Cybersecurity in water critical infrastructure

WEBINAR 6

WELCOME!

Also on behalf of JRC and the speakers of today:

Christos Makropoulos, NTUA, Professor

Juan Caubet, EURECAT, Director of IT&OT Security Unit

Gustavo Gonzalez-Granadillo, ATOS, Cybersecurity r&d engineer

Dora Karali, RISA Sicherheitsanalysen, Business Development and r&d manager

Michel Bosco, RHEA Group, Strategic Advisor

Václav Jirovský, UNI PRAGUE, Professor

WHY A WEBINAR ON CYBERSECURITY?

Fig. credits to Rui Teixeira

- **Relevance to the Water Security Plan**:

Although beyond the scope of the Water Security Plan, the guidance (RIGHTLY) highlights the relevance of increasing resilience of water critical infrastructure against cyber attacks which can be the vector to intentional water contamination!

- **The need**:

Even if many utilities have invested resources in cybersecurity, more progress is necessary to secure water infrastructure at strategic, tactical and operational level.

- **The aim of the webinar**:

To raise **awareness** about the water critical infrastructure needs for protection against cyber threats by presenting the solutions results of international research projects and investigating the social changes impact on cyber security.

STOP-IT

The program for today!

1. Cyber security importance in the water sector and the contribution of the STOP-IT project (Rita Ugarelli, 10 min)
2. Physical and Cyber security integration and modelling at strategic and tactical level (Christos Makropoulos, 20 min)
3. Applying Machine Learning algorithms to build anomaly-based cyber and physical detection systems (Juan Caubet, 15 min)
4. Cyber-physical solutions for real-time detection at operational level (Gustavo Gonzalez-Granadillo, 15 min)
5. Empowering informed decision making with an overarching solution for the security of water critical infrastructures (Dora Karali, 15 min)
6. Water supply & cybersecurity (Michel Bosco, 10 min)
7. Social changes impact of cyber security (Václav Jirovský, 15 min)

- Questions and Answers and closing remarks (10 min)
- Formal closure of the webinar series (JRC)-5 min

Cyber security importance in the water sector and the contribution of the STOP-IT project

STOP-IT

stop-it-project.eu

Project funded by the European Union's programme Horizon 2020 under the call **CIP-2016-2017-1** "Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe".

Rita Ugarelli (PhD), SINTEF AS
Chief Scientist
Project Coordinator

Rita.Ugarelli@sintef.no

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.740610.
The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

INDEX

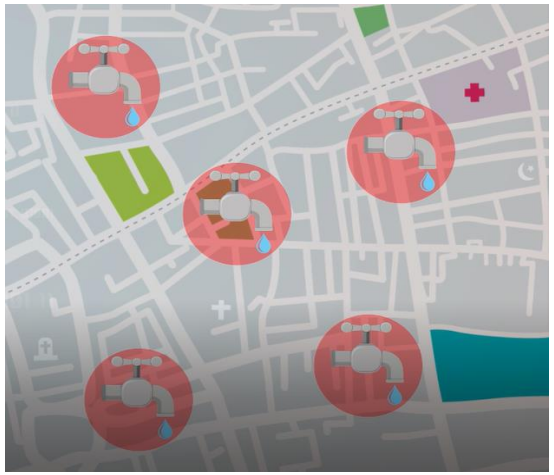
- Why do we need STOP-IT?
- Objectives of STOP-IT and Consortium
- Examples of technological and non outcomes
- Join us!

