnel voor de verkeersveiligheid
- ...

## Definitie Operationele Technology<sup>1</sup>

Operationele Technology (OT) is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld zoals het aansturen en monitoren van (industriële) apparatuur. Het kan dan gaan om het uitlezen van sensoren of het inschakelen van een pomp of schakelaar op basis van een bepaalde conditie.

---

<sup>1</sup> Bron: Nationaal Cyber Security Centrum [NCSC - Operational Technology](#)

## 1.1 Doel van OT Thema architectuur

De OT Thema architectuur is een kader voor de verantwoorde inzet van operationele technology binnen de gemeente Utrecht dat dient als basis voor project start architecturen en solution architecturen.

We bieden daarmee een gemeenschappelijke taal en een gedeelde visie, zodat OT binnen Utrecht aansluit op:

- wetgeving
- gemeentelijke kaders en normen en waarden
- onze maatschappelijke doelen
- strategische ambities van de gemeente

Het doel van de OT Thema architectuur is dat de kaders en richtlijnen toegepast worden in project start architecturen en in solutionarchitecturen en daarmee:

- de functionele werking van OT en IT verduidelijkt wordt ten behoeve van **uitlegbaarheid & transparantie, traceerbaarheid en testbaarheid** (het kunnen uitvoeren van risico assessments voor toetsing op beleid en wetgeving)
- **versnellen** van de realisatie in OT- & IT implementatie projecten doordat de architectuur bouwstenen, patronen, implementatie richtlijnen (non functionals) hergebruikt kunnen worden
- **consistente benadering** van de **markt** kunnen bereiken doordat er voor gezorgd is dat de architectuurpatronen en bouwblokken goed aansluiten op de OT-producten die leveranciers kunnen bieden waardoor OT- & IT projecten beter slagen
- een goede invulling gegeven kan worden aan het **gemeentelijk OT-beleid** vanuit de benodigde organisatie-, proces-, informatie- en technologische verandering

## 1.2 Doelgroep document

De Algoritmen & AI Thema architectuur heeft de volgende doelgroepen:

- **Businessmanager:** benodigde organisatorische verandering kunnen realiseren voor professioneel OT-beheer (nieuwe capability en bedrijfsfuncties, taken van functionarissen, werkprocessen en applicaties die veranderen in de organisatie)
- **Projectarchitecten:** om project start architectuur te kunnen maken voor OT-projecten, incl. non-functionals/ aansluitvoorwaarden en de toetsing van de solutionarchitectuur
- **Solutionarchitecten** (vaak de leverancier): solutionarchitectuur kunnen maken
- **Architectuur Community:** kennis en inzicht in algoritmen & AI architectuur
- **Security & privacy officer:** kennis, inzicht voor toetsing gegevensbeschermingsbeleid
- **Informatie Proces Managers, strategisch adviseurs:** over benodigde organisatorische verandering kunnen adviseren aan lijnorganisatie (nieuwe bedrijfsfuncties, taken van functionarissen, werkprocessen die veranderen in de organisatie)
- **DISO's en recordmanagers** achtergrondinformatie voor uitvoeren van risico-assessments voor mitigerende maatregelen in project start architectuur voor OT- & IT

## 1.3 Scope OT Thema architectuur

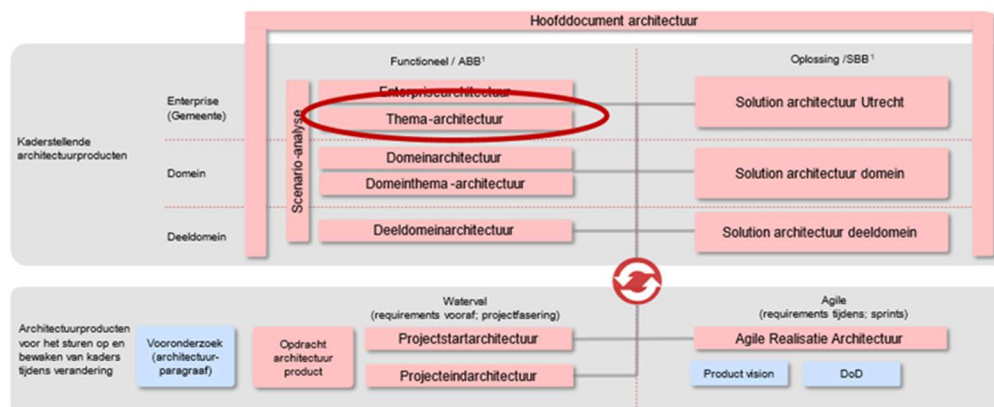
De scope van de algoritmen en OT Thema architectuur omvat:

- nieuwe OT architectuur principes
- Nieuwe capability en impact op de bestaande bedrijfsfuncties, taken & functies en werkprocessen
- OT-architectuurbouwstenen (Architecture Building Blocks) en architectuurpatronen
- AI-aansluitvoorwaarden/ AI non-functionals (beschreven in een separaat document)

Deze thema-architectuur zet daarmee de lijnen uit voor de nieuwe capability (bekwaamheid van de gemeente op strategisch niveau in het beheer van OT) en geeft inzicht in de verandering van de gemeentelijke bedrijfsfuncties, taken van functionarissen, werkprocessen en applicaties en daarmee handvaten waarmee we de transitie in de gemeente in werking kunnen stellen.

Onderstaand de scope van dit document afgebeeld:

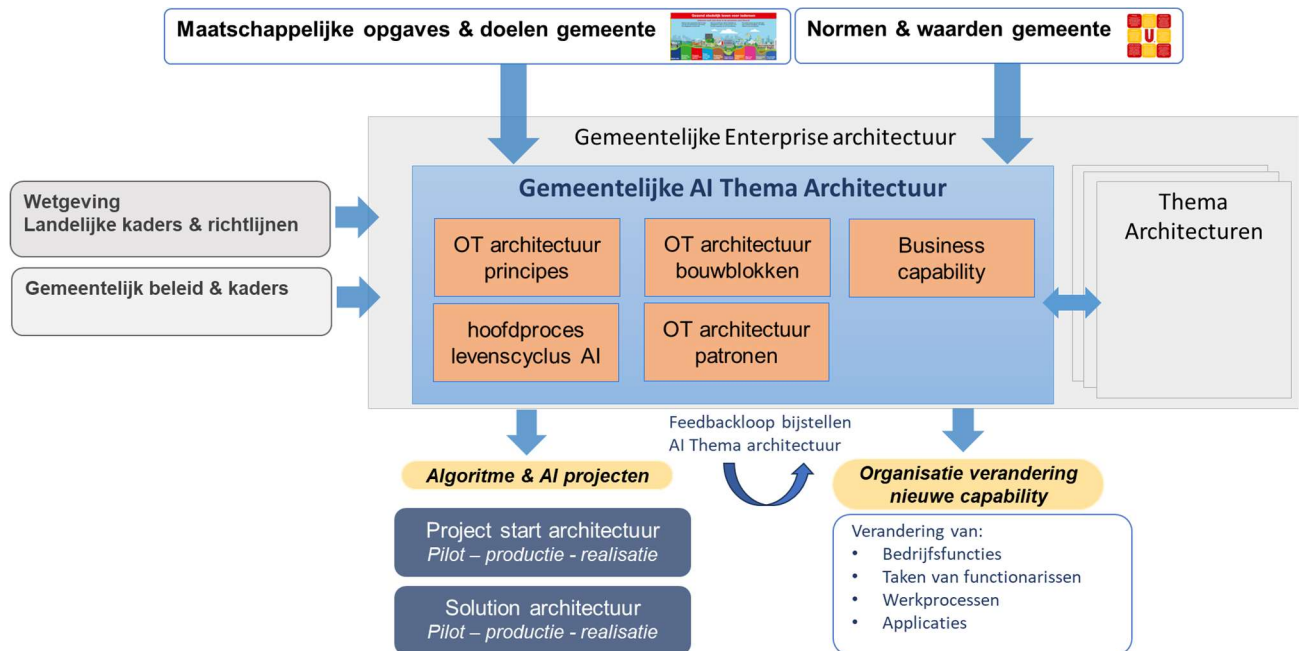
### Overzicht architectuurproducten



In presentatiemodus kun je elk architectuurproduct aanklikken en je komt dan direct op de slide met de specificatie van dat product. Met de knop 'Terug naar overzicht' kom je weer terug op deze overzichtsslide.

<sup>1</sup>ABB staat voor Architecture Building Block, SBB staat voor Solution Building Block

De scope van deze thema-architectuur in relatie tot de omgeving staat in het blauwe kader:



Figuur....

## 1.4 Leeswijzer

Dit document beschrijft de **Operationele Technology (OT) Thema Architectuur** voor het **OT-landschap** dat door gemeente Utrecht continue wordt beheerd, verbeterd en vernieuwd ten behoeve van de fysieke assets in de stad.

- In hoofdstuk 1 is de **Inleiding** van de OT Thema architectuur met een beschrijving van doel van de architectuur, doelgroep, scope en samenhang met andere thema architecturen.
- Hoofdstuk 2 beschrijft de OT Thema **architectuurprincipes**, de implicaties van de principes zijn opgenomen in een separaat document met de **aansluitvoorwaarden** voor OT-aanbieder (non-functionals)
- In hoofdstuk 3 is de nieuwe **capability** “verantwoorde inzet van OT” toegelicht en de benodigde verandering van de bestaande bedrijfsfuncties en nieuwe bedrijfsfuncties.
- Hoofdstuk 4 beschrijft de verandering van de bestaande bedrijfsfuncties en nieuwe bedrijfsfuncties in meer detail: de wijziging van **de rollen, taken en verantwoordelijkheden, bedrijfsprocessen, informatie- en applicatielandschap** voor verantwoorde inzet van API's
- Hoofdstuk 5 beschrijft het **Purdue-model**.
- Hoofdstuk 7 beschrijft de **architectuurbouwstenen** voor ontwikkelingen en beheren van AI toepassingen op een verantwoorde manier
- Hoofdstuk 9 beschrijft de **architectuurpatronen** voor de ontwikkeling van OT met inzet van de architectuurbouwstenen.

## 1.5 Relatie met ander gemeentelijke documenten

- Enterprise Architectuur Utrecht (EAU) [<link toevoegen>](#)
- OT Beleid Stadsbedrijven (...*nog niet aanwezig*)
- integraal informatiebeleid [<link toevoegen>](#)
- gemeentelijk gegevensbescherming-beleid [<link toevoegen>](#)
- gemeentelijke Cloud-strategie [<link toevoegen>](#)
- gemeentelijke Common Ground-strategie [<link toevoegen>](#)
- relevante nationale en Europese wetgeving
- BIO
- Wbni en NIS2
- Landelijke normenkaders
  - handreiking PA- systemen van VNG
  - CSIR normenkader voor OT-security voor het beveiligen van de OT-objecten
  - IEC62443

## 2. Context OT in gemeente Utrecht

### 2.1 Definitie Operationele technologie

Operationele technologie (OT) binnen de gemeente Utrecht omvat alle systemen, componenten en voorzieningen die direct worden ingezet voor het monitoren, besturen, beveiligen en automatiseren van fysieke processen en objecten in de openbare ruimte en gemeentelijke infrastructuur.

OT-systemen verwerken real time-signalen van sensoren en sturen actuatoren aan om de fysieke processen veilig, betrouwbaar en beschikbaar te laten functioneren. Hieronder vallen onder meer besturingssystemen, veldapparatuur, industriële netwerken en ondersteunende software die noodzakelijk zijn voor de operationele taken.

OT onderscheidt zich van informatietechnologie doordat OT primair is gericht op fysieke procesbesturing en veiligheid, met hoge eisen aan de beschikbaarheid, voorspelbaarheid en de fail-safe werking. OT-systemen functioneren autonoom en blijven veilig opereren, ook bij uitval van de bovenliggende IT-systemen.

Binnen de gemeente Utrecht wordt de OT ingericht conform een gelaagde architectuur (Purdue Reference Architecture) met duidelijke scheiding tussen OT-, OT/IT- en IT-domeinen. Integratie met IT vindt uitsluitend plaats via expliciet ingerichte en beveiligde koppelvlakken, conform de geldende normen en richtlijnen, waaronder IEC 62443 en NIS2.

### 2.2 Ontwikkelingen digitalisering IoT & IT & OT integratie

Digitalisering en IoT zorgen voor een sterke toename van verbonden systemen in de fysieke leefomgeving. Sensoren en slimme apparaten leveren real-time data die wordt gebruikt voor monitoring, beheer en besluitvorming.

Hierdoor neemt de integratie tussen IT- en OT-systemen toe. Deze integratie biedt kansen voor efficiënter, maar vraagt om duidelijke architectuurkeuzes en goede beveiliging om veiligheid en betrouwbaarheid te waarborgen.

### 2.3 Wettelijke en normatieve kaders

#### **Wettelijke kaders**

Binnen de context van OT-architectuur zijn de volgende wettelijke en normatieve kaders van toepassing:

- **NIS2-richtlijn (EU) / Nederlandse implementatie**
  - Verplicht maatregelen voor cyberbeveiliging, risicomanagement en incidentmelding
  - Van toepassing op essentiële en belangrijke entiteiten, waaronder infrastructuur en vitale processen.
  - Grote impact op OT-architectuur, governance en beheer.
- **Wet beveiliging netwerk- en informatiesystemen (Wbri / opvolgers)**
  - Nationale uitwerking van Europese cybersecuritywetgeving.
  - Eisen aan beveiliging, monitoring en incidentenafhandeling.

- **Privacy & gegevensbescherming**
  - Algemene verordening gegevensbescherming (AVG)
    - Relevant als OT-systemen direct of indirect persoonsgegevens verwerken.
    - Vereist privacy by design en by default, ook binnen de OT-architectuur.
- **Veiligheid, aansprakelijkheid en arbeidsomstandigheden**
  - Arbowet
    - Eisen aan veilige werking van installaties en systemen.
    - Relevant voor OT-besturing, noodvoorzieningen en calamiteitenfunctionaliteit.
- **Burgerlijk wetboek**
  - **aansprakelijkheid**
    - Onveilige of falende OT-systemen kunnen leiden tot aansprakelijkheid bij schade of letsel.
    - Architectuur moet aantoonbaar bijdragen aan veilige en betrouwbare werking.
- **Openbaarheid en informatiebeheer**
  - **WOO**
    - Data en informatie uit OT-systemen kunnen onder de openbaarheidsverzoeken vallen.
    - Architectuur moet rekening houden met archivering, ontsluiting en transparantie.
  - **Archiefwet**
    - Van toepassing op het beheer en bewaring van OT-gerelateerde data en documentatie.
- **Aanbesteden en leveranciersrelaties**
  - **Aanbestedingswet 2012**
    - Van toepassing bij de aankoop van OT-systemen, software en diensten.
    - Vereist transparantie, objectieve eisen en toetsbare architectuurkaders.

