



IACS & CYBERSECURITY CONFERENCE



April 15th 2025 • Amersfoort • The Netherlands



Cyber resilience through engineer focused training



Co-funded by
the European Union

Dutch Authority for Digital
Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security

IACS Coalition



Wie ben ik?



Sebastiaan Schuemie

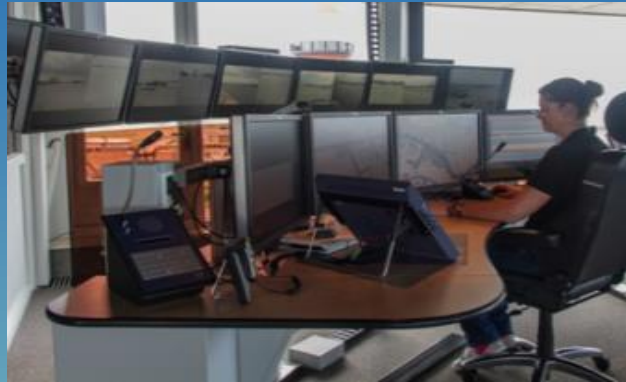
Senior Adviseur Cybersecurity / Project lead ATHENA
@Rijkswaterstaat

Achtergrond:

- Security Architect Wegverkeersmanagement & Smart Mobility
- Information Security Manager / Projectmanager IT & Water
- BSc Information & Communication Technology
- MSc Business Administration
- CISSP / GICSP / ISFS (ISO27001) / TOGAF



Wie is Rijkswaterstaat?



Dutch Authority for Digital
Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security

IACS Coalition



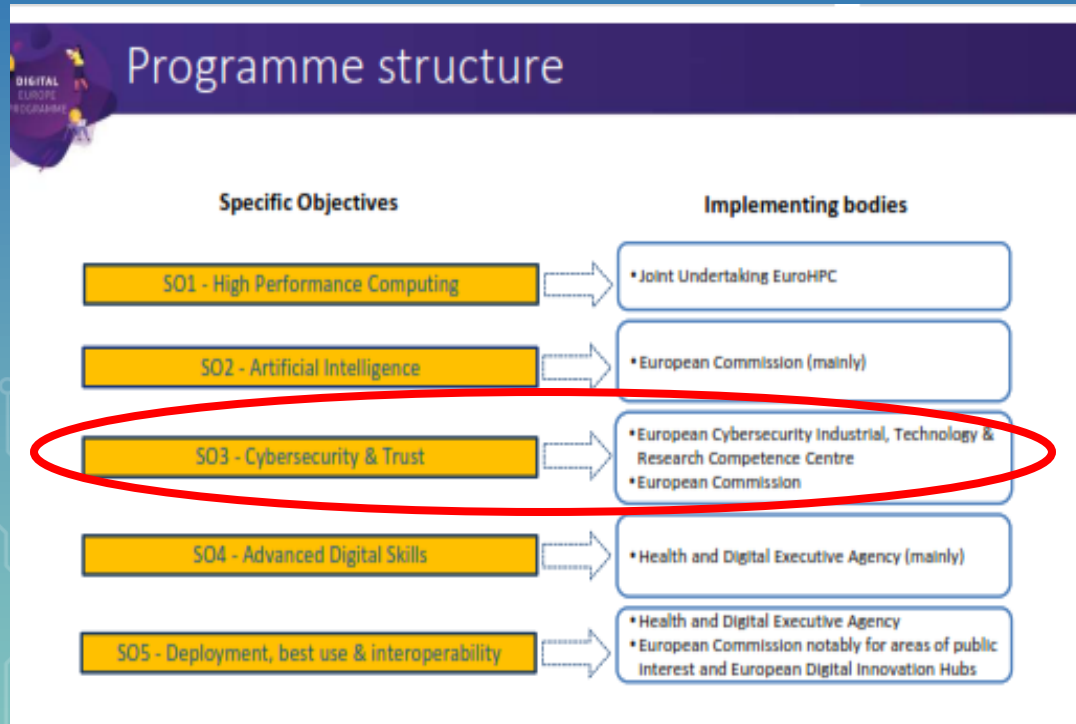
Vitaal!

Keren en Beheren waterkwantiteit en **Transport** zijn de twee sectoren waar o.a. RWS een verantwoordelijkheid in heeft. Verstoring van deze processen kan direct leiden tot maatschappelijke ontwrichting, economische schade, imagoschade of verlies van levens. Hierdoor is het risicoprofiel van de maatschappelijke vitale processen van RWS hoog en vraagt om passende cybersecurity weerbaarheid.

Industriële Automatisering (IA/PA/OT) speelt een cruciale rol in het functioneren van de objecten die zorgen voor de uitvoer van deze processen.