Background

Water networks are vital for life

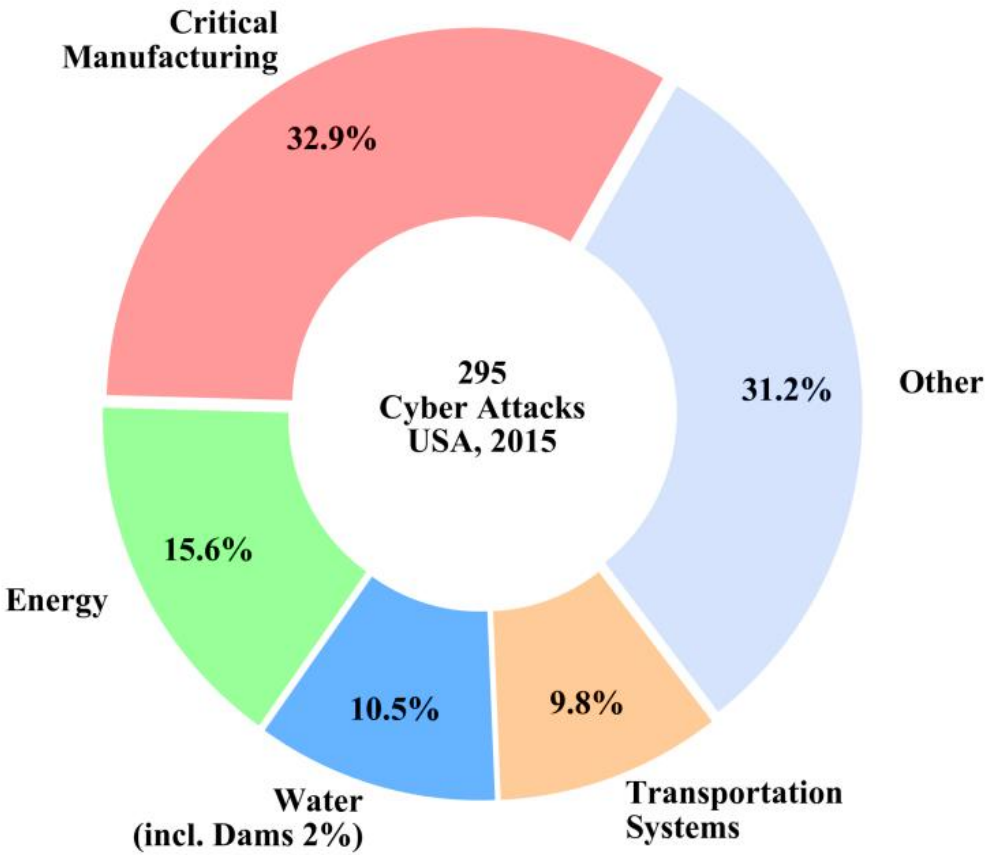
The use of digital technologies means new opportunities, but also new risks.

Cyberattacks on water utilities can have impacts on public health; not only in the delivery of clean, potable water to consumers but to other critical services that depend on the continuous delivery of water.



AND THE ATTACKERS INTEREST IN WATER SECTOR IS GROWING….

- Already a prominent target (**3rd most targeted**).
- Many cybersecurity incidents go either **undetected and unreported**, or undisclosed. (reputation+ customers trust)
- **Cyber security** is of course already part of the agenda for water companies.
- **Physical security** has been part of the agenda for some time.
- **Anything else?**



Cyber attack incidents in USA, 2015 (DHS, 2016)

STOP-IT will:

Make water critical infrastructure secure and resilient by improving preparedness, awareness and response level to physical, cyber threats, and their combination, while taking into account systemic issues, as well as cascading effects.

STOP-IT solutions will help water utilities operators to prioritize risks and develop a realistic approach and plan for enhancing physical and cyber protection.

Project duration: 2017-2021

STOP-IT SPECIFIC OBJECTIVES & Progress

Raise AWARENESS and COOPERATION in the water sector

Enhance external impact

Enhance ability to IDENTIFY and DETECT

STOP-IT

Enhance ability to COMPLY

Enhance ability to ANALYSE

Ensure wide applicability of security solutions

Enhance ability to PREVENT, TREAT or RESPOND

- Ready for demonstration and feedback
- Work in progress
- Running along the entire project duration

Who are we?

