The European research project STOP-IT brings together a group of water utiltities, water engineers, computer scientists and researchers. Together they develop solutions for safe water infrastructures, addressing different risks and threats.

Visit the STOP-IT website and take a look at our strategic, tactical, operational and real-time solutions and tools: stop-it-project.eu

Water utilities need to be prepared!

Our Communities of Practice

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

Join us:

https://stop-it-project.eu/about-stop-it/community-of-practice/

Project Partners

SINTEF · IWW Water Centre · CETAQUA Water Technology Centre · KWR · Aigües de Barcelona · emasagra · World Sensing · Berliner Wasserbetriebe · maemonic – securing your business · Aplicatzia · hessenwasser · eurecat · Water Europe – Technology & Innovation · MEKOROT · Technion Israel Institute of Technology · RISA Sicherheitsanalysen GmbH · Bergen Kommune · De Watergroep · PNO – Connecting Ambitions · Atos · ovio – Smart Engineering · Oslo

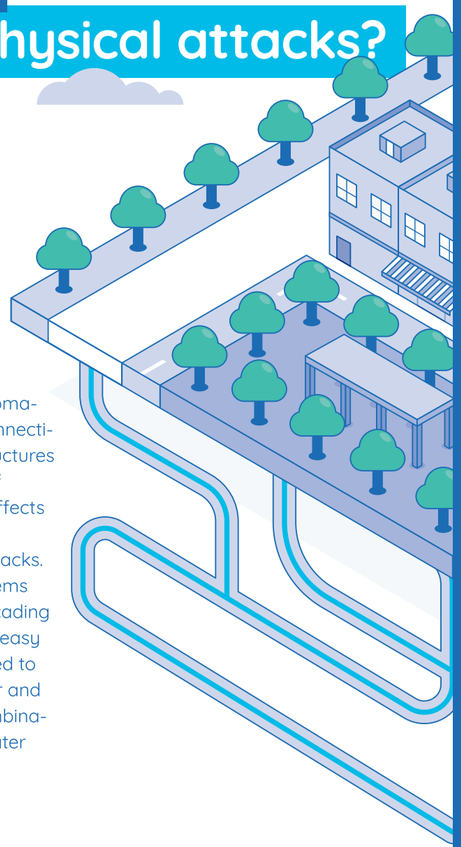
STOP-IT

Secure your water infrastructures against cyber-physical attacks and threats with STOP-IT

stop-it-project.eu

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.

Are your water infrastructures safe from cyber-physical attacks?



Digital solutions bring several benefits to the water sector, but also make the attack surface wider.

The increasing dependency of physical infrastructure on automation and the emerging interconnectivity of cyber-physical infrastructures come with an increased risk of technical failures, cascading effects and vulnerability to malicious actions and cyber-physical attacks. Since cyber and physical systems interact continuously and cascading effects between them are not easy to track, there is an urgent need to combine and implement cyber and physical solutions – and a combination thereof - to make your water utility safe again.

The threats and risks you can handle with STOP-IT solutions and tools

From system failures and human errors, over malicious actions, to cascading effects of interdependent critical infrastructures.

Can you quickly alert operators and citizens if a threat arises?

Are you able to detect attacks and malicious events against your infrastructure in real time?

How would the hydraulic behaviour of a water distribution network change if sensors/actuators are affected by a SCADA DoS attack?

Do you use smart locks that provide the ability to arm and disarm the security systems on the site on demand?

Are you prepared to deal with zero-days vulnerabilities and attacks? Do you include artificial intelligence and machine learning approaches in your security mechanisms?

What would be the impact on a utility's reputation or, even worse, to citizens' health if someone succeeds in manipulating water quality sensors by "blinding" them, making contaminants injected into the water going undetected by system operators?

Is your infrastructure ready to correlate, analyse and manage cyber and physical security data?

Is your SCADA infrastructure protected from unauthorized reading of your confidential data?

Are you able to detect unusual or unauthorized behaviour around your sites by using intelligent cameras?

Can you deal with cascading effects to other parts or infrastructure of the network and prevent escalation from a single unit failure to a system collapse?