Digital Europe Programme



01-01-2021 t/m 31-12-2027

Het programma Digitaal Europe heeft als doel: Om digitale technologieën breed beschikbaar te maken voor bedrijven, burgers en overheidsdiensten.

Het richt zich op belangrijke gebieden zoals kunstmatige intelligentie, cyberbeveiliging en geavanceerde digitale vaardigheden.

Daarnaast ondersteunt het de digitale transformatie van de Europese samenleving en economie, met een focus op duurzaamheid en veiligheid





Waarom ATHENA?



Cybersecurity training / bewustwording is voornamelijk IT gericht

Digitalisering is een kans met toenemend (nieuwe) risico

- Supply chain-aanvallen & Remote access
- (Spear) Phishing & Social engineering
- Ontevreden werknemer
- Beschikbaarheid van OT

De impact van een cyberaanval in OT (kritische infrastructuur) kan grote gevolgen hebben voor de samenleving

De EU-verordening (NIS2) stelt vereisten voor het opbouwen en onderhouden van cybersecurity kennis

De ambitie van ATHENA

Kritieke infrastructuur in de watersector beter beschermd en weerbaar tegen cyberdreigingen

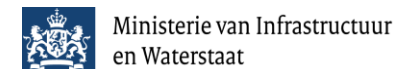


- Ontwikkeling van **innovatieve trainingsmodules** voor OT
- Ontwikkeling van een **uniforme OT cyber risicotraining** op Europees niveau
- Ontwikkeling van **risicobewustzijn EN handelingsperspectief**
- Training op basis van **wetenschappelijke methoden en principes**
- Aantrekkelijk door gebruik van **aansprekende oplossingen** (o.a. VR, Gamification)

ATHENA is a Digital Europe Project, co-funded by the European Union.



Advisory board members



The project funded under Grant Agreement No. 101127970 is supported by the European Cybersecurity Competence Centre.





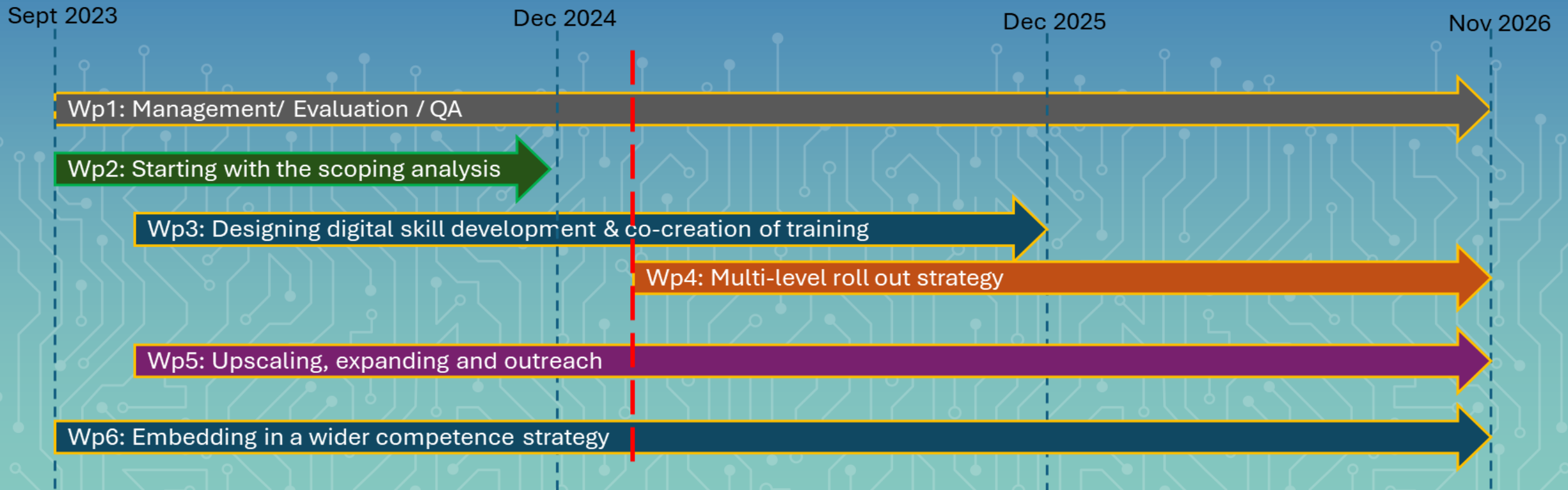
ATHENA budget & tijdslijnen

Tijdslijnen:

- Project start: September 2023
- Project einde: November 2026

Budget:

Totaal 39 maanden (3 jaar, 3 maanden)
Totaal project budget: € 3.042.193





Scope analyse

- OT-operator en OT-leiderschap in de water sector (water infra, drinkwater- en afvalwater)
- Bewustwording / risico-inventarisatie & Incident response
- Preventie, Detectie & Mitigatie

Wetenschappelijke onderbouwing:

- We onderzoeken het werkveld van de operators
- We creëren een leerplatform en leerpaden op basis van OT-rollen



Wetenschappelijk - Human factor!