STOP-IT involves 23 partners from across Europe and Israel

7 research centres

SINTEF

IWW
IWW Zentrum Wasser

KWR
Watercycle Research Institute

CETAQUA

eurecat
Centre Tecnològic de Catalunya

TECHNION
Israel Institute of Technology

ΕΠΙΣΕΥ
ICCS

7 Industry / SME sector

Atos

oylo
Trust Engineering

PNO

WORLD SENSING

RiSA
Sicherheitsanalysen GmbH

mnemonic
- securing your business

1 Technology Platform

Water Europe
Technology & Innovation

4 Front Runner Water Utilities

MEKOROT

Oslo

Aigües de Barcelona

Berliner Wasserbetriebe

4 Followers Water Utilities

hessenwasser

CITY OF BERGEN

emasagra

De Watergroep
WATER. VANDAAG EN MORGEN.

STOP-IT: TOOLS AND TECHNOLOGIES (1/5)

Modular components of
the STOP-IT risk management platform

Strategic & Tactical

Operational

Solutions that support:

- **Strategic/tactical planning and post action assessment**
- **Operational decision making**

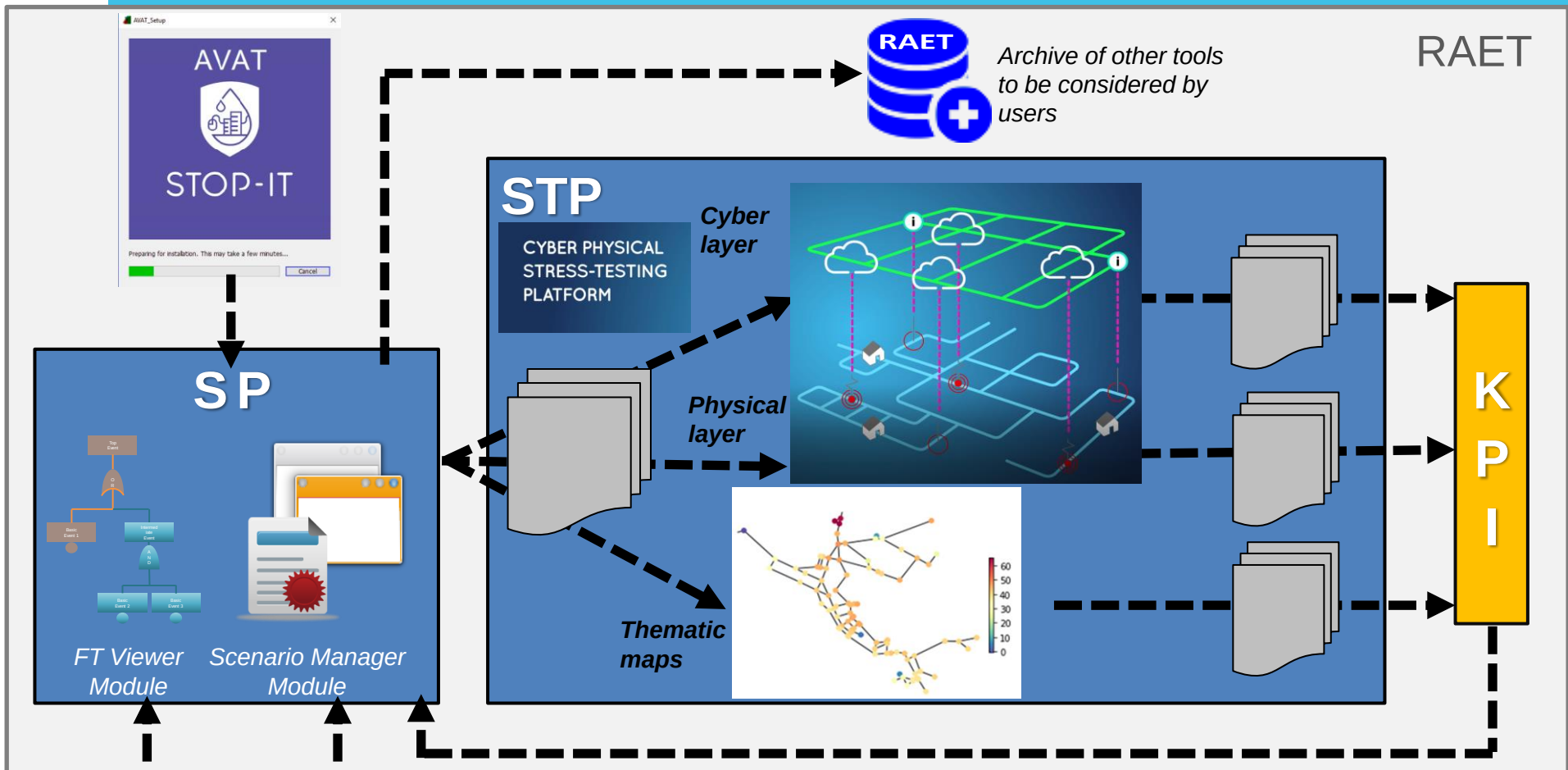
towards cyber-physical security of water infrastructures

Scalable **Adaptable** **Flexible**

STOP-IT modules:

- ❑ Module1: Risk Assessment and Treatment Framework
- ❑ Module 2: Secure wireless sensor communications module
- ❑ Module 3: Toolbox of technologies for securing IT and SCADA
- ❑ Module 4:Toolbox of technologies for protecting against physical threats in CI
- ❑ Module 5: Cyber Threat Incident Service
- ❑ Module 6: Real-Time anomaly detection system
- ❑ Module 7: Public Warning System-Secure Information Exchange Technologies
- ❑ Module 8:Reasoning Engine
- ❑ Module 9: Enhanced Visualisation Interface for the water utilities

STOP-IT: TOOLS AND TECHNOLOGIES (3/5)
Conceptual diagram of Module I



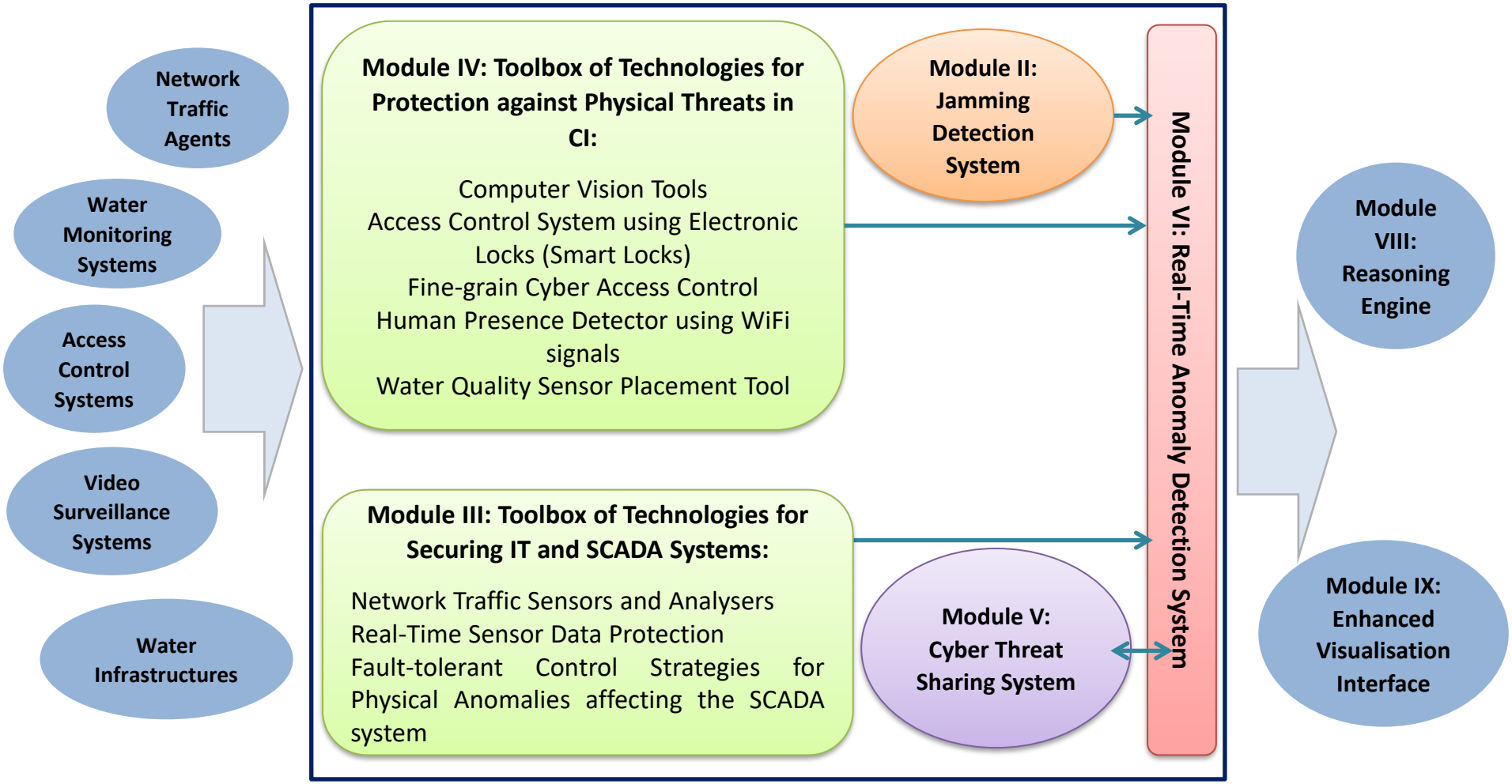
High level use-cases of Module I components:

1. **Assess vulnerability**
2. **Navigate through potential risks & design/configure** multiple **risks scenarios**
3. **Simulate physical** system interacting with their **cyber layer**
4. **Visualise system's response and quantify/assess** overall **impacts**
5. **Assess scenarios' of measure(s) implementation** to the system

Detailed information on Module I will be provided by Christos Makropoulos …!

STOP-IT: TOOLS AND TECHNOLOGIES (4/5)

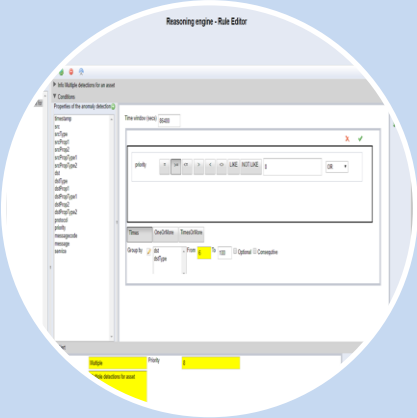
Operational solutions and technologies for cyber & physical protection



Detailed information on anomaly detection will be provided by Juan Caubet and Gustavo Gonzalez-Granadillo!

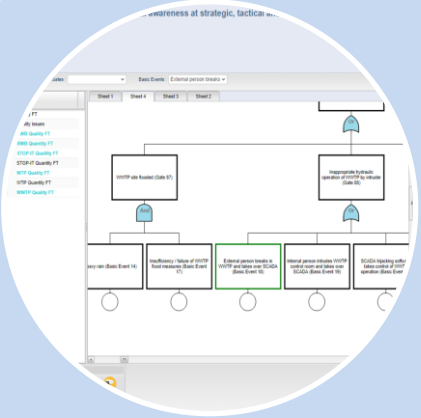
STOP-IT: TOOLS AND TECHNOLOGIES (5/5)

