EPiC Series in Engineering
Volume 3, 2018, Pages 2112–2119
HIC 2018. 13th International
Conference on Hydroinformatics

STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats

R. Ugarelli[1], J. Koti[2], E. Bonet[3], C. Makropoulos[4], J. Caubet[5], S. Camarinopoulos[6], M. Bimpas[7], M. Ahmadi[1], L. Zimmermann[2], M. G. Jaatun[1]

[1]SINTEF, Forskningsveien 3b, Oslo, Norway;
[2]IWW Zentrum Wasser, Moritzstr. 26, Mülheim an der Ruhr, Germany
[3]Cetaqua Barcelona, Ctra. d'Esplugues, 75, Cornellà de Llobregat, Barcelona, Spain
[4]KWR, Water Cycle Research Institute, Groningenhaven 7, PE Nieuwegein, the Netherlands
[5]Eurecat, Carrer de Bilbao, 72, Barcelona, Spain
[6]RISA Sicherheitsanalysen GmbH, Xantener Straße 11, Berlin-Wilmersdorf
7ICCS 28is Oktovriou 42, Athina, Greece
rita.ugarelli@sintef.no

Abstract

Water supply and sanitation infrastructures are essential for our welfare, but vulnerable to several attack types facilitated by the ever-changing landscapes of the digital world. A cyber-attack on critical infrastructures could for example evolve along these threat vectors: chemical/biological contamination, physical or communications disruption between the network and the supervisory SCADA. Although conceptual and technological solutions to security and resilience are available, further work is required to bring them together in a risk management framework, strengthen the capacities of water utilities to systematically protect their systems, determine gaps in security technologies and improve risk management approaches. In particular, robust adaptable/flexible solutions for prevention, detection and mitigation of consequences in case of failure due to physical and cyber threats, their combination and cascading effects (from attacks to other critical infrastructure, i.e. energy) are still missing. There is (i) an urgent need to efficiently tackle cyber-physical security threats, (ii) an existing risk management gap in utilities' practices and (iii) an un-tapped technology market potential for strategic, tactical and operational protection solutions for water infrastructure: how the H2020 STOP-IT project aims to bridge these gaps is presented in this paper.

G. La Loggia, G. Freni, V. Puleo and M. De Marchis (eds.), HIC 2018 (EPiC Series in Engineering, vol. 3), pp. 2112–2119

1 Introduction

Water supply and sanitation are critical infrastructures (CI) essential for human society, life and health. CI can be endangered, disrupted or destroyed by events related to physical and cyber threats including, but not restricted to, deliberate attacks, with fatal consequences for society. The spectrum of potential physical and cyber threats in the water sector, including cyber terrorism, has grown to a problem of general concern within the last two decades. For instance, as water utilities expand their reliance upon information technology and begin integrating industrial control systems (ICS) infrastructure to increase productivity and reduce operating costs, such reliance exposes utilities to potential cyber-related risks. A successful attack could cause major damage, responsible for long periods of operational downtime, financial losses, loss of trust for water utilities and most importantly, a direct threat to public health and societal stability.

Managing the risks from significant physical and cyber threat to CI (both physical and cyber asset of it) requires an integrated approach across this diverse community to:

- Identify, deter, detect, disrupt, and prepare for threats and hazards to the CI;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences of incidents or adverse events that do occur.

The success of an integrated approach depends on leveraging the full spectrum of capabilities, expertise, and experience across the CI community and associated stakeholders. This requires efficient co-creation of technological solutions and sharing of actionable and relevant information among partners to build situational awareness and enable effective risk-informed decision making.

This paper will describe how the H2020 project STOP-IT will have a major impact for strategic, tactical and operational protection of water CI against physical and cyber threats.

The results of the STOP-IT project will allow the development of new safety and security plans to protect CIs associated to the water networks, as well as new avenue of business activities related to security audits in water utilities. STOP-IT started in June 2017 and will last for four years (www.stop-it-project.eu).

2 STOP-IT objectives, approach and expected technological outcomes

2.1 STOP-IT strategic and technical objectives

The strategic goal of STOP-IT is to make water systems secure and resilient by improving preparedness, awareness and response level to physical, cyber threats, and their combination, while considering systemic issues and cascading effects. The ultimate goal will be achieved by meeting the following technical objectives:

- Raise awareness and cooperation in the water sector on cyber-physical security and facilitate exchange of best practices, knowledge and benchmarks by networking between stakeholders through the creation of Communities of Practice (CoP).
- Enhance water utilities ability to identify and test alternative risk treatment options.
- Improve the water industry's procedures for assessing the vulnerability of systems to physical, cyber, as well as combined physical-cyber security threats.
- Strengthen current response and recovery capacities and improve preparedness through enhanced event detection and prevention capabilities.

- Ensure wide applicability of security solutions by developing flexible and validated ones for different usage contexts.
- Protect the inhabitants near the CI of the water utility and enhance communication with the personnel, the security/First Responder and monitoring teams by providing an innovative method based on public warning systems for sharing information.
- Enhance the external impact of the project by demonstrating financing and investment options for the different project outcomes.
- Enhance practical knowledge on cyber-physical water infrastructure protection through training and accreditation schemes for water system operators.
- Contribute to an open access knowledge
- Contribute to the pre-establishment of certification mechanisms crossing boundaries between different CI sectors.

2.2 STOP-IT methodology

The STOP-IT overall methodology is based on the development, demonstration, evaluation and preparation for market uptake of the STOP-IT platform, as Scalable, Adaptable and Flexible solution to support strategic/tactical planning, real-time/operational decision making and post-action assessment for the key parts of the water infrastructure.

STOP-IT solutions are demonstrated through a front-runner/follower approach (FR/FL) where four advanced utilities, Aigües de Barcelona (Spain), Berliner Wasserbetriebe (Germany), MEKOROT (Israel) and Oslo VAV (Norway) are twinned with four ambitious water utilities, Hessenwasser (Germany), Bergen Kommune (Norway), Emasagra (Spain) and DeWatergroep (Belgium) to stimulate mutual learning, transfer and uptake.

The methodology followed to achieve the overall STOP-IT aim, through the activities performed in 9 Work Packages (WP), is depicted in Figure 1.

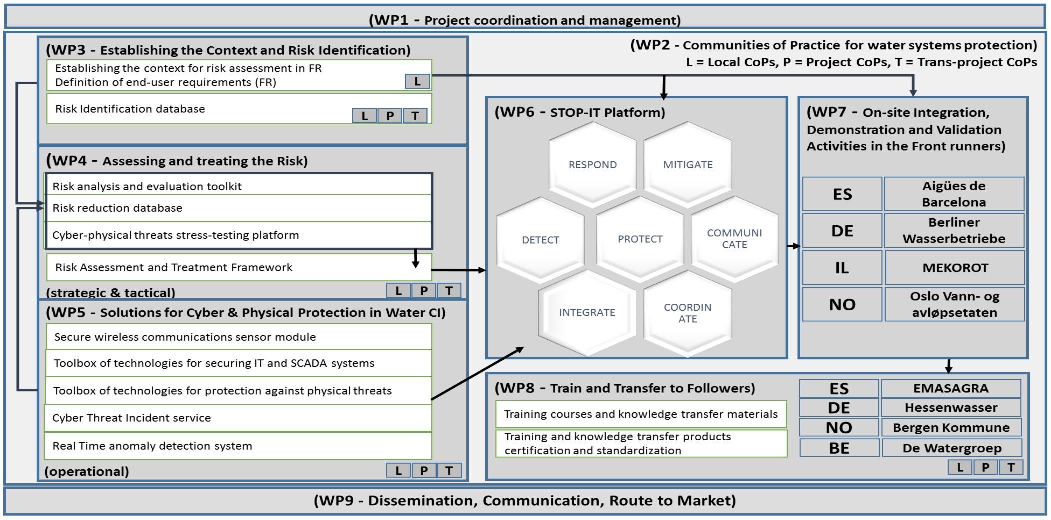
(WP1 - Project coordination and management)
(WP3 - Establishing the Context and Risk Identification)
Establishing the context for risk assessment in FR
Definition of end-user requirements (FR)
L
Risk Identification database
L P T
(WP2 - Communities of Practice for water systems protection)
L = Local CoPs, P = Project CoPs, T = Trans-project CoPs
(WP4 - Assessing and treating the Risk)
Risk analysis and evaluation toolkit
Risk reduction database
Cyber-physical threats stress-testing platform
Risk Assessment and Treatment Framework
(strategic & tactical)
L P T
(WP6 - STOP-IT Platform)
RESPOND
MITIGATE
DETECT
PROTECT
COMMUNI CATE
INTEGRATE
COORDIN ATE
(WP7 - On-site Integration, Demonstration and Validation Activities in the Front runners)
ES
Aigües de Barcelona
DE
Berliner Wasserbetriebe
IL
MEKOROT
NO
Oslo Vann- og avløpsetaten
(WP5 - Solutions for Cyber & Physical Protection in Water CI)
Secure wireless communications sensor module
Toolbox of technologies for securing IT and SCADA systems
Toolbox of technologies for protection against physical threats
Cyber Threat Incident service
Real Time anomaly detection system
(operational)
L P T
(WP8 - Train and Transfer to Followers)
Training courses and knowledge transfer materials
Training and knowledge transfer products certification and standardization
ES
EMASAGRA
DE
Hessenwasser
NO
Bergen Kommune
BE
De Watergroep
L P T
(WP9 - Dissemination, Communication, Route to Market)

Figure 1 - The STOP-IT approach

The STOP-IT methodology is inspired by the risk management procedure from ISO Risk Management Framework (ISO 31000:2009), including the steps of "Establishing the context", "Risk identification", "Risk analysis", "Risk evaluation" and "Risk treatment". Compatibility with this standard will be key for the acceptance and interoperability of the STOP-IT framework with existing procedures in the water sector.