- Er is behoefte aan een **holistische benadering** en **co-creatie van cybersecuritytrainingen en -onderwijs in OT**
- Focus op het **opbouwen van de vaardigheden, kennis en zelfredzaamheid van individuen**, zodat ze zich gesterkt voelen om cybersecuritybedreigingen te herkennen en er op de juiste manier op te reageren.
- Daarnaast is er ook behoefte bij organisaties om een **positieve cybersecuritycultuur** op te bouwen die zich richten op weerbaarheid, in plaats van schuld, bij het omgaan met cyberdreigingen, aangezien dit een collectieve verantwoordelijkheid is van iedereen.

39% of cybersecurity risks involve human factors

95% of successful breaches are due to human error (Alsharif et al., 2022)





Human factor!

Zelfredzaamheid:

- Door training en ervaring
 - Kijken naar competenties
- Moet worden versterkt door leiderschap en cultuur
 - Samenwerken & communicatie

Zodat:

- Er wordt gehandeld wanneer je iets opmerkt in plaats van 'alleen' denken
- Niet verstoppen: 'Dit is niet mijn verantwoordelijkheid'
- Iemand anders weet het beter, en zal het opmerken als er iets mis is





Versterken competenties

Risk awareness track

Preventie

E-learning – Risico bewustzijn
(o.a. access management, social engineering,..)

Preventie

Risico inventarisatie in een bedieningsruimte (VR)
(o.a. insider threat, risico management)

Incident response track

Detectie

Compromitteren van data integriteit in een bedieningsruimte (VR)

Mitigatie

Compromitteren van SCADA (VR / table top)
Cyber kill chain

Mitigatie

Supply chain attack (VR / table top)
Cybercrisis - communicatie



Vooruit kijken

- We werken naar direct toepasbare cybersecurity training
- Organiseren pilottraining voor de watersector EU breed
- Feedback & ervaringen om de training te verbeteren
- We nemen ook Webinars op



Disseminatie & betrokkenheid van de watersector in de EU

- Rijkswaterstaat (NL), Waterschappen - Waterschapshuis (NL), Vlaamse Waterweg (BE), Epal (PRT), Tallinn Vesi (EST), Eau de Paris (Fr), SUEZ (Fr)

Ook interessant voor andere OT-sectoren (o.a. energie, nucleair, maritiem):

- Presentaties op conferenties in NL en elders in de EU
- Verbinden met andere EU projecten
- Verbinden met andere (nationale) initiatieven
- Lessons learned overdragen d.m.v. White papers, wetenschappelijke publicaties, enz.

Wetenschappelijk onderzoek en experimenten

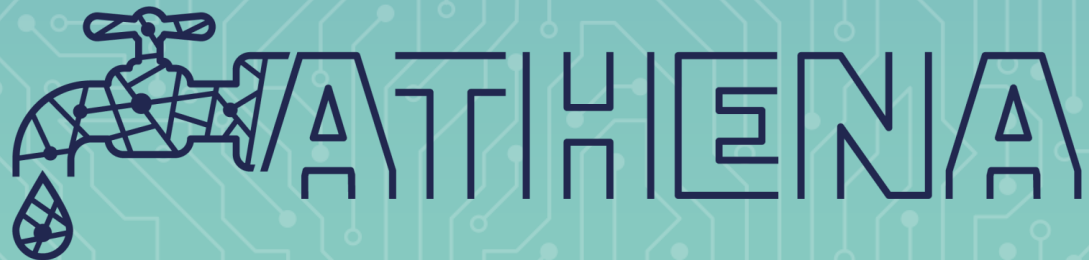
- Onderzoek naar de behoefte van en manier waarmee OT cybersecurity training wordt toegepast
 - Gebruik van VR / Digital Twin als trainingsmethode
 - Effect van Capture the Flag als vorm van cybersecurity training
 - Invloed van een Virtual assistant in cybersecurity training
- Presentaties op conferenties (o.a. HCI 2024, HCI 2025, Educon 2025)





Dank voor je aandacht

Volg ons op LinkedIn:



ATHENA is a Digital Europe Project, co-funded by the European Union.



Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat



Østfold University College



het Waterschapshuis



Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University



Water Security Management
Assessment Research and Technology

LUXEMBOURG
INSTITUTE OF SCIENCE
AND TECHNOLOGY



The project funded under Grant Agreement No. 101127970 is supported by the European Cybersecurity Competence Centre.



Co-funded by
the European Union



ECCE
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE