STOP-IT

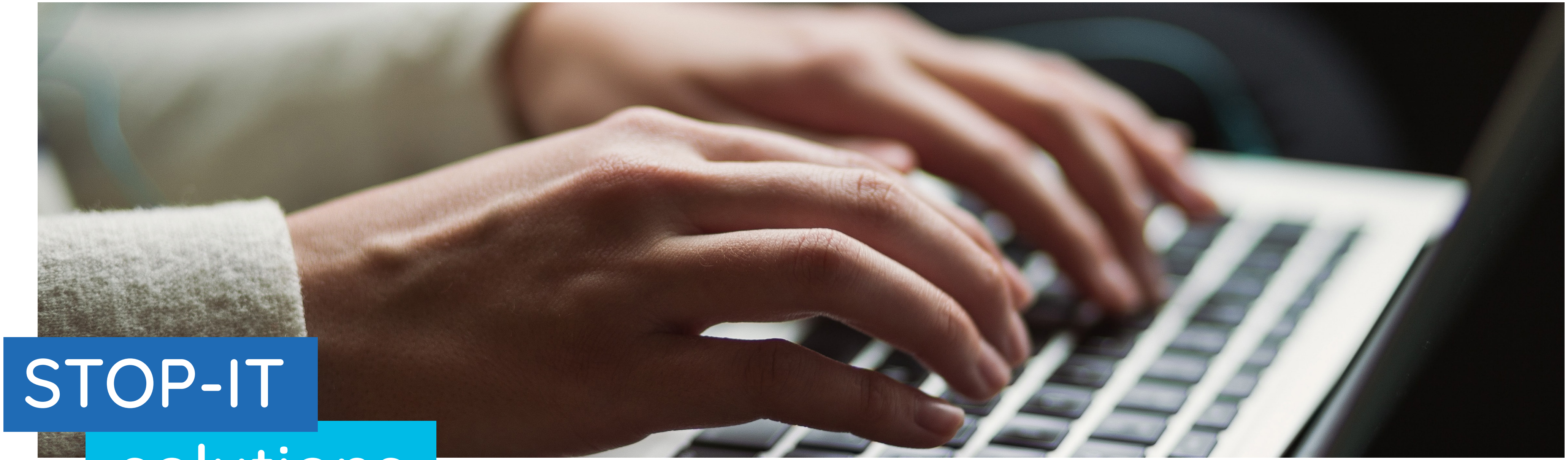
MAY 2020
ISSUE 3

STOP-IT Magazine
stop-it-project.eu

WORKING TOGETHER FOR A SAFER FUTURE

Strategic, tactical and operational protection of water infrastructure against cyber-physical threats

STOP-IT



STOP-IT solutions

Cyber and physical protection in critical water infrastructures at operational level.

Cyberattacks are an increasing threat in our world. They are especially dangerous for critical infrastructures and therefore also for the water sector. In order to enable water utilities to face the growing challenges, the STOP-IT project has developed technologies and scientific/technological initiatives to provide innovative solutions to risk treatment for Critical Infrastructures (CI) at operational, strategic and tactical level in the water sector. Two toolboxes of technologies have been developed for this purpose and are available on the STOP-IT website.

TOOLBOX OF TECHNOLOGIES FOR SECURING IT AND SCADA:

Aiming at monitoring and protecting SCADA and IT systems integrity, both against intentional attacks and malfunctions. The toolbox includes real-time Fault Tolerant Control Strategies (FTCS), enabling reconfiguration mechanisms to minimize the impact and ensuring the CI availability; a Network Traffic Sensor and Analyzer tool (NTSA), to detect anomalous behavior in the network traffic; and a Real-time Sensor Data Protection (RSDP) tool using blockchain schemes to protect the integrity of the data generated during CI operations (logs, sensor data, etc.).

TOOLBOX OF TECHNOLOGIES FOR PROTECTION AGAINST PHYSICAL THREATS IN CI:

Including Computer Vision tools (CVT) for automated surveying of the large-area of the water utility; a Fine-grained Cyber Access Control (FCAC) that employs user specified policies to determine who can access which resources and for what purpose; a Human Presence Detector (HPD) tool using WiFi signals reflection in human body to detect the presence of persons in restricted areas; a Water Quality Sensor Placement (WQSP) tool for the early detection and impact minimization of contamination events; and an access control system based on intelligent electronic locks (Smart-Locks) and dedicated applications to service employees and to central management system.

In addition to these two toolboxes, a Jammer Detector, and a Cyber Threat Sharing Service are developed to converge information to the Real-Time Anomaly Detection system

(as seen in Figure 1 on the next page).

The Jammer Detector informs about wireless channel activities affecting regular network communications and provides an innovative method to locate the identified threats geographically, so that corrective actions can be implemented to face the security threats.

The Cyber Threat Sharing System collects sources of existing threats from relevant feeds and structures the information using standards to facilitate the exchange of the security threats identified (e.g., MITRE, OASIS). This service ensures the mitigation of threats to CI; enhances the coordination within CI establishing exchange methods to prevent, reduce, mitigate and recover from existing threats; and allows the coordination between similar centers in the world to deal with CI threats in a global approach.

The real-time anomaly detection system is composed of two main tools: a Cross-Layer Security Information and Event Management (XL-SIEM), and a Real-Time Anomaly Detector (RTAD) that uses a combination of cyber, physical, behavioral and surrounding contextual information to detect anomalies in the critical infrastructure. All these components are necessary for the water consumers to detect threats in water utilities. The main outputs of these components are messages to alert about imminent threats to increase the security feeling of the citizens. Different layers of threat detection are foreseen through the exploitation of different components, each of them is useful for detecting a certain threat under a specific condition.

By using these solutions, water critical infrastructures can detect in real time (or near real time) malicious incidents against IT applications (e.g. brute-force attacks, SQL injections, cross-site scripting, privilege scalation, policy violations, etc.), as well as incidents against the network systems (e.g. denial of service attacks, buffer overflow, network scanning, man-in-the-middle attacks, abnormal network traffic behavior, etc.) and incidents against operational technology equipment (e.g. jamming signals, abnormal human presence in physical units, unauthorized database access, unauthorized read or write request to a SCADA device, etc.). As a result, the developed solutions help security administrators and C-level managers in the decision-making process of defining the most appropriate strategy to mitigate the negative effects of the detected events. Water critical infrastructures are therefore able to protect themselves against a myriad of cyber and physical malicious incidents at operational level.

Our public tools and solutions can be found on our website: https://stop-it-project.eu/

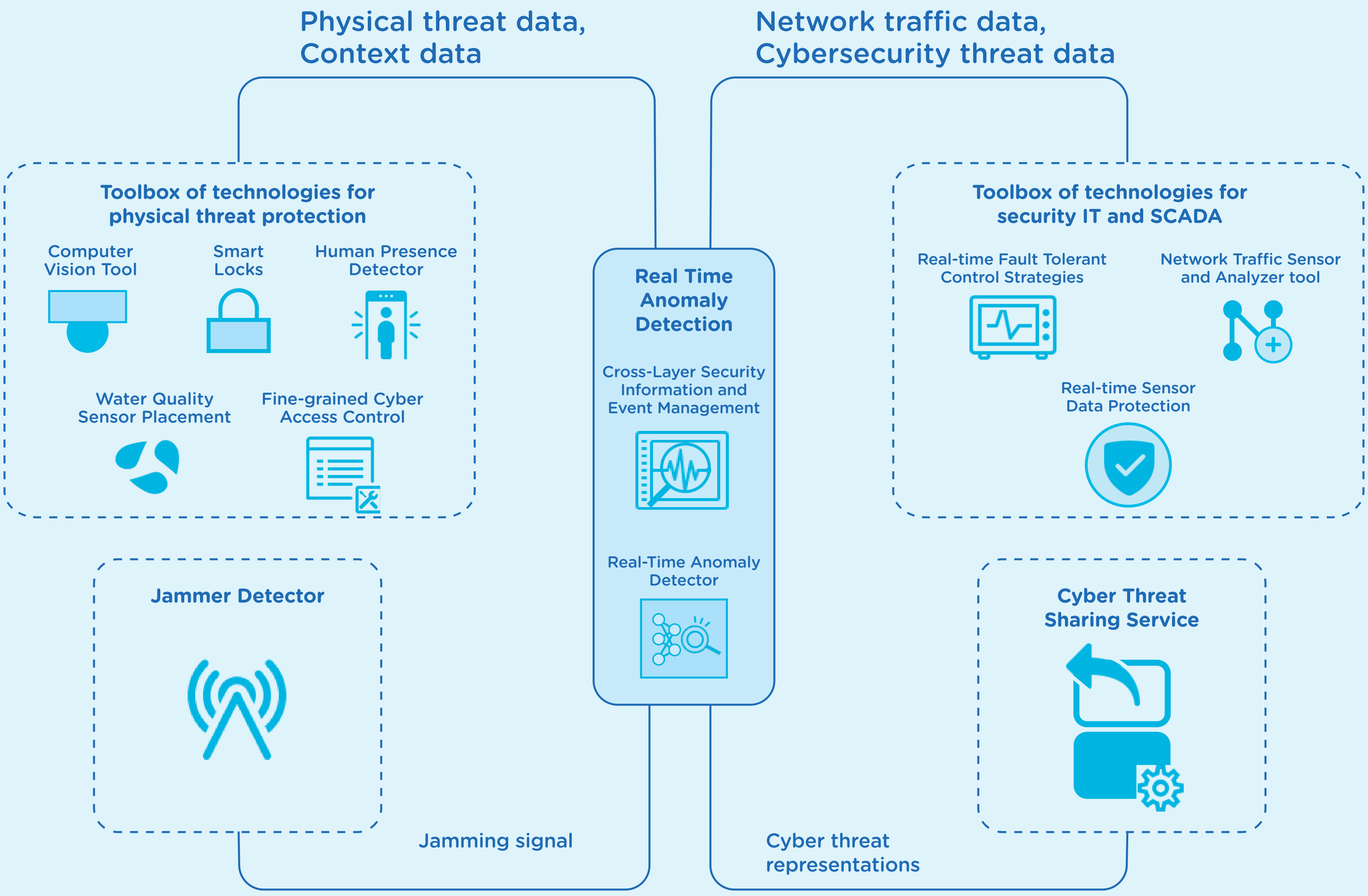

Physical threat data,
Context data
Network traffic data,
Cybersecurity threat data
Toolbox of technologies for physical threat protection
Computer Vision Tool
Smart Locks
Human Presence Detector
Water Quality Sensor Placement
Fine-grained Cyber Access Control
Real Time Anomaly Detection
Cross-Layer Security Information and Event Management
Real-Time Anomaly Detector
Toolbox of technologies for security IT and SCADA
Real-time Fault Tolerant Control Strategies
Network Traffic Sensor and Analyzer tool
Real-time Sensor Data Protection
Jammer Detector
Jamming signal
Cyber Threat Sharing Service
Cyber threat representations

FIGURE 1. SOLUTIONS FOR CYBER AND PHYSICAL PROTECTION IN CRITICAL WATER INFRASTRUCTURES AT OPERATIONAL LEVEL

Demonstration Activities

Water infrastructures are essential for society, life and health but they can be endangered with severe consequences by physical and/or cyber threats.

Therefore, the H2020 funded STOP-IT project brings together a strong team formed by 23 partners from all across Europe and Israel, including water utilities, industrial technology providers, small and medium-sized enterprises and top research and development institutes. Together they develop and provide solutions to the most pressing cyber- and physical threats in water infrastructures.

One important part of the STOP-IT project are the demonstration activities of the developed tools and solutions. The purpose of these activities, which have recently kicked-off, is to implement, assess, validate, and evaluate the STOP-IT solutions (e.g. software or hardware based tools developed within the project) in the context of "real-world" operations at the premises of water utilities. Particularly, the demonstrations are held at four major water utilities from Germany, Norway, Spain, and Israel, which are called Frontrunners (FRs) within the project's context. They already implement procedures and protocols to manage cyber-physical risks and therefore have pre-existing experiences in this field.

The efficient and smooth demonstration of STOP-IT solutions required a careful design and preparation, which among other things, ensured the uninterrupted operation of the FRs' existing systems. As a first step towards demonstration of STOP-IT solutions we have opted for the development and use of Virtual Machines (VMs), which offer easy deployability and installation and provide an isolated and safe environment for the demonstration and testing of STOP-IT solutions. Furthermore, we created a detailed list of general technical requirements for all STOP-IT solutions in terms of both functional and non-functional requirements, helping to identify the necessary adaptations of the pilot sites in terms of both, software and hardware. That was to specify the different technical requirements of each pilot site as well as to identify realistic and plausible demonstration cases. In more detail, the STOP-IT demonstration plan foresees three phases.

The first phase:
Is a "beta"-type demonstration activity, where the STOP-IT solutions are provided to the FRs (using VMs – through cloud services when applicable, and/or webinars) accompanied with synthetic/test/dummy datasets. The goal of this phase is twofold, a) to provide an early "hands-on" experience of the solutions' functionality and usability to the FRs, and b) to receive first feedback on the project's solutions, which will be used for further improvement of the solutions (until the end of the project).

In the second phase:
we build up the experience (understanding/preference of some of the solutions, site-specific technical requirements, etc.) gained through Phase I, and demonstrate the STOP-IT solutions using FRs data (real world data from water utilities – possibly anonymized).

As a final demonstration step:
Phase III (optional), regards the full and operational deployment of the STOP-IT solutions in FRs systems (using real-time data when required). In such cases, it is planned to further support the FRs by developing business and exploitation plans for use after the end of the project.

At this point in the project, we have entered Phase II of the demonstration activities, where we are planning to test all STOP-IT solutions at least at one FR pilot site under various configurations - involving both hypothetical, yet plausible scenarios of cyber-physical threats, as well as real-world data from the pilot sites.

Ultimately, through the demonstration activities we aim to provide new insights regarding the suitability and validity of STOP-IT solutions to secure water utilities against cyber-physical threats. We also aim on providing valuable information and experience (lessons learnt) on the domain for future references and use, in terms of both, societal impact and market uptake.

Knowledge transfer through training activities

One important part of the STOP-IT project are the training activities for the developed tools and solutions. STOP-IT builds on a Frontrunner (FR) and Follower (FL) approach, where the four FR water utilities, more advanced with regard to managing risks arising from physical and cyber threats, have been twinned with four ambitious water utilities, in terms of awareness and preparedness. By training the Followers, this concept stimulates mutual learning, transfer and uptake of solutions.

Aiming to develop highly interactive and engaging training methods, tools and materials to increase the transferability and impact of the project outputs, the training material and activities have been designed to target three different users' profiles.

Decision Makers

Board members of a utility and relevant top managers with various background and expertise.

Risk Managers/Officers

At different levels, performance and quality managers, including personnel for modelling activities.

Staff responsible for real time operations

Such as operators, maintenance managers, SCADA room operators etc.

The three different profiles have been aligned with three main objectives of the training material and activities: a) awareness raising on the new era of smart digital solutions and the emerging interconnectivity of cyber-physical infrastructures which are under a wider attack surface of combined cyber-physical risks, b) the enhanced strategic/tactical planning and post action assessment through seamlessly integrated cyber-physical modelling, risk assessment and treatment in the context of strategic and tactical planning for the water sector, and c) the strengthened preparedness, protection and real time response through secure communications, improved IT, SCADA and physical security, sharing of cyber threats and anomaly detections technologies.

Training activities have taken different forms, from face to face meetings and discussions for knowledge, practice and experience exchange among FL utilities to online webinars and execution of hands on activities with STOP-IT technologies.

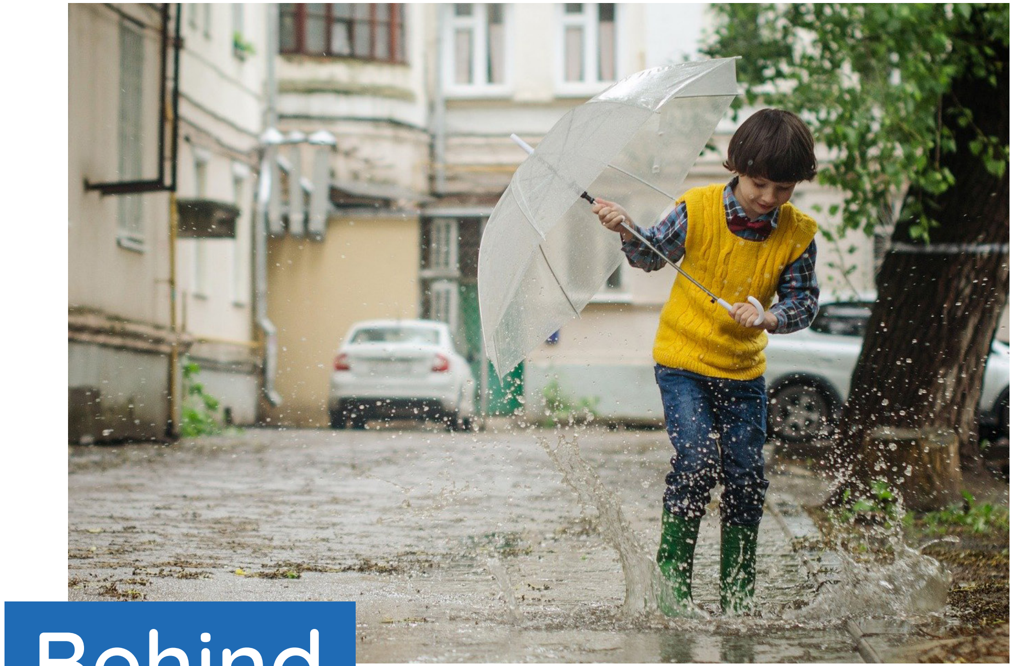
Setting the ground for a constructive discussion during the face-to-face training activities, a video animation focused decision makers' attention on the growing danger coming from the combination of cyber and physical threats **(https://youtu.be/kG6lekwhmJo)**. Further presentations raised awareness on the need to invest in cyber physical security and the fact that cyber and physical infrastructures cannot be seen as separate anymore. The threat of cyber security breaches has emerged as a growing risk for water utilities and the cyber and physical world are connected as water infrastructures lie in the interplay of analogue and digital.

After presenting the objectives of STOP-IT, the discussion that followed revealed important findings. Among them that currently risk analysis focus and investments are mainly on the physical part and only include the cyber side in theory, or that utilities tend to invest on aspects that will have positive feedback on utilities' reputation. There is the misconception from the upper parts of the hierarchy that investing more in cyber physical security might have impact on covering consumers' demand. According to the FLs' representatives, utilities tend to incorporate fully automated processes, but they are not adequately prepared on securing their cyber-physical infrastructures. Based on their testimonies, there is also the challenge of having up-to-date IT infrastructure in order to overcome upgrade issues and problems caused due to interoperability of equipment/systems. As concluded by the FL, STOP-IT can have an added value both at a strategic/tactical and operational level. They are eager to collaborate with FRs but also to be informed on how STOP-IT technologies can interact and complete their systems and have more in-depth knowledge on PLC, SCADA and automation security.

Training activities of risk officers focused on the STOP-IT technologies that aim to enhance risk management processes at the operational/strategic and tactical level. Initially, in the form of a webinar, FLs obtained insights on how the STOP-IT tools function through an overview presentation which was followed by a "live" demonstration in a stepwise approach of the integrated use and tools' functionalities. During a discussion that came next, some FLs and the associated partners expressed their positive feedback by stating that they are "impressed with the work" and that the tools are "customer friendly". The questions raised were related to tools' functionalities and most importantly to data requirements, which would be prerequisite for the actual deployment of technologies to their premises.

The next step of the training process were hands-on experiences of the FLs in the STOP-IT technologies for strategic and tactical planning. Through scheduled sessions with real time support from the technology providers (teleconferences and live chats), FLs accessed and used the developed tools resolving any issue raised immediately. For the easier implementation of activities, FLs were also provided with supportive material which included an overview video of the demonstrated toolkit, a document with step-by-step instructions on accessing and using the tools, brief presentations, manuals and the recorded video of the webinar. Training activities of this profile were finalised by collecting FLs' feedback on the ease of access, facilitation of users learning, support during demonstrations, data requirements, tools' integrity, usability and usefulness. All traits received passing scores, the tools were found reliable and stable and their rates in usefulness were aligned with user's role in the utility. The trait that received the highest marks were the live support sessions.

In the next period, FL utilities will undertake training and knowledge transfer on the technologies focusing at the operational level.



Behind the scenes

Stephanos Camarinopoulos and Dr. Ioannis Tsoukalas are leading the work packages 6 (STOP-IT platform) and 7 (On-Site Integration, Demonstration and Validation activities in the frontrunner utilities) in the STOP-IT project.

What is being done in those work-packages (WP)?

› **Stephanos Camarinopoulos:** Work package (WP) 6 embraces all **STOP-IT** solutions under an integrated **STOP-IT** platform that aspires to cover strategic, tactical and operational needs of water utilities. To serve the requirements of this overarching platform, decision making, alerting and visualisation tools are developed in WP6 to allow the effective handling of information and thus the informed decision making. Before the platform is demonstrated in water utilities, we prepare a validation plan for the entire **STOP-IT** platform that will verify the behaviour of the platform under real-life scenarios, implemented in a controlled environment.

› **Dr. Ioannis Tsoukalas:** The ultimate purpose of **STOP-IT** WP 7 is to provide a hands-on, real-world demonstration of the proposed solutions of the project, involving tools that help water utilities to cope for both, physical and cyber threats, as well as a combination of them. The demonstration activities are performed at four major water utilities called Frontrunners (FRs): AdB (Spain), BWB (Germany), MEK (Israel) and VAV (Norway). Therefore, WP7 can be conceived as a “bridge” between research and real-world application and is also tightly linked with the training and knowledge transfer activities of the project.

What are the main outcomes you are expecting from your WP?

› **Stephanos Camarinopoulos:** The **STOP-IT** platform and the tools developed under WP6 to support it are our main outcome, covering both, the cyber and the physical domain.

› **Dr. Ioannis Tsoukalas:** At the end of the day we are expecting, and hoping that we will be able to communicate a “success story” about each and every **STOP-IT** solution. These “success stories” will allow us to validate the proposed solutions, as well as deploy risk management plans for each pilot site, thus eventually paving the ground to secure water utilities against cyber-physical threats. Finally, we also expect that through WP7 we will gain and provide useful material and knowledge for future training and market uptake activities.

Who is the target audience for your main outcomes and why?

› **Dr. Ioannis Tsoukalas:** Regardless of their technological-adaptation/awareness level, I strongly believe that all water utilities have something to learn from the outcomes of WP7 (and **STOP-IT** in general). For instance, they may identify a solution that fills a gap in their risk management plan, they can explore/valuate alternative (and better) solutions for tasks already implemented in their daily security-related workflows, or even build a risk management plan against cyber-physical threats from bottom-up, which can be the case for small/emerging water utilities.

› **Stephanos Camarinopoulos:** Designed to be scalable, flexible and adaptive, the **STOP-IT** platform is a completely customizable environment where any water utility or industrial organisation can unite a variety of tools and data sources in a single intelligent dashboard.

What do you enjoy most when working for the STOP-IT project?

› **Dr. Ioannis Tsoukalas:** That’s a difficult question. If I had to choose, I would say it’s the “bridge” character. I really enjoy working in the intercept formed between research and real-world practice. This interplay has always something interesting to offer, not to mention the interaction with a wide spectrum of professionals, such as passionate researchers and devoted industry-oriented professionals. Yet in my view the most intriguing part is witnessing and being part of efforts related with bringing novel research developments into fruition. It is always satisfactory to see an idea getting developed, and finally implemented to solve a problem.

› **Stephanos Camarinopoulos:** I firmly believe in taking a collaborative approach to each project and the teamwork required for the **STOP-IT** platform really inspires me. Adding to that the scope of this innovative work - protection of water critical infrastructures - the experience is really fascinating!

Which aspects of the STOP-IT project can affect the water future in a positive way and how?

› **Stephanos Camarinopoulos:** The holistic approach of the solutions developed in STOP-IT can help the Water Future to become safer and smarter by making informed decisions.

› **Dr. Ioannis Tsoukalas:** Arguably Heraclitus' famous quote: "The only thing that is constant is change" is more apparent than ever. The world is evolving, making a transition from an industrial-based economy to an information-based one. This transformation has a different set of key drivers for growth and development, such as information (i.e., data) and its processing (typically by computers). Both these aspects are closely related with the concepts and notions addressed within the field of artificial intelligence. Of course, the above also apply to the water industry. Therefore, and due to the critical nature of water industry, we ought to be prepared. STOP-IT objectives are particularly aligned with this emerging digital era, aiming to provide water utilities with the necessary solutions to cope with this "change"; and thus secure their infrastructures and quality of services beyond physical risks/threats against cyber-physical ones, whose frequency and magnitude is anticipated to increase in this new digital world.

"Recalling the introductory aphorism of E. J. Gumbel's book "Statistics of extremes" that states that 'The improbable is bound to happen one day', the **STOP-IT** project can be viewed as an attempt to secure and prepare water utilities and infrastructures in general against the day where (im-) probable risks of cyber-physical threats become a reality"

Dr. Ioannis Tsoukalas, PhD researcher at NTUA/ICCS and WP7 leader of STOP-IT

"The holistic approach of the solutions developed in **STOP-IT** have a tremendous potential to make the future of water supply and waste water treatment safer and smarter. Decisions can be developed based on solid information, where nowadays intelligent guesses of the experts have to fill in, what is not (yet) available."

Stephanos Camarinopoulos, RISA Germany and WP6 leader of STOP-IT

Update from the communities of practice in STOP-IT

Communities of Practice (CoPs) are defined as groups who share a concern, set of challenges, or interest in a topic, share experience and co-develop knowledge and expertise by continuously interacting across disciplines and fields of practice. Within the STOP-IT project, CoPs have been designed to generate a safe, stimulating space for frontrunners, followers, water utilities, project partners and external stakeholders to exchange knowledge and continuously learn from each other.

THE CoPs IN STOP-IT

Aim to encourage communication, networking and co-learning on cyber physical threats to the water infrastructure. The project CoPs also serve the purpose of connecting the project to other international initiatives related to critical water infrastructure, with the ultimate goal of creating a long term learning alliance on water infrastructure protection.

Because STOP-IT deals with confidential information, a three level CoP approach has been designed:

1. Local CoPs built around the frontrunner cases. These are highly confidential expert meetings, including relevant decision makers and stakeholder representatives

2. Project CoPs involving the STOP-IT project partners and relevant authorities and stakeholders. The confidentiality level of these meetings is medium-low.

3. Trans-project CoP consisting of STOP-IT representatives interacting with the research community, international networks, organizations and companies dealing with critical infrastructure. These CoPs have low to no confidentiality issues for knowledge-exchange.

Since the project is well into its third year, around 30 CoP meetings have been organized.

Local CoPs

Around 20 local CoPs have been organized since the beginning of the project. The local CoPs followed a steps-wise approach with each phase building on the other. The first round of CoPs revolved around getting to know the project and the participants and creating mutual understanding, trust and shared expectations. The second round of CoPs aimed to identify the key risks of the cyber physical threats. The third round, focused on the preparation of the demonstration of the cyber-protection tools developed in the project. The upcoming fourth, and final, round of CoPs will most likely focus on the demonstration of the developed tools. Given the confidentiality of the issues addressed, the local CoPs were designed to be exclusively face-to-face meetings. However, the current global pandemic has led to exploring options for safely host online local CoPs. Overall, the local CoPs are appreciated for their positive and open atmosphere, the creation of collaboration opportunities, the capacity to connect to fellow project members and create better understanding between the technology providers and the end users.

Project CoPs

Up until now, four Project CoPs have been organized. The annual Project Steering Board (PSB) meeting is taken as an opportunity to organize a project CoP with

all partners. The first project CoP managed to set up a framework for knowledge exchange and to come to shared expectations on the project results among project partners. The subsequent project CoPs focused more on the project content such as risk management and joint preparation for the demonstration of the developed tools. The CoPs participants valued these meetings highly, both in terms of content and facilitation format (World Café). In particular, having face to face discussions was highly appreciated as it offered the opportunity to better bridge the gaps between utilities and research institutes.

Trans-project CoPs

Activities related to the Trans-project CoPs are organized centrally by the coordinator of the project, and include project experts. This high degree of involvement of project partners allowed the STOP-IT project to be recognized as a very active contributor to security issues by experts across Europe. So far, STOP-IT is connected via trans-project CoP activities with the following international networks:

- International network of National Contact Points for the Societal Challenge (Net4Society)
- Community of Users on Secure, Safe and Resilient Societies (CoU)
- IMG-S network
- European Reference Network for Critical Infrastructure Protection (ERNCIP)
- ICT4water cluster
- European Cluster for Securing Critical infrastructures (ECSCI)

The contribution of STOP-IT to Trans-project CoP was appreciated by international experts, scientist and security providers, and in particular by operators with own tools and solutions against cyber and physical attacks to which much of the STOP-IT dissemination activities are oriented to.

Upcoming activities

In the upcoming months several local CoPs will take place to prepare the 2nd demonstration phase of the project. The Frontrunners play a significant role in this context. The learnings and results of the local CoPs will be shared and discussed at the next project meeting in June 2020. A project CoP is also planned for October 2020. Finally, in October the training of followers with a learning method called a 'serious game' will also be evaluated from a CoP perspective. This activity will provide insights on the use of serious games as facilitation format for CoPs.

STOP-IT

stop-it-project.eu
info@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.