STOP-IT Integrated platform

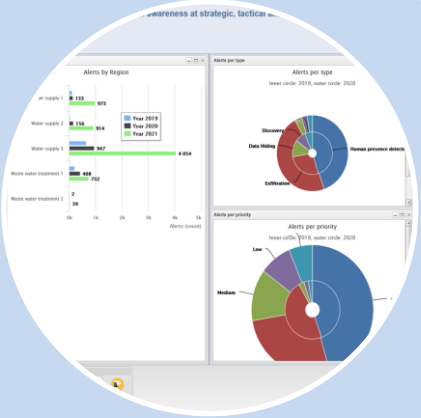


Alert generation based on configurable rules

Mitigation action proposition



Risk assessment



History view for gathering metrics

Operational – Tactical - Strategic

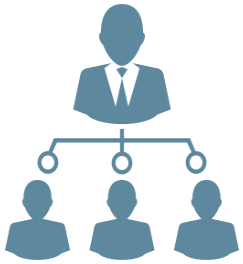
The STOP-IT platform embraces the various STOP-IT solutions, facilitates their communication and provides access to the web-accessible tools of the toolbox through the Enhanced Visualization Interface.

The STOP-IT platform will be validated in a simulated operational environment and demonstrated in the four FR demo sites.

Detailed information on anomaly detection will be provided by Dora Karali!

STOP-IT: CUSTOMIZED TRAINING MATERIAL (1/2)
…FOR DIFFERENT End-user profiles

- Profile 1: **Decision makers**
  - **Board members** of the utility & relevant **top-managers**
  - People with **various background** and **expertise**
  - Training activities geared towards **awareness raising**




- Profile 2: **Risk management officers**
  (and modellers that support them)
  - **Risk managers/officers** at different levels, performance and quality managers incl. personnel for modelling activities
  - Training activities seeking to **enhance risk management processes** of a utility by utilizing STOP-IT solutions


- Profile 3: **Staff responsible for real time operations**
  - **Operators, maintenance managers** and staff responsible for real time operations e.g. SCADA room operators
  - Course goal is to train on i**nstallation/operation/use of technologies** and solutions targeting at the operational level of risk management


Our Trans-Project communities of practice (CoP's)

STOP-IT has created CoPs and learning alliances with a multi-stakeholder perspective to contribute to the development of the project products.

The trans-project CoP is crossing boundaries between different critical infrastructure sectors and involves international networks and non-project expert groups.

Collaborations have been already established with relevant communities:
the ICT4Water cluster (www.ict4water.eu/) , the "Community of Users on Secure, Safe and Resilient Societies" (CoU) (www.securityresearch-cou.eu/about), the JRC ERNCIP TG Water (https://erncip-project.jrc.ec.europa.eu/networks/tgs/water), ECSI - the European Cluster for Securing Critical Infrastructures (https://www.finsec-project.eu/#comp-k38hag4h) – contacts with ENISA and ECSO in progress

... Possibly more opportunity after today! ….

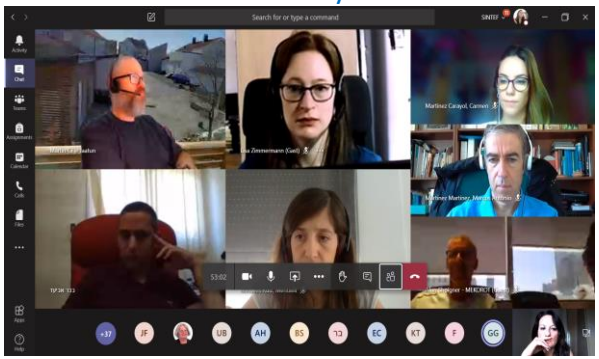
Interested? Contact the STOP-IT Team!

https://stop-it-project.eu/

General Assembly 2017

General Assembly 2018

General Assembly 2019



General Assembly 2020

STOP-IT

THANK YOU FOR YOUR ATTENTION

stop-it-project.eu

Project Twitter: https://twitter.com/STOPIT_Project

Rita Ugarelli – STOP-IT Project Coordinator

Contact:
e-mail: rita.ugarelli@sintef.no
Mobile: +47 454 29 787
Skype: Rita24204
Linkedin: ritaugarelli

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.740610.
The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.