***Normatieve kaders en standaarden (niet wettelijk maar richtinggevend)***

- **IEC 62443**
  - Cybersecurity voor OT (Zones & conduits)
- **Purdue Reference architecture**
  - Gelaagde OT/IT architectuur
- **NORA / GEMMA**

## **2.4 Positionering met betrekking tot de Enterprise Architectuur Utrecht**

OT vormt binnen de Enterprise architectuur van de gemeente Utrecht een volwaardig onderscheidend domein naast IT. OT is primair gericht op de veilige en betrouwbare besturing en monitoring van fysieke processen in de openbare ruimte en gemeentelijke infrastructuur, en kent eigen eisen aan de beschikbaarheid, veiligheid en continuïteit.

Binnen de Enterprise architectuur wordt OT gepositioneerd volgens een gelaagde architectuur, met een duidelijke scheiding tussen business-, applicatie- en technologiegebieden en een

expliciete afbakening tussen OT- en IT-domeinen. Integratie tussen OT en IT vindt plaats via gestandaardiseerde, beveiligde koppelvlakken, waarbij OT autonoom kan functioneren bij verstoringen van IT.

Door OT expliciet te positioneren binnen de Enterprise architectuur wordt samenhang geborgd tussen beleid, beheer, beveiliging en doorontwikkeling, terwijl gelijktijdig wordt voldaan aan wet-en regelgeving en landelijke architectuorkaders.

## 2.5 Samenhang andere thema architecturen

De OT-thema architectuur is een van de thema architecturen binnen de gemeente, de samenhang met de andere thema architecturen is in deze paragraaf beschreven.

In het ontwerp en de ontwikkeling van OT- & IT-systemen wordt gebruik gemaakt van de architectuurbouwblokken (ABB's Architecture Building Blocks) en architectuurpatronen van bestaande thema architecturen. In deze thema architectuur zijn ook nieuwe architectuurbouwblokken beschreven die relevant zijn voor de andere thema architecturen. Het document OT-aansluitvoorwaarden/non-functionals is een aanvulling op het bestaand gemeentelijk non-functionals document voor IT-projecten.

- **Data Thema Architectuur**

De test en productiedata zijn een belangrijk grondstof voor OT-systemen. Het is van belang dat de kwaliteit van de data goed inzichtelijk en beschreven is volgens het datakwaliteitsraamwerk [<link....>](#). In de context van het gebruik van de OT- en IT-systeem bepaal je voorafgaand in de projectfase welke datakwaliteit vereist is voor stuurinformatie voor de eindgebruiker.

- **Integratie Thema Architectuur**

De thema architectuur Operationele Technologie vormt een integraal onderdeel van de gemeentelijke architectuur van de gemeente Utrecht en is richtinggevend voor alle OT-gerelateerde ontwikkelingen. De architectuur sluit aan op de vastgestelde gemeentelijke architectuur, externe normen en relevante landelijke architecturen.

- **Common Ground Thema Architectuur**

Het Purdue Enterprise Reference Architecture (PERA) model, bidet een gelaagde structuur voor OT-omgevingen, waarin fysieke processen, SCADA, OT-diensten en koppelingen strikt van elkaar gescheiden zijn.

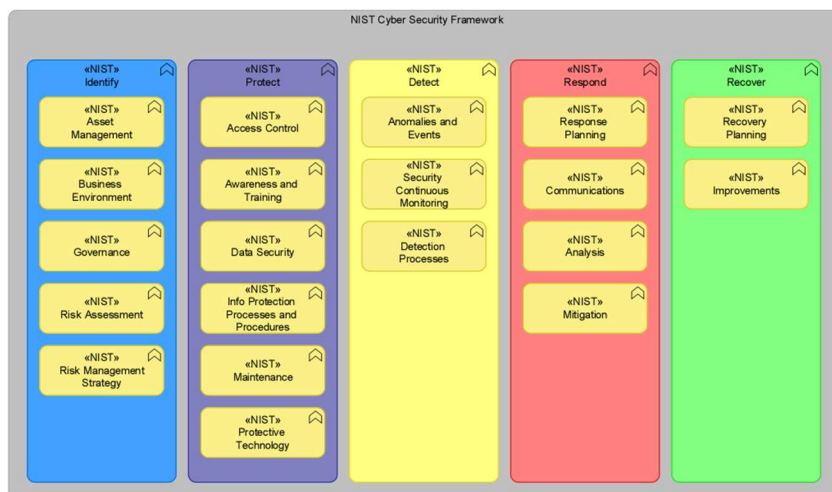
Het Common Ground principe richt zich op het ontkoppelen van gegevens, applicaties en processen zodat informatie duurzaam, herbruikbaar en domein overstijgend beschikbaar is.

Hoewel beide modellen uit verschillende werelden komen, vullen ze elkaar goed aan. Het Purdue model vormt de technische en operationele segmentatie, terwijl Common Ground de informatie- en data-logica organiseert.

Een cruciaal onderdeel hiervan is duidelijk eigenaarschap van brondata., zodat de gemeente controle houdt over haar eigen informatie en niet afhankelijk wordt van leveranciers of systemen.

- **Securitygegevensbescherming Thema Architectuur**

OT-systemen beveiligen is van cruciaal belang om te voorkomen dat de data én technologie gemanipuleerd wordt, gestolen wordt, misbruik van wordt gemaakt, etc. Dit betekent zowel technologische als organisatorische beveiligingsmaatregelen te treffen met alle direct betrokkenen partijen. In de ontwikkeling van OT-systemen wordt gebruik gemaakt van de architectuurbouwblokken van de Securitygegevensbescherming thema architectuur, zie hoofdstuk 6. Onderstaand het NIS Cyber Security Framework.



Figuur....

## **3. Architectuurprincipes OT**

Om de OT-architectuur binnen de gemeentelijke infrastructuur beheersbaar, veilig en toekomst vast in te richten, wordt onderscheid gemaakt tussen logische, fysieke en operationele architectuur. Dit onderscheid helpt om complexiteit te structureren en vormt de basis voor ontwerp, beheer en beveiliging van OT-systemen. Dit onderscheid wordt in de paragrafen 4.3 t/m 4.5 verder toegelicht.

### **3.1 Purdue referentie architectuur**

Verbinden van operationele technologie (OT) en informatietechnologie (IT) is noodzakelijk om inzicht, voorspelbaarheid en sturing te realiseren binnen kritieke infrastructuur. Tegelijkertijd brengt de verbinding risico's met zich mee voor de beschikbaarheid, veiligheid en betrouwbaarheid van OT-systemen.

Het Purdue model is belangrijk omdat het een gestructureerd en beproeft referentiekader biedt om deze verbinding beheerst en veilig tot stand te brengen.

### **3.2 Implicaties van architectuurprincipes**

De in deze referentiearchitectuur vastgelegde principes hebben directe gevolgen voor de wijze waarop projecten worden ingericht, hoe beheer wordt georganiseerd en welke eisen aan leveranciers worden gesteld. Om deze samenhang toetsbaar en expliciet en te maken, zijn de implicaties van de principes gelaagdheid, security by design, herbruikbaarheid en toetsbaarheid hieronder uitgewerkt voor projecten, beheer en leveranciers. Dit overzicht biedt daarmee een kader voor consistente toepassing van de architectuur in de gehele lifecycle van OT-systemen en ondersteunt sturing, toetsing en verantwoording bij realisatie, beheer en inkoop.

## Projecten

| Architectuurprincipe | Implicatie                                                                                                                     |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Gelaagdheid          | Ontwerpen en realiseren conform vastgestelde architectuurlagen (OT, IT, integratie), zonder ongecontroleerde kruiskoppelingen. |
| Security by design   | Cybersecurity eisen worden vanaf de ontwerpfase meegenomen en aantoonbaar geïmplementeerd.                                     |
| Herbruikbaarheid     | Gebruik bestaande bouwstenen, standaarden en generieke voorzieningen is het uitgangspunt.                                      |
| Toetsbaarheid        | Ontwerpen en opleveringen zijn toetsbaar aan architectuur-, Security- en beheercriteria.                                       |

## Beheer

| Architectuurprincipe | Implicatie                                                                           |
|----------------------|--------------------------------------------------------------------------------------|
| Gelaagdheid          | Beheerprocessen en verantwoordelijkheden zijn per laag duidelijk belegd.             |
| Security by design   | Beveiligingsmaatregelen zijn structureel onderdeel van beheer en lifecyclemanagement |
| Herbruikbaarheid     | Beheer maakt gebruik van gestandaardiseerde oplossingen en uniforme werkwijzen.      |
| Toetsbaarheid        | Beheeractiviteiten zijn meetbaar via KPI's en audits.                                |

## Leveranciers

| Architectuurprincipe | Implicatie                                                                             |
|----------------------|----------------------------------------------------------------------------------------|
| Gelaagdheid          | Oplossingen sluiten aan bij de gelaagde architectuur en respecteren domeinscheidingen. |
| Security by design   | Leveranciers zijn verifieerbaar en toetsbaar aan vastgestelde eisen en normen.         |
| Herbruikbaarheid     | Leveranciers leveren modulaire, open en herbruikbare oplossingen.                      |
| Toetsbaarheid        | Leveringen zijn verifieerbaar en toetsbaar aan vastgestelde eisen en normen.           |

### 3.3 Koppeling principes

De gemeentelijke architectuurprincipes uit EAU, NORA, en GEMMA vormen het normatieve kader voor de inrichting, integratie en sturing van informatiesystemen binnen de gemeente Utrecht. Om te waarborgen dat de OT-architectuur en telemetriesystemen ook voldoen aan de wettelijke- en cybersecurity-eisen, worden deze principes expliciet gekoppeld aan de relevante normatieve kaders zoals NIS2, BIO en IEC 62443.

Het volgende overzicht maakt inzichtelijk op welke wijze de principes worden vertaald na concrete verplichtingen en toetsingscriteria en ondersteund daarmee consistentie, compliance en interoperabiliteit in projecten, beheer en leveranciersrelaties.

#### Beheer van OT Thema Architectuur

De OT Thema architectuur is een dynamische architectuur, dat betekent dat deze Thema architectuur wordt ververst op basis van nieuwe inzichten, ervaringen uit de praktijk (intern en extern gemeente), nieuwe technologieën en veranderingen in de omgeving (bijvoorbeeld

nieuwe landelijke kaders). Het actueel houden van de OT-architectuur gebeurt door de OT Thema architect. Het beheerproces:

Nieuwe of wijzigingen in architectuurbouwblokken (ABB), architectuurpatronen en de aansluitvoorwaarden/non-functionals worden aangeboden aan architectuurboard als een addendum voor een beoordeling.

Wijzigingen in de architectuurprincipes wordt een nieuwe versie van de Algoritmen & AI Thema architectuur aangeboden aan architectuurboard voor een beoordeling.

De OT Thema architectuur wordt door AI Thema architect regulier gecommuniceerd met de volgende doelgroepen, zoals bijvoorbeeld:

Asset beheerders en lijnmanagers

Architectuur community

Decentrale Informatie Security Officers, recordmanagers, dashboard ontwikkelaars

Informatiemanagers

Auditing

Functioneel applicatie beheerders in de Organisatie Onderdelen

-

-

## 4. OT-Referentie Architectuur

De OT-referentie architectuur beschrijft de samenhang, principes en bouwblokken van de operationele technologie binnen de gemeentelijke infrastructuur. Het doel is om een uniform, veilig en beheersbaar fundament te bieden voor alle OT-domeinen, zoals beweegbare bruggen,, tunnels, gemalen, verkeersinstallaties en andere vitale objecten. De architectuur vormt het kader voor ontwerp, realisatie, beheer en lifecycle-management van OT-systemen, en zorgt voor consistente keuzes binnen projecten en leverancier ketens.

<Toevoegen kernplaat referentiearchitectuur (Utrecht specifiek)>

### 4.1 Architectuurprincipes

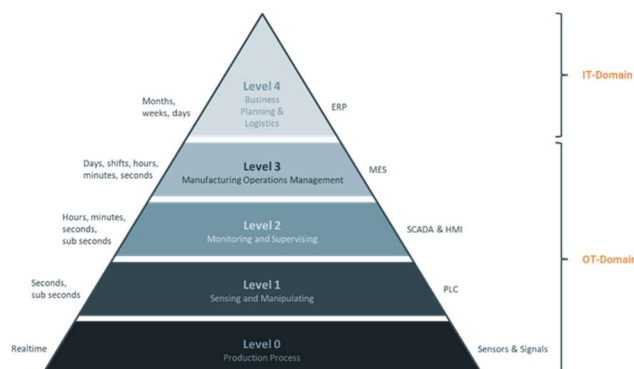
De OT-referentiearchitectuur past de in hoofdstuk 3 beschreven architectuurprincipes toe binnen de context van operationele technologie. Deze principes vormen de basis voor ontwerpkeuzes, beveiligingsmaatregelen en standaardisatie binnen het OT-domein.

### 4.2 Purdue model

De gemeente Utrecht past het Purdue Enterprise Reference Architecture model (PERA, de ISA-95 standaard voor verticale integratie OT- en IT-domein), toe als fundament voor inrichting. Beveiliging en beheersbaarheid toe van alle OT-omgevingen binnen de fysieke leefomgeving.

Het Purdue-model vormt daarmee een essentieel onderdeel van de Utrechtse OT-referentiearchitectuur en ondersteund zowel technische als organisatorische doelstellingen waaronder veiligheid, continuïteit, datakwaliteit en eigenaarschap van brondata.

In het model worden 5 automatiseringsniveaus onderscheiden:



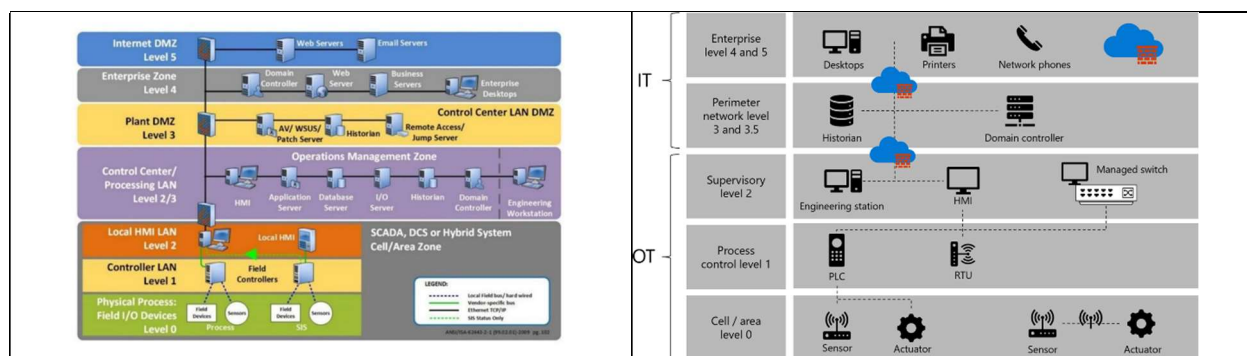
**Niveau 4:** IT-domein o.a. kantoorprocessen, ERP systemen voor planning, inkoop, financiën, etc. IT heeft andere eisen dan OT-domein t.a.v. beschikbaarheid, betrouwbaarheid en veiligheid.

**Niveau 3:** MES Manufacturing Execution System(s) besturen gehele industriële automatisering, zijn overkoepelend voor niveaus 1 t/m 3, met focus op continue operationele productie.

**Niveau 2:** HMI of 'Human Machine Interface'. In verleden waren dat knoppen, nu vaak touchscreens of een noodstop.<sup>2</sup>

**Niveau 1:** Aansturende systemen, PLC's besturen machines en productie-installaties. Hoge beschikbaarheid, betrouwbaarheid en veiligheid van aansturende systemen is belangrijk.

**Niveau 0:** Dit is de fysieke proceslaag waarin de daadwerkelijke objecten die uitvoeren en meten. Dit zijn de componenten die direct invloed hebben op de fysieke wereld (brug beweegt, gemaal opent, sluis opent/sluit)



## 4.1 Logische OT-architectuur

De logische OT-architectuur beschrijft welke functies en componenten nodig zijn voor de besturing, monitoring en aansturing van kritieke infrastructuur, los van concrete leveranciers of technische implicaties.

Binnen de logische infrastructuur wordt onder andere onderscheiden:

- Procesbesturing (zoals besturen van bruggen, sluizen en gemalen)
- Monitoring en visualisatie (HMI, SCADA)
- Alarmering en meldingen
- Dataverzameling en historisering
- Koppeling met IT-systemen voor analyse en rapportage

De logische OT-architectuur sluit aan op het Purdue-model, waarbij functies worden gepositioneerd over de verschillende niveaus (0 t/m 4). Deze indeling vormt de basis voor de scheiding van verantwoordelijkheden, beschikbaarheidseisen en beveiligingsmaatregelen

<sup>2</sup> HMI zijn vaak SCADA-systemen ('supervisory and data acquisition') waarmee men totale proces centraal kan overzien, besturen en ingrijpen. SCADA-software communiceren met aansturende systemen, PLC's (en PLC's communiceren cq. besturen machines)

## 4.2 Fysieke OT-infrastructuur

De fysieke OT-infrastructuur beschrijft hoe de logische componenten technisch zijn gerealiseerd en waar zij zich bevinden binnen de infrastructuur. Hieronder vallen onder andere:

- PLC's, RTU's, sensoren en actuatoren
- SCADA-servers en bedieningsstations
- Netwerken, zones en verbindingen (volgens IEC 62443)
- Fysieke locaties zoals objecten, bedieningscentrales en datacenters

In de fysieke OT-architectuur wordt expliciet aandacht besteed aan:

- Segmentatie van netwerken (zones en conduits)
- Scheiding tussen OT- en IT-domeinen
- Beschikbaarheid en redundantie van kritieke componenten

De fysieke infrastructuur volgt de uitgangspunten van het Purdue-model en ondersteunt de vereiste beveiligingsniveaus (security levels)

## 4.3 Operationele OT-infrastructuur

De operationele OT-infrastructuur beschrijft hoe OT-systemen worden gebruikt, beheerd en bewaakt in de dagelijkse praktijk. Dit omvat onder andere:

- Beheer en onderhoud van OT-componenten
- Monitoring, logging en alarmering
- Incident- en calamiteiten afhandeling
- Wijzigingsbeheer (changes) in OT-omgevingen
- Samenwerking tussen OT-beheer, IT-beheer en assetmanagement

De operationele architectuur is cruciaal voor het borgen van:

- Continuïteit en beschikbaarheid
- Veilig en gecontroleerd gebruik van OT-systemen
- Naleving van wet- en regelgeving zoals NIS2

### Samenhang

De logische, fysieke en operationele OT-architectuur vormen gezamenlijk een geheel. Wijzigingen in een van de lagen hebben impact op de andere lagen en moeten daarom integraal worden beschouwd. Deze samenhang vormt de basis voor OT-security, risicoanalyses en compliance met normenkaders zoals IEC 62443 en NIS2.

## 4.4 Zones en Conduits (IEC-62443)

Zones en conduits zorgen voor segmentatie van het netwerk waardoor de beveiliging per zone kan worden afgestemd op de risico's en functies. Hiermee wordt voorkomen dat incidenten zich ongecontroleerd kunnen verspreiden en er meer controle is over de datastromen waarmee het risico op ongewenste toegang of datalekken wordt gereduceerd. Binnen het telemetrie domein wordt de indeling van zones en conduits toegepast om de OT-omgeving logisch, beheersbaar

en veilig te segmenteren. Deze segmentatie volgt het Purdue model en sluit aan op de beveiligingsprincipes uit IEC-62443, waarin zones en conduits een centrale rol spelen voor risicobeheersing en toegangscontrole. Een zone is een logisch of fysiek afgebakend De scheiding van zones (segmentatie) volgens Purdue en IEC-62443 is als volgt:

## Zones

- **Zone 0-1: Veldzone (sensoren en actuatoren)**
  - Bevat sensoren, actuatoren, meetinstrumenten en veldapparatuur.
  - Direct gekoppeld aan fysieke processen (brugbewegingen, waterstanden, debieten)
  - Minimale netwerkfunctionaliteit, vaak via industriële protocollen.
  - IEC-62443-principe: laagste exposure maar hoogste integriteitsvereisten
- **Zone 1-2: Besturingszone (PLC/RTU-laag)**
  - PLC's . RTU's, embedded controllers en lokale I/O
  - Real time besturing en telemetrie-data verzameling
  - Strikte scheiding van andere zones om manipulatie te voorkomen
  - IEC-62443 principe: strikte toegangscontrole, hardening en beperkte communicatie
- **Zone 2-3: Scada- telemetrie netwerkzone**
  - SCADA-servers, historians, telemetrie gateways
  - Centrale monitoring, alarmering en trendanalyse
  - Data wordt voorbereid voor ontsluiting naar IT
  - IEC-62443 principe: hogere beveiligingsniveaus (SL@-SL#), logging en monitoring
- **Zone 3 : OT-servicelaag**
  - Remote access-voorzieningen
  - Patch- en update mechanismen
  - OT-monitoring en beheer
  - IEC-62443 principe: streng gecontroleerde toegang, multi factor authenticatie
- **Zone 3.5: DMZ-zone**
  - Bufferzone tussen OT en IT
  - Telemetrie data wordt gevalideerd, gefilterd en beveiligd
  - Geen directe verbinding tussen SCADA en IT applicaties
  - IEC-62443 principe: gecontroleerde datastromen, protocol-whitelisting
- **Zone 4-5: IT-zone**
  - Gemeentelijke applicaties , dashboards, assetmanagement, dataplatformen
  - Telemetriedata read only
  - IEC-62443 principe: OT-data blijft eigendom van de gemeente

## Conduits

Een conduit is een beveiligde communicatieverbinding tussen twee zones. Binnentelemetrie zijn conduits onmisbaar om:

- Datastromen te kunnen reguleren
- Beveiligingsniveaus te kunnen handhaven

- Risico's te isoleren
- Toegang te controleren

Voorbeelden van conduits binnen de telemetrie zijn:

- **Level 0-1 naar level 1-2 – Veld -> PLC/RTU**
  - Industriële protocollen (Modbus, 4-20 mA, digitale I/O)
  - Geen directe IP-connectiviteit vanuit hogere lagen
  - Conduit is fysiek of via industriële bus
- **Level 1-2 naar level 2-3 - PLC/RTU -> SCADA**
  - Telemetrieprotocollen zoals DNP3, Modbus-TCP, OPC-UA
  - Firewall gecontroleerde verbindingen
  - Alleen noodzakelijke poorten en verbindingen
- **Level 2-3 naar level 3.5 – SCADA -> DMZ**
  - Dat extractie via beveiligde protocollen
  - Eenrichtingsverkeer (data-diode) waar mogelijk
  - Validatie en filtering via DMZ
- **Level 3.5 naar level 4-5 – DMZ -> IT-diensten**
  - API's, MQTT, REST of gestandaardiseerde protocollen
  - Geen directe verbinding met SCADA of PLC's
  - Conduit strikt gereguleerd en gelogd

IEC schrijft voor dat:

- OT-omgevingen worden opgedeeld in zones met vergelijkbare risico's
- Communicatie tussen zones uitsluitend via gecontroleerde conduits plaatsvindt
- Elke zone haar eigen securitylevel krijgt
- Conduits beveiligingsmaatregelen afdwingen (encryptie, filtering, authenticatie)

De toepassing van het Purdue model sluit hier naadloos op aan:

- Purdue bepaald waar zones liggen
- IEC-62443 bepaald hoe zones beveiligd worden.

## 5. Organisatie& Governance

### Capabilities

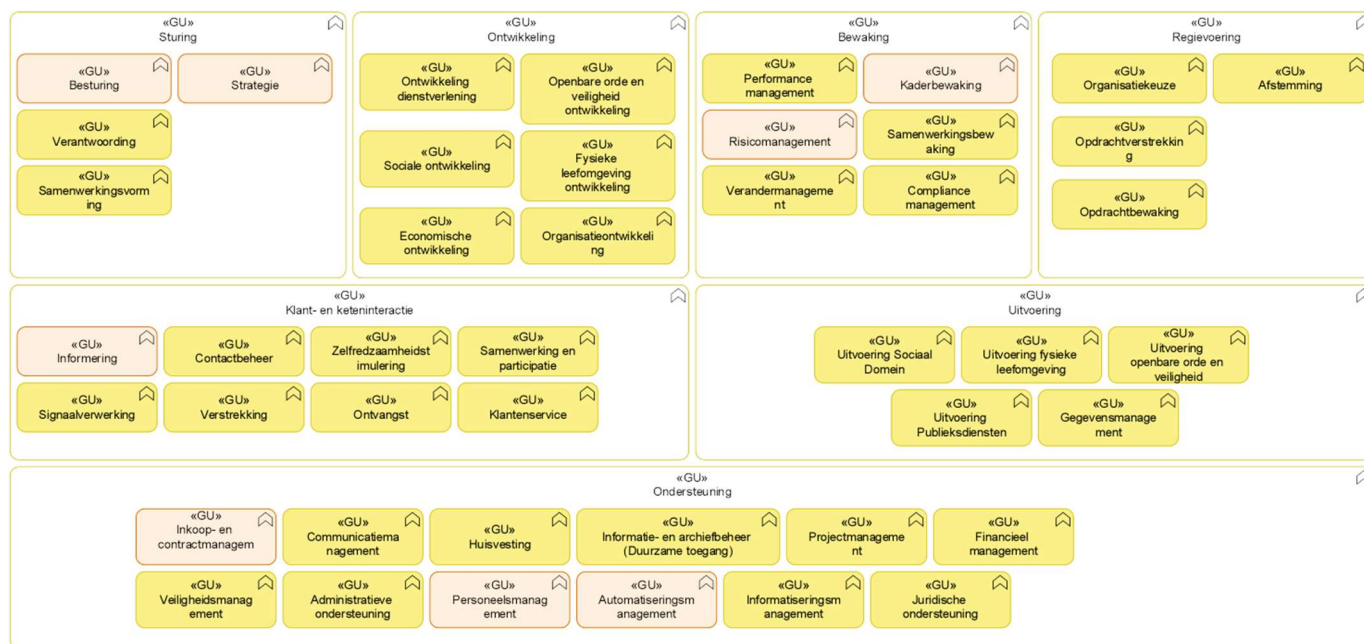
Een capability is het vermogen of capaciteit van een organisatie om een bepaald doel of resultaat te bereiken. Ze voldoen hierbij aan het volgende:

- Capabilities beschrijven wat je organisatie doet of kan doen, niet *hoe* het wordt gedaan of *wie* het doet. Ze verschillen van bedrijfsprocessen, functies, services, organisatie-eenheden of IT-systemen, hoewel deze onderdelen wel kunnen bijdragen aan een capability.
- Eenzelfde capability kan op verschillende manieren worden gerealiseerd, bijvoorbeeld handmatig, ondersteund door IT of volledig geautomatiseerd.
- Capabilities zijn eigendom van de business en worden benoemd en gedefinieerd in zakelijke termen. De beschrijving moet voor alle betrokkenen gemakkelijk te begrijpen zijn.
- Capabilities zijn uniek en stabiel. Elke capability wordt slechts één keer gedefinieerd voor de hele organisatie en verandert zelden, tenzij er bijvoorbeeld een nieuwe markt wordt betreden of een bedrijfsactiviteit wordt afgestoten.
- Capabilities kunnen bestaan uit sub-capabilities en kunnen ook andere capabilities gebruiken.
- De volwassenheid van een capability kan worden beoordeeld op verschillende dimensies, zoals mensen, processen, technologie, informatie en andere middelen. Zulke beoordelingen vormen de basis voor capability-based planning.

### 5.1 Nieuwe capability “Beheer OT”

Om de nieuwe capability “Beheer operationele technology” te realiseren zijn wijzigingen in de bestaande bedrijfsfuncties nodig en er zijn twee nieuwe bedrijfsfuncties in de gemeente nodig. In onderstaand figuur zijn in oranje gearceerd de bedrijfsfuncties waarin aanpassingen nodig zijn en in paars gearceerd twee nieuwe bedrijfsfuncties in het gemeentelijk bedrijfsfunctiemodel.

## 5.2 Gewijzigde bedrijfsfuncties



### Wijzigingen in bestaande bedrijfsfuncties:

De capability “Beheer operationele technology” omvat het vermogen om OT-systemen en telemetrievoorzieningen functioneel integraal te beheren, met aandacht voor beschikbaarheid, veiligheid, betrouwbaarheid en lifecycle. Deze capability vormt de verbindende schakel tussen fysieke objecten, operationele besturing en de gemeentelijke informatievoorziening.

De effectiviteit van de capability wordt gestuurd en gemonitord via KPI's zoals:

- Beschikbaarheid en storingsduur van systemen;
- Tijdige en gecontroleerde afhandeling van wijzigingen;
- Naleving van cybersecurity-eisen (o.a. IEC 52443);
- Kwaliteit en continuïtet van telemetriedata.

Door het beheer van OT als afzonderlijke capability te positioneren, wordt eigenaarschap geborgd en ontstaat gerichte sturing op prestaties en risicomitigatie, in samenhang met andere gemeentelijke capabilities en landelijke architectuurkaders.

Om de nieuwe capability “Beheer operationele technology” te realiseren zijn de wijzigingen in de bestaande bedrijfsfuncties in onderstaande tabel toegelicht.

| Gewijzigde bedrijfsfunctie | beschrijving wijziging van bedrijfsfunctie                   |
|----------------------------|--------------------------------------------------------------|
| informering                | Het geven van algemene of persoonlijke informatie of advies. |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | Burgers, bedrijven, ketenpartners en medewerkers worden door de gemeente geïnformeerd over de dienstverlening.<br><i>Wijziging:</i> In het geval sensoren worden ingezet in OT, moet de gemeente de inwoner ook hierover informeren                                                                                                                                                                                               |
| Inkoop- en contract management | Het verwerven van middelen middels inkoop en het bewaken van de afspraken hierover met de leverancier<br><i>Wijziging:</i> opstellen van aanvullende inkoopvoorwaarden en verplichtingen in SLA voor OT. Indien nodig een verwerkersovereenkomst                                                                                                                                                                                  |
| Besturing                      | Het inrichten en uitvoeren van de besluitvormingsprocessen en -structuren en het nemen van strategische besluiten<br><i>Wijziging:</i> assetmanager (proceseigenaar) besluit over de inzet van OT en het borgen van de mitigerende maatregelen voor de risico's.                                                                                                                                                                  |
| Strategie                      | Het bepalen welke veranderingen zouden moeten worden doorgevoerd en de doelstellingen die daaraan ten grondslag liggen.<br><i>Wijziging:</i> opstellen van een OT Uitvoeringskader gemeente                                                                                                                                                                                                                                       |
| Kaderbewaking                  | Het bewaken of processen binnen de zelf opgestelde beperkingen worden uitgevoerd.<br><i>Wijziging:</i> werken onder architectuur in OT-ontwikkelingen<br>Monitoring bedrijf continuïteit en beveiliging OT en tijdig maatregelen nemen                                                                                                                                                                                            |
| Risicomanagement               | Het bepalen en bewaken van de risico's waaraan de organisatie wordt blootgesteld.<br><i>Wijziging:</i> risico analyses uitvoeren OT-landschap & rapportage                                                                                                                                                                                                                                                                        |
| Personeelsmanagement           | Het strategisch plannen, werven en ontwikkelen van medewerkers om de bedrijfsdoelstellingen te behalen. Het omvat taken als werving en selectie, personeelsadministratie, ontwikkeling, leiding, en het vertalen van bedrijfsstrategieën naar personeelsbeleid om het potentieel van medewerkers optimaal te benutten<br><i>Wijziging:</i> strategisch personeelsmanagement voor regievoeren ontwikkeling- en beheer OT-landschap |

Bron: gemeentelijk bedrijfsfunctiemodel gebaseerd op GEMMA

## Wijzigingen in bestaande bedrijfsfuncties, bedrijfsprocessen, functies, informatie- en applicatielandschap

De wijzigingen in de bestaande bedrijfsfuncties worden gerealiseerd door wijzigingen in:

- Bestaande bedrijfsprocessen
- Bestaande functies van medewerkers, taken, rollen en verantwoordelijkheden
- Bestaand instrumentarium en informatie-objecten
- Bestaand applicatielandschap

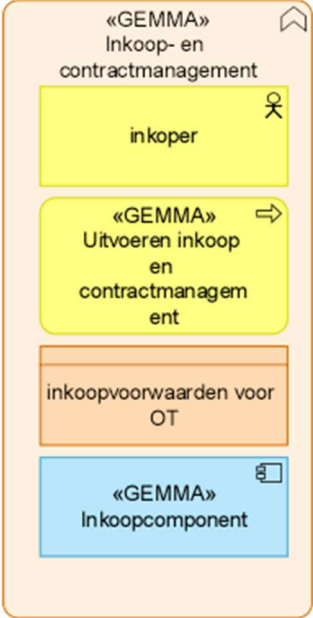
In onderstaande tabel de beschrijving van de wijzigingen in de bestaande bedrijfsfuncties. Een detailbeschrijving van de nieuwe taken, rollen en verantwoordelijkheden is in het Uitvoeringskader.

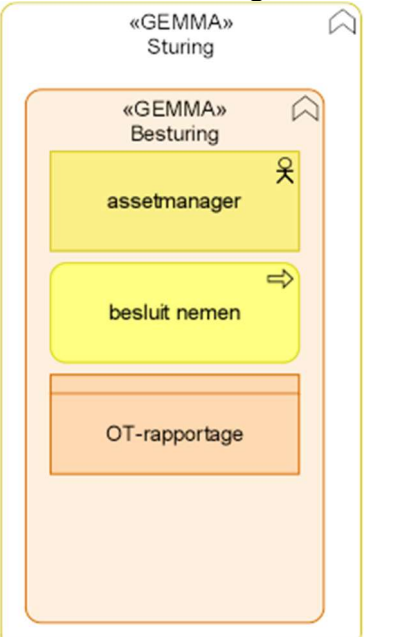
### 5.3 Rollen, taken en verantwoordelijkheden

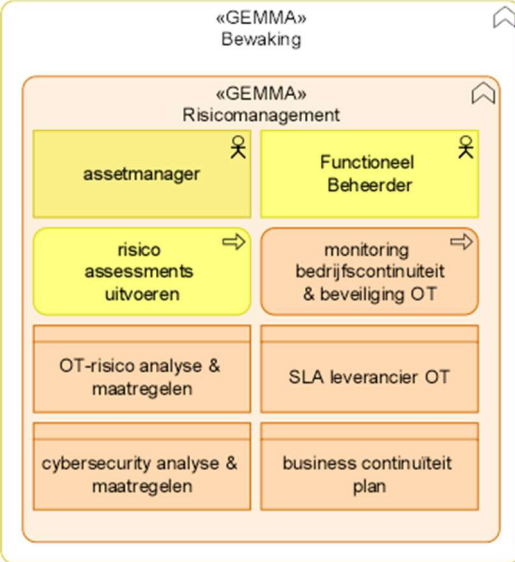
Deze paragraaf beschrijft de rollen, taken en verantwoordelijkheden die van toepassing zijn op de inrichting, het beheer en de doorontwikkeling van operationele technologie. Binnen de organisatie. Een heldere rolverdeling is noodzakelijk om de veiligheid, betrouwbaarheid en continuïteit van OT-systemen te borgen en om effectief invulling te geven aan de architectuurprincipes, wet- en regelgeving en beheerafspraken.

Door verantwoordelijkheden expliciet te beleggen, wordt samenwerking tussen projecten, beheer en leveranciers versterkt en ontstaat een toetsbaar kader voor sturing en besluitvorming gedurende de gehele cyclus van OT-systemen.

| Bedrijfsfunctie                              | Beschrijving van de wijziging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Informerings</b></p>                   | <p>Functie (actor): <b>assetmanager/ proceseigenaar</b> (accountable)<br/>Projectleider (responsible)</p> <p>Bedrijfsproces:</p> <ul style="list-style-type: none"> <li>informer van de inwoners en/of de eigen medewerkers middels een beschrijving van sensoren in het sensorregister volgens de voorschriften. Dit wordt uitgevoerd door projectleider of de proceseigenaar zelf.</li> </ul> <p>De proceseigenaar is verantwoordelijk dat de inwoners en/of de eigen medewerkers van de gemeente volledig in heldere taal geïnformeerd worden over de sensoren die worden ingezet in een gemeentelijk bedrijfsproces.</p> <p>Informatie: informatie over algoritmen en AI volgens voorschrift en vastgelegd in sensorregister.</p> <p>Applicatie: landelijk sensorregister (beheerd door Kadaster)</p> |
| <p><b>Inkoop- en contract management</b></p> | <p>Functie (actor): <b>assetmanager/ proceseigenaar</b> (accountable)<br/><b>Inkoper</b> (responsible)</p> <p>Bedrijfsproces: inkoop- en contract management.</p> <p>De inkoper:</p> <ul style="list-style-type: none"> <li>adviseert assetmanager/proceseigenaar en projectteam over inkoop van OT- &amp; IT-systeem</li> <li>bepaalt (met projectleider) de inkoopvoorwaarden voor OT (aanvulling op non-functionals) en zorgt voor afspraken met leverancier in SLA die daarna beheerd worden door de functioneel applicatiebeheerder</li> </ul>                                                                                                                                                                                                                                                       |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <pre> graph TD     subgraph "«GEMMA» Ondersteuning"         subgraph "«GEMMA» Inkoop- en contractmanagement"             UC1[inkoper]             UC2[«GEMMA» Uitvoeren inkoop en contractmanagement]             UC3[inkoopvoorwaarden voor OT]             UC4[«GEMMA» Inkoopcomponent]         end     end     UC1 --&gt; UC2     UC2 --&gt; UC3     UC3 --&gt; UC4           </pre> <p>The diagram shows a nested structure. The outer container is «GEMMA» Ondersteuning. Inside it is «GEMMA» Inkoop- en contractmanagement. This container contains four use cases: 'inkoper' (yellow), «GEMMA» Uitvoeren inkoop en contractmanagement (yellow), 'inkoopvoorwaarden voor OT' (orange), and «GEMMA» Inkoopcomponent (blue). Arrows indicate dependencies: 'inkoper' depends on «GEMMA» Uitvoeren inkoop en contractmanagement, which depends on 'inkoopvoorwaarden voor OT', which in turn depends on «GEMMA» Inkoopcomponent.</p> | <p>Informatie:<br/>aanvullende inkoopvoorwaarden voor OT-systeem<br/>aanvullende afspraken t.a.v. verplichtingen voor OT-systeem in SLA Service Level Agreement</p> <p>Applicatie: inkoop- en contract beheer applicatie</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Bedrijfsfunctie                                                                                                                  | Beschrijving van de wijziging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Strategische personeelsplanning</b></p>  | <p>Functie (actor): <b>assetmanager/ proceseigenaar</b> (accountable)<br/>HRM medewerker (responsible)</p> <p>Bedrijfsprocessen:</p> <ul style="list-style-type: none"> <li>• strategische personeelsplanning met medewerkers, zoals het ontwikkelen van OT kennis en vaardigheden, bewustwording</li> <li>• werven van nieuwe medewerkers (ook) met OT kennis en vaardigheden</li> </ul> <p>Informatie:</p> <ul style="list-style-type: none"> <li>• Persoonlijk ontwikkel plan POP voor OT</li> <li>• Strategische Personeel Planning voor individuele medewerker en team voor OT</li> </ul> <p>Applicatie: HRM administratiesysteem</p>                                                                                                                                                                                                                                                 |
| <p><b>Besturing</b></p>                       | <p>Functie (actor): <b>assetmanager/ Proceseigenaar</b> (accountable)</p> <p>Bedrijfsproces:</p> <ul style="list-style-type: none"> <li>• Besturing op alle niveaus versterken door externe bronnen in processen te verwijzen</li> <li>• besluiten nemen voor wel/niet inzetten van OT-systeem in het bedrijfsproces(sen) met de borging van mitigerende maatregelen voor risico's in bedrijf continuïteit en beveiliging</li> <li>• besluiten nemen voor tijdens de exploitatie fase op basis van rapportages van de functioneel applicatiebeheerder en andere disciplines en leverancier over de resultaten van de monitoring bedrijf continuïteit en beveiliging van OT-systeem</li> </ul> <p>Informatie:</p> <ul style="list-style-type: none"> <li>• OT-rapportage opgesteld door functioneel beheerder en andere disciplines en leverancier</li> </ul> <p>Applicatie: projectmap</p> |

| Bedrijfsfunctie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Beschrijving van de wijziging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;"><b>Risicomanagement</b></p>  <pre> graph TD     subgraph "«GEMMA» Bewaking"         subgraph "«GEMMA» Risicomanagement"             direction TB             subgraph "Top Level"                 AM[assetmanager]                 FB[Functioneel Beheerder]             end             subgraph "Bottom Level"                 direction LR                 RA[risico assessments uitvoeren]                 MC[monitoring bedrijfscontinuïteit &amp; beveiliging OT]                 OTRA[OT-risico analyse &amp; maatregelen]                 SLA[SLA leverancier OT]                 CSA[cybersecurity analyse &amp; maatregelen]                 BCP[business continuïteit plan]             end             RA --&gt; MC             OTRA --&gt; SLA             CSA --&gt; BCP         end     end </pre> | <p>Functie (actor): <b>assetmanager/proceseigenaar</b> (accountable)</p> <p>Medewerkers in projectteam (responsible)</p> <ul style="list-style-type: none"> <li>• Decentraal Information Security Officer DISO</li> <li>• Projectarchitect</li> <li>• Recordmanager</li> <li>• OT-specialist</li> </ul> <p>Bedrijfsprocessen - nieuw:</p> <ul style="list-style-type: none"> <li>• Business continuïteit management</li> <li>• Security-by-design voor OT-systemen (beveiliging)</li> <li>• Cybersecurity management</li> <li>• Risico assessments voor inzet van OT-systemen</li> </ul> <p>bestaande werkprocessen:</p> <ul style="list-style-type: none"> <li>• Privacy risk assessment en BIA (optioneel DPIA) - DISO</li> <li>• project start architectuur &amp; toets- Project architect</li> <li>• Informatiebeheer toets - Recordmanager</li> </ul> <p>Informatie/ instrumentarium:</p> <ul style="list-style-type: none"> <li>• Business Continuïteit Plan</li> <li>• Richtlijnen security OT-systemen</li> <li>• OT risico analyse &amp; advies</li> </ul> <p>Applicatie: projectmap</p> |

| Bedrijfsfunctie              | Beschrijving van de wijziging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Kaderbewaking</b><br>     | <p>Functie (actor): <b>assetmanager/ proceseigenaar</b> (accountable)<br/> project architect (responsible)</p> <p>Bedrijfsproces:<br/> Project start architectuur maken voor OT- &amp; IT-systeem op basis van business analyse en getoetst gemeentelijke kaders en richtlijnen</p> <p>Informatie: project start architectuur</p> <p>Applicatie: architectuur repository</p> <p>Functionaris (actor): <b>assetmanager/ proceseigenaar</b> (accountable)<br/> Functioneel beheerder (responsible)</p> <p>Bedrijfsproces:<br/> monitoring van OT-systeem bedrijf continuïteit, beveiliging en performance volgens verplichtingen afgesproken in SLA en inkoopvoorwaarden</p> <p>Informatie: verplichtingen en SLA</p> <p>Applicatie: NVT</p> |
| <b>strategie vorming</b><br> | <p>Functie (actor): <b>directie OO's</b> (accountable)<br/> strategisch adviseur CIO Office (responsible)</p> <p>Bedrijfsproces:<br/> OT-beleid/ Uitvoeringskader voor de inzet van OT-systemen in gemeente</p> <p>Informatie:<br/> visie, beleid &amp; strategie voor de inzet van OT in de gemeente gebaseerd op gemeente doelstellingen en Europese- landelijke- en gemeentelijke kaders</p> <p>Applicatie: intranet</p>                                                                                                                                                                                                                                                                                                                |

| bedrijfsfunctie | Beschrijving |
|-----------------|--------------|
|-----------------|--------------|

|                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Automatisering management</b></p>  | <p>Functie (actor):<br/> Assetmanager/ proceseigenaar (accountable)<br/> projectteam (responsible) tijdens ontwikkeling<br/> functioneel beheerder (responsible) in beheer name en exploitatie OT-systeem</p> <p>Bedrijfsprocessen:<br/> Assetmanager: opdrachtgeven en regievoeren over laten leveren (ontwikkelen) van OT- en/of IT-systeem door aanbieder volgens afspraken<br/> projectteam: toetsen en uitvoeren acceptatie testen en OT-systeem functioneel in gebruik en beheer nemen<br/> Functioneel beheerder: toetsen en testen van OT- &amp; IT systeem tijdens de exploitatie fase</p> <p>Informatie/ instrument:</p> <ul style="list-style-type: none"> <li>• Opdracht beschrijving aan leverancier technisch ontwerp volgens project start architectuur incl. documentatie</li> <li>• Acceptatietest plan en testresultaten voor OT-systeem</li> <li>• In beheer name plan en monitoring performance van OT</li> <li>• Functioneel beheer werkinstructie monitoring OT</li> </ul> <p>Applicatie: projectmap en beheer map</p> |
|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 5.4 RASCI-tabel – Functioneel beheer OT-systemen

Verantwoordelijkheden en functies in onderstaande tabel:

| Activiteit                                                                                                                             | Functioneel beheer OT | Technisch beheer OT | Systeemeigenaar / Asset Owner | Architectuur | Cybersecurity | Leverancier |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|-------------------------------|--------------|---------------|-------------|
| Vaststellen functionele eisen                                                                                                          | R                     | C                   | A                             | C            | C             | I           |
| Beheer van gebruikersfunctionaliteit                                                                                                   | R                     | C                   | A                             | I            | I             | I           |
| Beoordelen wijzigingsverzoeken                                                                                                         | R                     | C                   | A                             | C            | C             | I           |
| Ontwerpen technische oplossing                                                                                                         | I                     | R                   | C                             | C            | C             | R           |
| Uitvoeren configuratiewijziging                                                                                                        | I                     | R                   | I                             | I            | I             | R           |
| Architectuurtoets                                                                                                                      | C                     | I                   | I                             | R            | C             | I           |
| Securitytoets (IEC-62443 / NIS2)                                                                                                       | R                     | C                   | A                             | I            | I             | C           |
| Testen en acceptatie (functioneel)                                                                                                     | I                     | R                   | A                             | I            | C             | C           |
| Incident en calamiteitenafhandeling                                                                                                    | R                     | R                   | A                             | I            | C             | C           |
| Lifecycle- en end-of-life planning                                                                                                     | R                     | C                   | A                             | C            | C             | I           |
| Legenda:<br>• R = Responsible (uitvoerend)<br>• A = Accountable (eindverantwoordelijk)<br>• C = Consulted (adviserend)<br>I = Informed |                       |                     |                               |              |               |             |

### Binnen het domein fysieke leefomgeving. Beheer van de referentiearchitectuur (eigenaarschap, wijzigingen, architectuurboard, versiebeleid)

Het beheer van de referentiearchitectuur is essentieel om consistentie, kwaliteit en toekomstvastheid te borgen. Daarom is een duidelijke governance structuur noodzakelijk, met afspraken over eigenaarschap, wijzigingsbeheer, besluitvorming en versiebeleid.

#### Eigenaarschap

De gemeente Utrecht is eigenaar van de OT-referentiearchitectuur. Dit eigenaarschap omvat:

- Het vaststellen van inhoud en reikwijdte
- Het bewaken van de samenhang imet de enterprise architectuur, IT-architectuur en Common-Ground
- Het borgen van data eigenaarswchap en kwaliteit
- Het bepalen van standaarden, richtlijnen en bouwblokken.

Het eigenaarschap ligt formeel bij de lead Enterprise architect of door de organisatie aangewezen eindverantwoordelijke.

## Wijzigingsbeheer

De referentiearchitectuur is een levend document dat meegroeit met technologische ontwikkelingen, wet- en regelgeving, gemeentelijke ambities en inzichten uit projecten. Wijzigingen worden beheerd volgens een gecontroleerd proces:

1. **Initiatie:** Wijzigingsvoorstellen kunnen worden ingediend door projecten, leveranciers, beheerteams of architecten.
2. **Analyse:** De impact op veiligheid, beheer, standaarden, interoperabiliteit en kosten worden beoordeeld door het architectuurteam.
3. **Advies:** Een conceptwijziging wordt besproken binnen de architectuurboard (zie hieronder).
4. **Besluitvorming:** Na goedkeuring wordt de wijziging opgenomen in de eerstvolgende versie van de referentiearchitectuur.
5. **Communicatie:** Wijzigingen worden gedeeld met projecten, leveranciers en beheerteams, inclusief instructies voor implementatie.

## Architectuurboard

De Architectuurboard is het centrale besluitvormingsorgaan voor wijzigingen in de referentiearchitectuur. De board bestaat uit:

- Domeinarchitecten IT en OT
- Security specialisten
- Vertegenwoordigers van beheer (OT-beheer, netwerkbeheer, SCADA-beheer)
- Vertegenwoordigers van relevante projecten of programma's indien nodig – externe experts of leveranciers

De board heeft de volgende verantwoordelijkheden:

- Beoordelen en goedkeuren van de wijzigingsvoorstellen
- Bewaken van de consistentie tussen OT, IT en IoT en Enterprise architectuur
- Toetsen of de wijzigingen voldoen aan wet- en regelgeving (IEC-62443, BIO, NIS2)
- Prioriteren van architectuurontwikkelingen
- Vaststellen van nieuwe standaarden en bouwblokken

## Versiebeheer

Om transparantie en traceerbaarheid te waarborgen wordt een formeel versiebeleid gehanteerd voor de referentiearchitectuur:

- **Major releases (X.0)**  
Grote wijzigingen, nieuwe architectuurprincipes, nieuwe zones/conduits- modellen, of ingrijpende wijzigingen in beveiligingskaders
- **Major releases (X.Y)**  
Aanpassingen in bouwblokken, verduidelijkingen, toevoegingen van standaarden of nieuwe koppelingen
- **Major releases (X.Y.Z)**  
Kleine correcties, tekstuele veranderingen of verduidelijkingen zonder tekstuele impact

Elke versie omvat

- Een changelog
- Datum inwerkingtreding
- Overzicht van impact op lopende projecten
- Instructies voor adoptie

## 6. Hoofdproces levenscyclus OT-systeem

Het hoofdproces voor operationele technology (OT-systeem), vergelijkbaar met de levenscyclus van een IT-systeem. Met de belangrijkste kenmerken:

- De fasen worden uitgevoerd door een **multidisciplinair team** met alle disciplines vertegenwoordigd
- We sluiten aan op gemeentelijk OT-beleid
- We maken gebruik van de **bestaande governance & werkprocessen** voor **IT-projecten** in de gemeente (bijvoorbeeld architectuurproces, risicoassessments)
- We maken gebruik van **nieuwe instrument: OT-risico analyse** én aanvullende **inkoopvoorwaarden** en aansluitvoorwaarden/**non-functionals** voor OT-systemen.

### 6.1 OT-systeem ontwerp en realisatie onder architectuur

Voor het ontwerpen, de levering (ontwikkeling), testen en beheer van OT-systemen werken we **onder architectuur** zoals we dit ook voor IT-projecten ook doen. In onderstaande tabel is beschreven dat de project architect (onderdeel van multidisciplinair projectteam) een architectuur ontwerp maakt óók voor het OT-systeem (eventueel enkele oplossingsrichtingen en scenario's) in de project start architectuur. De OT-systeem leverancier/ aanbieder maakt een solution architectuur dat door de projectarchitect getoetst wordt. Tijdens de realisatie fase wordt het OT-systeem getoetst op de project start architectuur. Ook tijdens de exploitatie fase (monitoring) wordt op reguliere basis een architectuur toets van het OT-systeem uitgevoerd in samenwerking met de andere disciplines getoetst.

| fase                                      | Toelichting werken onder architectuur                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | product                                         |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Ontwerpen en ontwikkelen van de oplossing | Door de projectarchitect wordt de project start architectuur gemaakt, met de architectuurbouwblokken en -patronen & richtlijnen. De risico assessments worden uitgevoerd incl. een OT risico analyse en de mitigerende maatregelen voor o.a. beveiliging en bedrijf continuïteit, etc. wordt beschreven in project start architectuur. De aansluitvoorwaarden/non-functionals voor OT-systeem worden specifiek gemaakt voor het project. Project start architectuur en non-functionals voor OT-systeem zijn onderdeel van programma van eisen | project start architectuur & OT non-functionals |
| Realiseren van de oplossing               | Dit is de fase waarin de OT- & IT-systeem wordt ingericht door de leverancier. Hiervoor maakt de leverancier een solution design/architectuur volgens project start architectuur en non-functionals (aansluitvoorwaarden)                                                                                                                                                                                                                                                                                                                     |                                                 |
| Test & implementatie                      | In deze fase wordt algoritme of OT-systeem getest of gebouwd is volgens de project start architectuur en of voldoet aan de businessanalyse en businesscase. Na testen in testomgeving wordt het naar productieomgeving                                                                                                                                                                                                                                                                                                                        | Testrapport architectuur toets                  |

|                                          |                                                                                                                                                      |                                |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
|                                          | gebracht en geïntegreerd in het bedrijfsproces volgens het architectuurontwerp en de generiek en specifieke implementatierichtlijnen                 |                                |
| 7. Beheer, doorontwikkeling & monitoring | Het OT-systeem wordt in deze fase voortdurend gemonitord om ervoor te zorgen dat het blijft presteren zoals afgesproken in inkoopvoorwaarden en SLA. | Testrapport architectuur toets |

## 6.2 Nieuw instrument kwetsbaarheid- en risicoanalyse OT-systeem

We ontwikkelen een nieuw instrument voor kwetsbaarheid- en risicoanalyse van OT-systeem dat toegepast wordt in de ontwerp fase van projecten of voor een bestaand OT-systeem. Met uitvoering van kwetsbaarheid- en risicoanalyse maken we in 3 pijlers kwetsbaarheden en risico's inzichtelijk: OT architectuur, IT/OT verwevenheid en cybersecurity. In iedere pijler analyseren we op gebied van mens, techniek en proces, de focusgebieden waarin mogelijke kwetsbaarheden en risico's kunnen ontstaan. Focusgebieden analyseren we m.b.v. documentatie en interviews met relevante personen uit organisatie. In analyse nemen we relevante normen en standaarden mee, zoals GEMMA, IEC-62443 en de BIO. Bron: Verminderen kwetsbaarheid en risico's IT/OT integratie in het waterdomein (twynstragudde.nl)

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Business Driver</b><br>(aanleiding)<br>Het gebruik van IT technologie neemt toe in de procesautomatisering, dat leidt tot integratievraagstukken tussen OT en IT. Dat kan leiden tot onverwachte kwetsbaarheden.<br>Daarnaast kan een klant specifieke aanleidingen hebben voor een kwetsbaarhedenonderzoek. Voorbeelden zijn het voornemen om een deel van de IT of OT te outsourcen, een recent security incident, etc. De business driver stuurt het onderzoek in een klantspecifieke richting. |                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Inventarisatie PA domeinen</b>                                                                                                                                                                                                                                                                                                                                                | <b>Onderzoek kwetsbaarheden</b>                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Risico's en aanbevelingen</b>                                                                                                                                                                                                                                                                                                                                                           |
| <b>Techniek</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>Inventarisatie en bestudering bestaande architec-tuurdocumentatie voor automatisering van water-keten, watersysteem</li> <li>Identificering OT- en IT-onderdelen</li> <li>Identificering netwerk topologie en security maatregelen</li> <li>Deskstudie aangevuld met interviews van architect of lead engineers, indien nodig.</li> </ul> | Technische kwetsbaarheden worden besproken naar aanleiding van de inventarisatie en de business driver(s). Typische kwetsbare domeinen zijn: <ul style="list-style-type: none"> <li>Integratie OT en IT technologie</li> <li>Cybersecurity</li> <li>Quality attributen zoals schaalbaarheid, beschikbaarheid, uitwijkmogelijkheden.</li> </ul> Het onderzoek wordt gedaan middels interviews met architecten en lead engineers. | Er worden twee integrale spiegelsessies georganiseerd. Voor beide spiegelsessies worden alle geïnterviewden en de opdrachtgever(s) uitgenodigd.<br><br>In de eerste sessie worden de deelnemers meegenomen in de bevindingen en kwetsbaarheden. Deze betreffen alle assen: Techniek, Mens en Organisatie en Proces. De deelnemers worden gevraagd om te reflecteren op het gepresenteerde. |
| <b>Mens en Organisatie</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>Inventarisatie organisatiestructuur van de PA domeinen</li> <li>Onderverdeling IT en OT specialisten per domein</li> <li>Competenties IT en OT specialisten</li> <li>Eigen organisatie en leveranciers</li> <li>Deskstudie en interview met betreffende managers.</li> </ul>                                                              | M&O kwetsbaarheden worden besproken naar aanleiding van de inventarisatie en de business driver(s). Typische kwetsbare domeinen zijn: <ul style="list-style-type: none"> <li>Samenwerking IT en OT engineers</li> <li>Kennisiniveau en innovatiekracht</li> <li>Arbeidsmarkt en vergrijzing.</li> </ul> Het onderzoek wordt gedaan middels interviews met management en architecten/lead engineers.                             | In de tweede sessie wordt gekeken naar de risico's in de PA domeinen, ook weer over de Techniek, Mens en Organisatie en Processen. De gespreksleider haalt samen met de deelnemers de risico's naar boven. Op deze manier worden de risico's gedragen door de organisatie.<br><br>De gedocumenteerde aanbevelingen worden geformuleerd als concrete handvatten voor de organisatie.        |
| <b>Proces</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>Inventarisatie beheerprocessen, waaronder Incident management, regulier onderhoud</li> <li>Inventarisatie nieuwbouw/vervangingsprocessen</li> <li>Inventarisatie processtandaarden</li> <li>Inventarisatie outsourcing en regie.</li> </ul>                                                                                               | Procesmatige kwetsbaarheden worden besproken naar aanleiding van de inventarisatie en de business driver(s). Typische kwetsbare domeinen zijn: <ul style="list-style-type: none"> <li>IT vs OT beheerprocessen</li> <li>Uitbesteding en regievoering</li> <li>Fallbacksituaties</li> <li>Beheer op afstand vs lokaal beheer</li> <li>Cybersecurity.</li> </ul>                                                                  | Ter afsluiting worden de kwetsbaarheden, risico's en aanbevelingen samenvattend gepresenteerd aan de opdrachtgever.                                                                                                                                                                                                                                                                        |

Figuur ...

## 6.3 Aansluitvoorwaarden / non-functionals voor OT-systemen

De aansluitvoorwaarden/non-functionals worden uitgebreid met eisen voor OT-systeem.

Pas 'security by design' toe en tref compenserende maatregelen in OT-systeem. Voorbeelden van aanvullende non-functionals zijn: fysieke toegangsbeveiliging van bedienlocaties en maatregelen op netwerkniveau, zoals het versleutelen van datacommunicatie via VPN-tunnels en het opdelen van het OT-netwerk in afgescheiden segmenten zodat niet de OT blootgesteld wordt aan een hackpoging. Realiseer veilige beheertoegang tot het OT-netwerk van monteurs en ander personeel, devices in eigen beheer uit te geven en/of met geautomatiseerde controles op het beveiligingsniveau. Fysieke objecten bedienen alleen via vertrouwde netwerken, zoals het besloten OT-netwerk en eventueel een beheernetwerk.

## **6.4 Nieuwe werkwijzen functioneel beheer OT-systeem**

In deze paragraaf zijn nieuwe werkwijzen (best practices) beschreven voor medewerkers in het beheer en gebruik van OT-systemen. Hiervoor kunnen trainingen en instructies gemaakt worden.

De gemeente Utrecht hanteert voor functioneel beheer van OT-systemen een eenduidige werkwijze die aansluit op de vastgestelde thema architectuur OT en op de bestaande gemeentelijke beheer- en beleidskaders. Functioneel beheer is verantwoordelijk voor het borgen van de functionaliteit, gebruik en informatievoorziening van OT-systemen en opereert binnen duidelijk afgebakende verantwoordelijkheden ten opzichte van technisch beheer en operationele besturing.

Binnen deze werkwijze is de rolverdeling als volgt ingericht: functioneel beheer is verantwoordelijk (R) voor de configuratie van wijzigingen en afstemmen met ketenpartners; technisch beheer is uitvoerend verantwoordelijk (R) voor configuratie, onderhoud en technische wijzigingen; de asset- of systeemeigenaar is eindverantwoordelijk (A) voor besluitvorming over wijzigingen; cybersecurity en architectuur zijn adviserend (C) en toetsen de naleving van architectuurprincipes, normen en richtlijnen; gebruikers en operationele rollen zijn geïnformeerd (I) over wijzigingen en impact.

Wijzigingen aan OT-systemen worden uitsluitend doorgevoerd via vastgestelde wijzigingsprocessen en getoetst aan de thema architectuur OT, de Purdue Reference Architecture en relevante normen waaronder IEC-62443 en NIS2. Functioneel beheer borgt dat security, continuïteit en beheersbaarheid integraal onderdeel zijn van wijzigingsvoorstellen en beheeractiviteiten.

Voor leveranciers gelden expliciete toetsingscriteria. Leveranciers dienen aantoonbaar te werken conform de vastgestelde OT-architectuur, de gescheiden verantwoordelijkheden tussen OT en IT te respecteren en wijzigingen uitsluitend via de gemeentelijke beheerprocessen te laten verlopen. Daarnaast moeten zij inzicht geven in de lifecycle-ondersteuning, cybersecuritymaatregelen (IEC 62443) en de impact van de wijzigingen op beschikbaarheid en veiligheid van OT-systemen.

Deze werkwijze is geharmoniseerd met bestaande gemeentelijke beleidsdocumenten en beheerhandboeken van de gemeente Utrecht en is compatibel met de best practices en de architectuurbenadering van Rijkswaterstaat.

## 6.5 Cyber Security Management System

**Nieuwe werkwijze:** Voor het beschermen van OT-assets is er het Cyber Security Management System (CSMS) op basis van IEC 62443 (normdeel 2-1). Het geeft concreet inzicht in welke OT-assets een organisatie in huis heeft, waar de cybersecurityrisico's zitten en wat de te nemen maatregelen zijn. Een CSMS omvat alle OT van een organisatie, de risicoanalyses en daaruit voortvloeiende cybersecurity maatregelen per soort OT (de kwetsbaarheden per soort kunnen verschillen). Voor de cybersecurity risicoanalyse aansluiten bij risicoanalysemethodieken die al in de organisatie gebruikt worden.

## 6.6 Cybersecurity op strategisch en tactisch niveau

- **Nieuwe taken op strategisch niveau** beleggen, bijvoorbeeld een Chief Information Security Officer (CISO): security-beleid naast informatie, ook de OT-assets worden meegenomen.
- **Tactisch niveau** bij de business assetmanagers en lijnmanagement.

## 6.7 Organiseer het beheer van de OT structureel

**Nieuw: inrichten regie-organisatie en functioneel beheer** in gemeente. Over de beheertaken die bij leveranciers liggen contractuele afspraken maken in 'service level agreements' waarin de eisen op het gebied van cybersecurity uit de risicoanalyses worden meegenomen.

## 6.8 Preventief beheer om cybersecurity incidenten te voorkomen

**Nieuwe werkwijze:** preventieve (technische) maatregelen nemen om cybersecurity incidenten te voorkomen. De norm IEC 62443 (deel 2-1) bevat een overzicht van mogelijke maatregelen per onderdeel van het CSMS. Op basis van een risicoanalyse kan de gemeente hieruit een keuze maken. Test regulier de effectiviteit van de preventieve maatregelen middels security assessments, bijvoorbeeld voer penetratietests en vulnerability scans uit.

## 6.9 Richt business continuïteit management

**Nieuwe werkwijze:** Er kunnen security incidenten optreden die leiden tot calamiteiten binnen de OT. Opstellen en borgen van calamiteiten herstelprocedures, inclusief tijdelijke lokale bediening, etc. op basis van de maximaal toegestane hersteltijd. Deze varieert per soort OT en kan worden bepaald met een business impact-analyse voor het aspect 'beschikbaarheid'. Het vastleggen en borgen business continuïteit plan met periodiek evalueren en waar nodig te testen.

## 7. Nieuwe architectuur bouwblokken

De informatie in hoofdstuk 8 is meer gedetailleerd. De doelgroep van hoofdstuk 8 zijn de architecten die de project start architecturen maken.

Voor de capability “beheer van operationele technology” zijn nieuwe architectuur bouwblokken nodig. Dit zijn componenten waarmee een OT- & IT systeem gerealiseerd/ geleverd kan worden en hebben de volgende kenmerken:

- Herbruikbaar: hetzelfde onderdeel kan steeds opnieuw binnen de organisatie worden gebruikt
- Vervangbaar: het kan worden uitgewisseld met een andere component met dezelfde functionaliteit
- Modulair: kan gebaseerd zijn op andere architectuurcomponenten
- Fundamenteel: andere architectuurcomponenten kunnen hierop gebaseerd zijn

Op basis van de businessanalyse voor AI-systeem (en businesscase) wordt een functioneel ontwerp gemaakt met behulp van de **OT-architectuurbouwblokken**. Het samenstellen van de OT-architectuurbouwblokken gaat volgens **architectuurpatronen** met bijhorende aansluitvoorwaarden/**non-functionals** (beschreven in een separaat document).

In onderstaand figuur zijn de nieuwe OT-architectuurbouwblokken weergegeven en zijn onderverdeeld volgens het Internationaal Perdue-model. Purdue-model is Enterprise Reference Architecture uit \ ISA-95 standaard voor verticale integratie van 5 automatiseringsniveaus

- Niveau 4 – generiek IT-systemen voor besturing van de OT ten behoeve van bedrijfsprocessen
- Niveau 3,5 – OT DMZ Demilitarized Zone
- Niveau 3 – OT netwerk
- Niveau 2 – OT supervisie centrale besturing operationele processen
- Niveau 1 – OT besturing Human Machine Interface
- Niveau 0 – OT fysieke systemen

Tevens zijn ook de architectuurbouwblokken weergegeven die vanuit andere Thema architecturen gebruikt kunnen worden voor het ontwerp van een OT- & IT-systeem.

In de bijlage is de beschrijving van alle architectuur bouwblokken.

## OT Thema architectuur bouwblokken (ABB Architecture Building Blocks)



Figuur: ... OT-architectuurbouwblokken en relevante architectuur bouwblokken van andere Thema architecturen

## 7.1 Gebruik architectuur bouwblokken andere thema architecturen

In het ontwerp en de ontwikkeling van OT toepassingen kan gebruik worden gemaakt van architectuur bouwblokken uit andere thema architecturen. In deze paragraaf zijn voorbeelden genoemd van architectuur bouwblokken die kunnen worden gebruikt.

### Thema integratie architectuur

API's (REST API; 2/3 D geowebsservices; GraphQL, SensorThings API) API's spelen een belangrijke rol in de integratie tussen OT en IT, maar uitsluitend in de hogere lagen van het Purdue-model (niveau 3–4). Ze worden gebruikt om **OT-data veilig en gecontroleerd beschikbaar te maken**, bijvoorbeeld voor monitoring, assetmanagement, voorspellend onderhoud of rapportages.

### API's zijn van belang voor OT-integratie omdat het zorgt voor;

- Veilige datastromen API's maken het mogelijk om sensordata, statusinformatie en storingsmeldingen uit OT-systemen te ontsluiten zonder directe koppeling met PLC's of SCADA-servers.
- Strikte domeinscheiding API's worden geplaatst in een DMZ of data-ontsluitingslaag (Purdue 3.5), zodat het OT-domein beschermd blijft.
- Standaardisatie en interoperabiliteit Door gebruik te maken van open standaarden (REST, OGC SensorThings API) kunnen verschillende leveranciers en systemen op een uniforme manier integreren.
- Ondersteuning datakwaliteit en governance API's zorgen voor consistente, traceerbare en betrouwbare ontsluiting van OT-data richting IT-systemen.

### Toelichting per type API

- REST API Geschikt voor het ontsluiten van statusinformatie, loggegevens en configuratiegegevens uit OT-systemen richting IT-toepassingen.
- 2D/3D-geowebsservices Relevant voor geografisch gepositioneerde OT-objecten zoals bruggen, gemalen en tunnels. Ondersteunt visualisatie in GIS-systemen.
- GraphQL Handig voor complexe datamodellen waarbij IT-systemen flexibel subsets van OT-data willen opvragen zonder de OT-bron te belasten.
- SensorThings API Een OGC-standaard voor IoT- en sensordata, zeer geschikt voor OT-omgevingen met veel meetpunten (waterbeheer, verkeersmanagement, energie).

### Randvoorwaarden voor gebruik van API's in OT-architectuur

Bij toepassing van API's gelden de volgende OT-specifieke eisen:

- API's worden nooit direct gekoppeld aan PLC's, RTU's of SCADA-servers.
- Ontsluiting vindt plaats via een gesegmenteerde architectuur (zones & conduits volgens IEC 62443).
- Alleen read-only ontsluiting vanuit OT naar IT, tenzij er expliciet een gecontroleerd terugschrijfmecanisme is ingericht.
- API-gateways worden geplaatst in Purdue-niveau 3.5 (DMZ).
- Alle API-koppelingen worden gelogd, gemonitord en geaudit.

- Authenticatie, autorisatie en certificaatbeheer zijn verplicht.

## Resultaat

Met deze aangepaste tekst sluit de integratie-architectuur volledig aan op:

- OT-principes
- Purdue-model
- IEC 62443
- Gemeentelijke OT-kaders
- De behoefte aan veilige, gecontroleerde datastromen

Voorbeelden van **architectuur bouwblokken** in het ontwerp van een OT toepassing zijn (niet uitputtend):

API's (REST API; 2/3 D geowebsservices; GraphQL, SensorThings API)

## Security Thema architectuur

Er kan bijvoorbeeld gebruik worden gemaakt van de volgende **architectuur bouwblokken** in het ontwerp van een AI toepassing (niet uitputtend):

Beveiliging op infrastructuur

Beveiliging van registratie (bron)systemen

Beveiliging van API en API gateway

Veilige gegevensuitwisseling met authenticatie via Persoonlijke Toegangstokens (PATs)<sup>3</sup>

Toegangsbeheer beveiliging middels authenticatie en autorisatie (doelbinding)

## 7.2 Beschrijving van architectuur bouwblokken

In deze paragraaf is de beschrijving van de architectuur bouwblokken.

|                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>Telemetrie<br/>informatiesysteem</p> <p>monitoring</p> <p>alarmering</p> | <p><b>Telemetrie informatiesysteem/ applicatie</b></p> <p>Een telemetrie- of SCADA-informatiesysteem (Supervisory Control and Data Acquisition) ondersteunt de centrale bewaking en aansturing van operationele processen binnen de fysieke infrastructuur. Het systeem verzamelt real-time gegevens uit het veld, visualiseert de status van objecten en maakt het mogelijk om waar nodig beheersmaatregelen te nemen.</p> |
|  <p>secure gateway</p>                                                       | <p><b>Secure gateway</b></p> <p>De SCADA-software staat via een beveiligde gateway, router en het private OT-netwerk in verbinding met PLC's en andere</p>                                                                                                                                                                                                                                                                  |

<sup>3</sup> Persoonlijke Toegangstokens (PATs) zorgen voor veilige gegevensuitwisseling doordat elke gebruiker of systeemcomponent een uniek, niet-overdraagbaar token krijgt waarmee toegang wordt verleend. Deze tokens bevatten alleen de strikt noodzakelijke rechten, zijn eenvoudig in te trekken en volledig te loggen, waardoor toegang tot OT-data controleerbaar, traceerbaar en goed beveiligd blijft.

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | <p>besturingscomponenten. Deze PLC's sturen op hun beurt de fysieke installaties aan, zoals pompen, bruggen, sluizen of ventilatiesystemen. Het telemetriesysteem vormt daarmee de schakel tussen de procesbesturing in het veld en de centrale bediening, monitoring en alarmering.</p>                                                                                                                                                                                                                                                                                                                                                                                             |
| <div>industriële router</div>                              | <p><b>Industriële router</b></p> <p>De industriële router vormt de beveiligde toegangspoort tussen het veldobject en het centrale OT-netwerk. Deze router:</p> <ul style="list-style-type: none"> <li>• ondersteunt redundante verbindingen (bijv. vaste lijn + 4G/5G-fallback),</li> <li>• biedt firewall-functionaliteit en VPN-tunnels,</li> <li>• zorgt voor versleutelde communicatie tussen object en centrale systemen,</li> <li>• is bestand tegen industriële omstandigheden (temperatuur, trillingen, vocht).</li> </ul>                                                                                                                                                   |
| <div>4G/5G private APN</div>                               | <p><b>4G/ 5g private APN</b> Voor de communicatie tussen veldobjecten en de centrale OT-omgeving wordt vaak gebruikgemaakt van een <b>private APN</b> binnen een 4G/5G-netwerk. Dit biedt:</p> <ul style="list-style-type: none"> <li>• een volledig afgeschermd mobiele dataverbinding,</li> <li>• geen toegang vanaf het publieke internet,</li> <li>• gegarandeerde bandbreedte en latency,</li> <li>• beheersbare IP-ranges voor OT-objecten,</li> <li>• een extra beveiligingslaag bovenop VPN-tunnels.</li> </ul> <p>Deze verbinding maakt het mogelijk om objecten op afstand te monitoren zonder dat de procesbesturing direct wordt blootgesteld aan externe netwerken.</p> |
| <div>PLC<br/>Programmeerbare<br/>Logische Controller</div> | <p><b>PLC / RTU</b></p> <p>De Programmable Logic Controller (PLC) of Remote Terminal Unit (RTU) vormt de kern van de lokale procesbesturing. Deze component:</p> <ul style="list-style-type: none"> <li>• leest sensoren uit,</li> <li>• stuurt actuatoren aan (bijv. pompen, kleppen, slagbomen),</li> <li>• voert logica uit voor veilige en autonome werking,</li> <li>• blijft functioneren bij netwerkuitval,</li> <li>• communiceert met SCADA via industriële protocollen (bijv. Modbus, DNP3, IEC-104).</li> </ul> <p>PLC's en RTU's bevinden zich in de lagere lagen van het Purdue-model (niveau 1–2) en worden strikt gescheiden van IT-systemen.</p>                     |

|                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div data-bbox="178 394 451 488">  schakelaar </div>     | <p><b>Industriële schakelaar</b></p> <p>De industriële schakelaar (switch) vormt de lokale netwerkhub binnen het object. Deze:</p> <ul style="list-style-type: none"> <li>• verbindt PLC's, sensoren, actuatoren en de industriële router,</li> <li>• ondersteunt VLAN-segmentatie en QoS,</li> <li>• is ontworpen voor robuuste OT-omgevingen,</li> <li>• speelt een rol in het afdwingen van zones &amp; conduits volgens IEC 62443.</li> </ul>                                                                                                                                                                       |
| <div data-bbox="178 801 489 929">  sensorregister </div> | <p><b>Sensorregister</b></p> <p>Het sensorregister is een centraal informatieobject waarin alle sensoren binnen de OT-omgeving worden vastgelegd. Het bevat onder andere:</p> <ul style="list-style-type: none"> <li>• type sensor en meetprincipe,</li> <li>• locatie en gekoppeld object,</li> <li>• dataklasse en gevoeligheid,</li> <li>• eigenaar en beheerder,</li> <li>• doel van de meting,</li> <li>• wettelijke en privacy-aspecten.</li> </ul> <p>Het sensorregister ondersteunt transparantie richting inwoners en medewerkers, en vormt een basis voor datakwaliteit, governance en risicobeoordeling.</p> |

## 8. Architectuur patronen

Architectuurpatronen zijn veelvoorkomende samenstellingen van de architectuur bouwblokken die nodig zijn om een OT-systeem toepassing functioneel te ontwerpen. Architectuurpatronen zijn bedoeld als inspiratie voor het ontwerp van een project start architectuur. In dit hoofdstuk wordt beschreven hoe architectuurblokken voor het geïntegreerde OT-IT-domein worden ontworpen, beheerd en toegepast. De richtlijn sluit aan op:

- Het Purdue-model voor OT-segmentatie
- De Archimate standaard voor architectuurmodellering
- De interne EA-governance en repository structuur van de gemeente

Het doel is om:

- Consistente en herbruikbare bouwblokken te creëren
- IT-OT-integratie veilig en beheersbaar te controleren
- De EA-repository te verrijken met gestandaardiseerde Archimate componenten

### 8.7 Principes voor IT-OT-architectuur binnen de gemeente Utrecht

De volgende principes vormen de basis voor bouwblokken:

#### Scheiding van domeinen

- IT en OT worden logisch én fysiek van elkaar gescheiden volgens het Purdue-model
- Communicatie verloopt uitsluitend via gecontroleerde DMZ

#### Standaardisatie van bouwblokken

- Alle bouwblokken worden gemodelleerd in ARchimate en opgeslagen in de EAU-repository
- Bouwblokken zijn domein-onafhankelijk waar mogelijk, domein-specifiek waar noodzakelijk

#### Security by design

- Elk bouwblok bevat expliciete security-aspecten (authenticatie, segmentatie, monitoring, logging)
- OT-componenten worden minimaal blootgesteld aan IT-systemen

#### Herbruikbaarheid

- Bouwblokken worden modulair opgebouwd zodat ze in meerdere projecten toepasbaar zijn

- Varianten worden uitsluitend gemaakt als dit functioneel noodzakelijk is

## **8.8 Structuur van architectuurbouwblokken**

Ieder bouwblok wordt in de EAU-repository opgenomen met een vaste structuur:

### **1. Identificatie**

- Naam
- EAU-repository ID
- Domein (IT, OT, DMZ, generiek)
- Relatie met Purdue-niveau

### **2. Archimate-representatie**

- Archimate-laag (Business, Application, Technologie)
- Archimate-type (Component, Device, Interface, Service, Node, etc.)

### **3. Functionele beschrijving**

- Doel en functionaliteit
- Interacties met andere bouwblokken
- Afhankelijkheden

### **4. Security & compliance aspecten**

- Toegangsbeperkingen
- Logging en monitoring
- Netwerksegmentatie
- Relevante wet- en regelgeving (BIO, NIS2, gemeentelijke kaders)

### **5. Integratie aspecten**

- Interfaces (API, OPC, UA, MQTT, REST, SOAP, file-based)
- Protocolspecificaties
- Richtlijnen voor dataflow-modellering

## 8.9 Bouwblokken voor IT-OT-integratie volgens het Purdue-model

### 1. OT-bouwblokken (Purdue-levels 0-3)

| Bouwblok                 | Archimate symbol      |
|--------------------------|-----------------------|
| 1. Sensor/Actuator       | Device                |
| 2. PLC/RTU               | Device                |
| 3. SCADA-server          | Application Component |
| 4. Historian OT          | Application Component |
| 5. MES                   | Application Component |
| 6. OT-Directory Services | Application Service   |
| 7. OT-Network Zone       | Technology Node       |

### 2. DMZ-bouwblokken (Purdue-levels 3.5)

| Bouwblok                                                                                                                                                            | Archimate symbol      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 8. Data Broker / Message Broker <ul style="list-style-type: none"><li>o MQTT-broker</li><li>o AMQP-broker</li><li>o OPC UA gateway</li><li>o Kafka-bridge</li></ul> | Application Component |
| 9. Reverse Proxy                                                                                                                                                    | Application Component |
| 10. Jump Server                                                                                                                                                     | Technology Node       |
| 11. Secure File Transfer Node                                                                                                                                       | Application Component |
| 12. DMZ-firewall                                                                                                                                                    | Technology Device     |
| 13. Monitoring Probe                                                                                                                                                | Technology Component  |

### 3. IT-bouwblokken (Purdue levels 4-5)

| Bouwblok                       | Archimate symbol      |
|--------------------------------|-----------------------|
| 14. ERP                        | Application Component |
| 15. Data Warehouse / Data Lake | Application Component |
| 16. IAM                        | Application Service   |
| 17. Analytics platform         | Application Component |
| 18. IT-Network Zone            | Technology Device     |

## 8.4 Modelleren van IT-OT-integratie in Archimate

### 1. Gebruik van lagen

- Technologie-laag: Fysieke OT-apparatuur, netwerksegmenten, firewalls
- Application-laag: SCADA, MES, brokers, interfaces
- Business-laag: processen als assetbeheer, storingsafhandeling, productieplanning

### 2. Modelleren van dataflows

- Gebruik flow-relaties voor datastromen
- Benoem richting (IT -> DMZ -> OT of OT -DMZ -> IT)
- Vermijd directe IT-> OT flows; altijd via DMZ-bouwblokken

### 3. Modelleren van security

- Gebruik Archimate Motivation-elementen voor security doelen
- Gebruik Constraints voor segmentatie-regels
- Gebruik Requirements voor compliance-eisen

### 4. Modelleren van brokers in DMZ

Een broker wordt gemodelleerd als:

- Application Component (de broker zelf)
- Application Service (publicatie/subscriptie-dienst)
- Technology Node (de server of VM waarop de broker draait)
- Interface (MQTT, AMQP, OPC UA, REST)

## 8.5 Governance en beheer in de EA-repository

### 1. Rollen

- Enterprise Architect: Eigenaar van de bouwblokken
- OT-Architect: Domeinspecialist voor OT-componenten
- IT-Architect: Domeinspecialist voor IT-componenten
- Security Officer: Borging van security-aspecten

### 2. Wijzigingsbeheer

- Nieuwe bouwblokken worden via een wijzigingsverzoek ingediend
- Impactanalyse op bestaande modellen is verplicht
- Versiebeheer wordt toegepast op alle bouwblokken

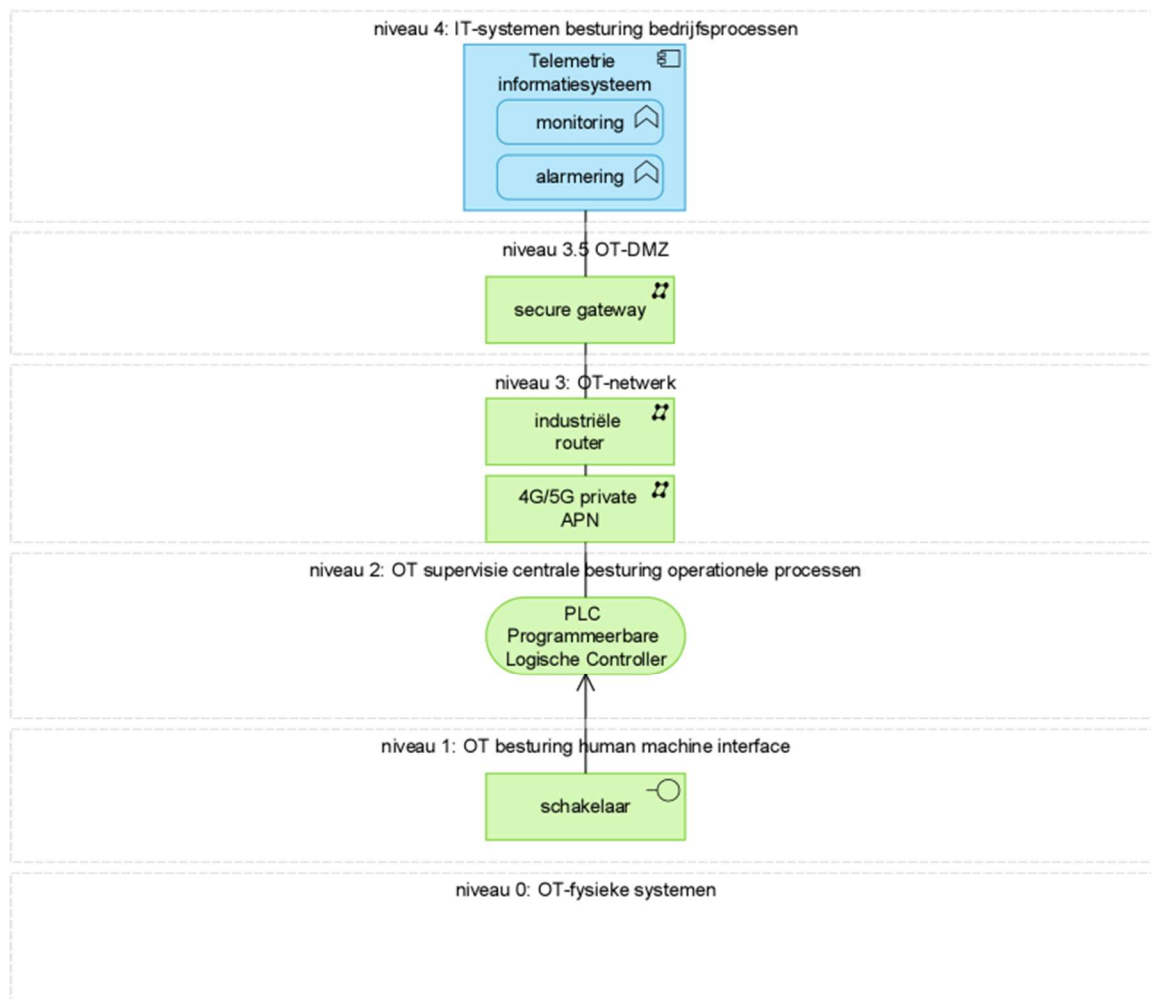
### 3. Kwaliteitscriteria

Een bouwblok wordt alleen opgenomen als het:

- Volledig is gedocumenteerd
- Voldoet aan de Archimate conventies
- Herbruikbaar is
- Security aspecten bevat
- Aansluit op gemeentelijke standaarden

Voor alle patronen zijn de implementatierichtlijnen in het separaat document “non-functionals” van toepassing, bij sommige patronen zijn specifieke “non-functionals” van toepassing.

## 8.1 Gebruik van architectuurblokken



## 9. BIJLAGEN

### Definities

#### a. OT-componenten

##### 1. Sensors

- Functie: Verzamelen van fysieke data uit de omgeving zoals temperatuur, druk of beweging.
- Verbindingen: Sturen data terug naar PLC's via analoge of digitale signalen.

##### 2. PLC's

- Functie: Programmable Logic Controllers die sensordata verwerken en besturingssignalen genereren.
- Verbindingen: Ontvangen data van sensors en sturen besturingscomando's naar SCADA en actuatoren.

##### 3. OT Acces Switches

- Functie: Netwerkswitches die apparaten binnen het OT-netwerk verbinden en dataverkeer beheren.
- Verbindingen: Verbinden sensors, PLC's en andere OT-apparaten met de OT-Core Switch.

##### 4. OT Core Switch

- Functie: Centrale Switch die het OT-netwerk backbone vormt en dataverkeer tussen subnetwerken regelt.
- Verbindingen: Verbindt de Access Switches met OT-firewall en andere netwerkcomponenten.

##### 5. OT Firewall

- Functie: Beveiligt het OT-netwerk door ongeautoriseerd verkeer te blokkeren en toegangscontrole toe te passen.
- Verbindingen: Verbindt het OT-netwerk met de DMZ-firewall via een routed VLAN.

## **6. OT IDS Sensor**

- Functie: Intrusion Detection System Sensor die het OT-netwerk monitord op verdachte activiteiten.
- Verbindingen: Stuurt logs en alerts naar de syslog/event relay voor verdere analyse.

## **7. SCADA**

- Functie: Supervisory Control en Data Acquisition systeem voor realtime monitoring en besturing van industriële processen.
- Verbindingen: Ontvangt data van de PLC's en stuurt informatie door naar Historian en DMZ Event Broker.

## **8. Historian**

- Functie: Opslag en beheer van tijdreeksdata van het OT-netwerk voor analyse en rapportage.
- Verbindingen: Ontvangt data van de SCADA en levert informatie DMZ Event Broker.

## **9. MES**

- Functie: Manufacturing Execution System dat productieprocessen beheert en optimaliseert.
- Verbindingen: Communiceert met DMZ Event Broker via REST/AMQP voor eventverwerking.

### **b. DMZ-componenten**

#### **1. DMZ Firewall**

- Functie: Bewaakt de grens tussen OT- en IT-netwerk door het filteren van verkeer en het afdwingen van toegangsregels.
- Verbindingen: Verbindt het OT-netwerk via de OT-firewall met het IT-netwerk via de IT-firewall en beheert het verkeer naar de DMZ-Switch.

#### **2. DMZ Switch**

- Functie: Netwerkswitch die apparaten binnen de DMZ verbindt en het dataverkeer tussen de DMZ-componenten regelt.
- Verbindingen: Verbindt de DMZ Firewall met de DMZ Server en andere DMZ apparaten.

### **3. DMZ Server**

- Functie: Functie host voor kritieke DMZ-applicaties zoals DMZ Event Broker en Syslog/Event Relay.
- Verbindingen: Verbindt met DMZ-switch en faciliteert communicatie met OT- en IT-componenten.

### **4. DMZ Event Broker**

- Functie: Verwerkt en routeert events tussen OT- en IT-systemen via protocollen zoals MQTT, AMQP en REST.
- Verbindingen: Ontvangt gegevens van Historian en MES en stuurt deze door naar SIEM.

### **5. Syslog/Event Relay**

- Functie: Verzamelt en verzendt loggegevens en events van OT- naar DMZ-componenten naar SIEM.
- Verbindingen: Verbindt met de DMZ-server en stuurt logs door naar SIEM via beveiligde protocollen.

### **6. DMZ IDS (optioneel)**

- Functie: Intrusion Detection System binnen DMZ die verdachte activiteiten detecteerd en rapporteert.
- Verbindingen: Stuurt alerts naar SIEM en SOC-portal voor verdere analyse.

## **c. IT-componenten**

### **1. IT Firewall**

- Functie: Beveiligt het IT-netwerk door ongeautoriseerd verkeer te blokkeren en toegangscontrole toe te passen.
- Verbindingen: Verbindt de DMZ-firewall met de IT-Core Switch en andere IT-componenten.

### **2. IT Core Switch**

- Functie: Centrale Switch die het IT-netwerk backbone vormt en gegevensuitwisseling tussen de netwerken regelt.
- Verbindingen: Verbindt de IT-firewall, SIEM-server-Node, SOC-platform node en andere apparaten.

### **3. SIEM**

- Functie: Security Information and Event Management systeem dat beveiligingslog verzamelt, analyseert en corrigeert.
- Verbindingen: Ontvangt logs van Syslog/Event Relay en DMZ IDS en stuurt alerts naar SOC Portal en ITSM/CMDB.

#### 4. SOC Portal

- Functie: Interface voor Security analisten voor monitoring en incidentenbeheer.
- Verbindingen: Verbindt met SIEM en ITSM/CMDB.

#### 5. ITSM/CMDB

- Functie: IOT Service Management en Configuration Management Database voor het beheren van IT- OT-assets en incidenten.
- Verbindingen: Ontvangt incidentinformatie van SIEM en SOC Poirtal en ondersteund beheerprocessen.

### RACI-tabel – Funtioneel beheer OT-systemen

| Activiteit                           | Functioneel beheer OT | Technisch beheer OT | Systeemeigenaar / Asset Owner | Architectuur | Cybersecurity | Leverancier |
|--------------------------------------|-----------------------|---------------------|-------------------------------|--------------|---------------|-------------|
| Vaststellen functionele eisen        | R                     | C                   | A                             | C            | C             | I           |
| Beheer van gebruikersfunctionaliteit | R                     | C                   | A                             | I            | I             | I           |
| Beoordelen wijzigingsverzoeken       | R                     | C                   | A                             | C            | C             | I           |
| Ontwerpen technische oplossing       | I                     | R                   | C                             | C            | C             | R           |
| Uitvoeren configuratiewijziging      | I                     | R                   | I                             | I            | I             | R           |

|                                                                                                                                                                                                              |   |   |   |   |   |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|
| Architectuurtoets                                                                                                                                                                                            | C | I | I | R | C | I |
| Securitytoets (IEC-62443 / NIS2)                                                                                                                                                                             | R | C | A | I | I | C |
| Testen en acceptatie (functioneel)                                                                                                                                                                           | I | R | A | I | C | C |
| Incident en calamiteitenafhandeling                                                                                                                                                                          | R | R | A | I | C | C |
| Lifecycle- en end-of-life planning                                                                                                                                                                           | R | C | A | C | C | I |
| <p>Legenda:</p> <ul style="list-style-type: none"> <li>● R = Responsible (uitvoerend)</li> <li>● A = Accountable (eindverantwoordelijk)</li> <li>● C = Consulted (adviserend)</li> </ul> <p>I = Informed</p> |   |   |   |   |   |   |

## **OT-sub domeinen binnen de gemeente**

### **1. Verkeersregelininstallaties (VRI's)**

#### **Primaire processen**

- Real-time verkeersafwikkeling
- Prioriteitsverlening (OV, hulpdiensten)
- Detectie van verkeer en voetgangers
- Monitoring van storingen en doorstroming
- Afstemming met regionale verkeerscentrales

### **2. Bruggen & Sluizen**

#### **Primaire processen**

- Openen en sluiten van bruggen
- Schutten van scheepvaart
- Monitoren van waterstanden en objectstatus
- Veiligheidslogica (slagbomen, sensoren, interlocks)
- Afstandsbediening vanuit bediencentrales

### **3. Gemalen & rioolwaterinstallaties**

#### **Primaire processen**

- Afvoer van afval en regenwater
- Pompregeling op basis van niveaus en debieten
- Monitoring van overstorten
- Alarmmeldingen bij storingen of wateroverlast
- Ondersteuning van klimaatadaptatie (piekbelasting)

### **4. Openbare verlichting (OVL)**

#### **Primaire processen**

- 5. Schakelen en dimmen van lichtmasten
- 6. Energiebeheer
- 7. Detectie van storingen
- 8. Slimme verlichting (bewegingsdetectie, adaptief licht)

### **5. Tunnels**

#### **Primaire processen**

- Ventilatie, verlichting, pompen
- Veiligheidsinstallaties (branddetectie, CCTV, intercom)
- Verkeersafwikkeling en afsluitingen
- Monitoring van luchtkwaliteit en temperatuur
- Integratie met verkeerscentrales

### **6. Waterbeheer& Peilbeheer**

#### **Primaire processen** *(vaak in samenwerking met waterschappen)*

- Sturing van waterpeilen
- Monitoring van waterstanden, debieten en kwaliteit

- Bediening van stuwen, kleppen en gemalen
- Overstroompreventie

## **7. Gebouw gebonden installaties (GBI)**

### **Primaire processen**

- Klimaatregeling (HVAC)
- Toegangscontrole
- Brandmeldinstallaties
- Energiebeheer
- Liftbesturing

## **8. Openbare ruimte sensoriek (Smart City)**

### **Primaire processen**

- Geluidsmetingen
- Luchtkwaliteit
- Slimme afvalbakken
- Parkeer- en mobiliteitscensoren

## **9. CCTV & Toezichtsystemen**

### **Primaire processen**

- Cameratoezicht in openbare ruimte
- Real-time monitoring
- Incidentdetectie
- Integratie met meldkamers

## **10. Laadinfrastructuur (EV-charging)**

### **Primaire processen**

- Energieverdeling en laadsturing
- Monitoring van laadpalen
- Slimme netsturing (load balancing)
- Afhandeling van transacties

## **11. Energie en Warmtenetten (indien gemeentelijk)**

### **Primaire processen**

- Warmteproductie en distributie
- Monitoring van druk, temperatuur en debiet
- Sturing van onderstations
- Storingsdetectie

## Risico- en gevolgenanalyse van OT-assets binnen een gemeente

### PLC's, RTU's en veldcontrollers

#### Risico's

- Ongeautoriseerde toegang of manipulatie
- Firmware kwetsbaarheden
- Verouderde protocollen (Modbus, DNP3, propriëtair)
- Geenlogging of monitoring

#### Gevolgen

- Onjuiste aansturing van bruggen, gemalen, VRI's
- Fysieke schade aan objecten
- Veiligheidsincidenten
- Stilstand van kritieke processen

#### PLC

#### Risico's

- Ongeautoriseerde toegang of manipulatie
- Fysieke schade aan objecten
- Veiligheidsincidenten (verkeer, water, openbare ruimte)

#### Gevolgen

On

#### Risico's

- Ongeautoriseerde toegang of manipulatie
- 

#### Gevolgen

On

#### Risico's

- Ongeautoriseerde toegang of manipulatie
- 

#### Gevolgen

On

#### Risico's

- Ongeautoriseerde toegang of manipulatie
-

**Gevolgen**  
On

**Risico's**

- Ongeautoriseerde toegang of manipulatie
- 

**Gevolgen**  
On

**Risico's**

- Ongeautoriseerde toegang of manipulatie
- 

**Gevolgen**  
On

**Risico's**

- Ongeautoriseerde toegang of manipulatie
- 

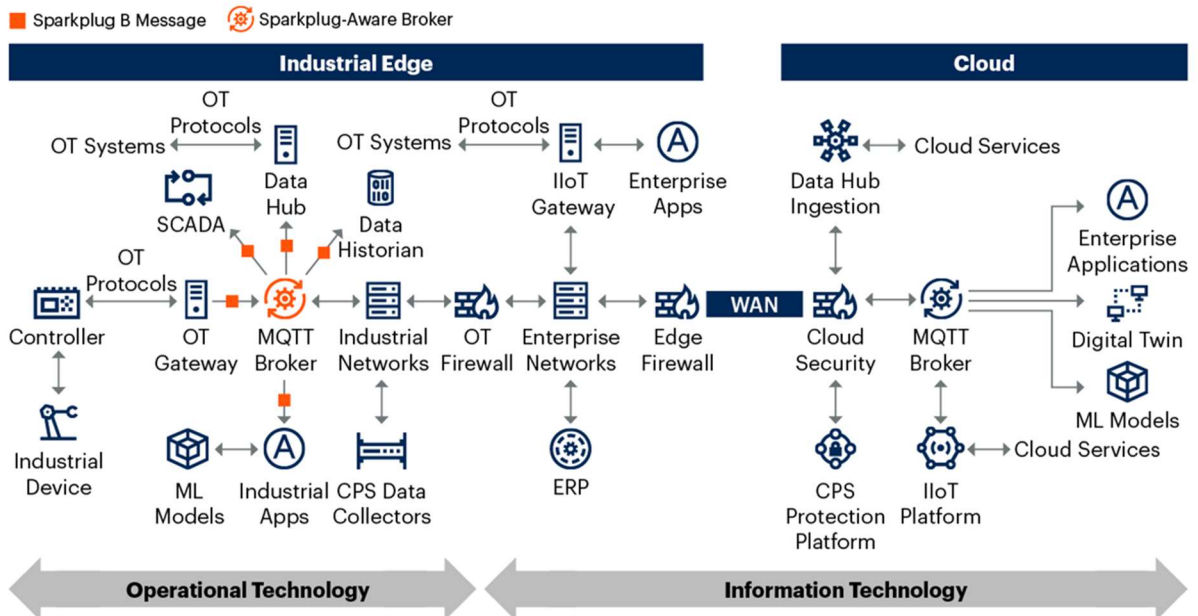
**Gevolgen**  
On

**Risico's**

- Ongeautoriseerde toegang of manipulatie
- 

**Gevolgen**  
On

## IT-OT Reference Architecture



Source: Gartner

CPS = Cyber-Physical System; ERP = Enterprise Resource Planning; HMI = Human-Machine Interface; IIoT = Industrial Internet Of Things; MQTT = MQ Telemetry Transport; MES = Manufacturing Execution System; ML = Machine Learning; OPC UA = Open Platform Communication Unified Architecture; OT = Operational Technology; SCADA = Supervisory Control and Data Acquisition; WAN = Wide-Area Network

792965\_C

**Gartner**