The development of a Risk Identification Database (RIDB) and the characterisation of the FRs infrastructure and technical requirements, for the integrated platform architecture and for the demonstration, are the current focus of the project.

The step "Establishing the context" has been performed in WP3 in close collaboration with the FR water utilities, along dedicated events organized in the local CoPs (WP2). Establishing the context includes:

- Characterisation of the FR infrastructure.
- Setting the scope, extent and specific objectives of risk management (such as protection of public health and safety, of the environment, of key economic activities; spatial scales and level of detail at key systems).
- Compiling formal requirements (legislation or regulations, standards, codes of practices, etc.)
- Understanding the internal context.
- Defining the context for risk assessment (such as, the risk management activities of the end users; responsibilities and authorities within the risk management process; risk assessment methods and tools to be used)
- Set criteria against which risk events will be evaluated risk depending on specific conditions at each FR site.

The step "Risk events identification" in WP3 has generated a comprehensive list of potential risk events that may affect a water utility in achieving each objective identified as part of the context. The outcome from this phase will be a RIDB covering the identified risks at strategic, tactical and operational level of planning and applied to the whole water CI system. The list of risk events covers (by a procedure of horizon scanning, based on the methodology developed in the project "new strains for society") also emerging risks, and include inputs from the CoPs, therefore not limited to the FR.

The RIDB will allow the users to commence the process and draw their attention to risk events that should be investigated, when local conditions indicate that these are somehow likely to happen. Furthermore, events considered in the database are not necessarily realistic for each application, but will be further analysed and evaluated in WP4. Only after the step of risk evaluation, the list of risk events requiring risk treatment will be identified.

The step “Risk Analysis and Evaluation” as well as the step “Risk Treatment” at strategic and tactical level will be performed with the risk assessment and treatment framework developed in WP4. The framework will integrate (see also Table 3):

(a) an online tool acting as procedural "step by step" guide for assessing the vulnerability of assets to (all identified) risk events due to potential physical and cyber threats and their combination, in view of existing protection measures;

(b) an advanced toolkit for the analysis and evaluation of risks to the water system comprising selected state of art models and tools. The toolkit will be able to simulate (in a simplified manner) the entire water system and assess the impact of potential incidents due to physical-cyber threats. Both water quantity and water quality effects will be simulated using the toolkit. The toolkit will contain four elements described in the following Table 1:

Table 1 - Risk assessment and treatment framework components

KPIs	Identification of a multiple key metrics against which (loss of) performance will be measured to assess the criticality of assets, including: affected populations in terms of various matrices such as loss of supplied water (customer minutes loss) or supply of sub-standard/polluted water and related health risks; disruption of service to critical customers (hospitals, schools, government, first responders); system survival time after an incident based on dynamic parameters such as water demand and incident response times.

Models	A multi-scale modelling approach will be employed based on whole hydro-system model (UWOT, Rozos & Makropoulos, 2013), while hydraulic modelling and contamination events propagation in water distribution networks will be based on EPANET. Technologies developed within the EFFINET FP7 project will be used to consider the ICT layer of sensors/actuators above the system. Cascading effects from multiple hazards and other infrastructure will be simulated through open source platforms. A probabilistic approach will be used to assess of the overall risk evolution.
Scenario Planner	An intuitive scenario planning environment will be developed in the project that will allow for the setup of different threat scenarios that will then be provided to the models for impact assessment.
Optimi-sation	The assessment will be driven by advanced multi-objective optimisation algorithms which will be used to calibrate the models identify most critical components from a combination of threats.

(c) online Risk Reduction Measures Database (RRMD) with advanced choice support capabilities (based on multi-criteria analysis) to facilitate the identification and selection of appropriate RRM. Using the database, the user will start by undertaking a priory systematic identification of RRM for each risk (trough semantic mapping between RIDB entries and the related RRMD entries), having a characterisation of the potential of that measure to reduce the risks found as not acceptable from the risk analysis and evaluation process (b).

(d) simulation-emulation stress testing platform that can simulate both physical and cyber sub-systems, based on JRC's EPIC (http://ses.jrc.ec.europa.eu/epic-hub) platform concept, coupling the simulation environment for the physical layer of the water system already developed in (b) to (i) simulations of physical layers of other interconnected infrastructure and also (ii) to an emulation environment able to model the cyber layer of the water system control and communication infrastructure where cyber protection solutions will be implemented and cyber-attacks attempted.

These elements (from a to d) will come together into a semantic enriched, Risk assessment and treatment framework, where additional methodologies will be added to evaluate the cost –effectiveness of RRMD selected, after stress test, for the risk events to be treated (e.g. cost effectiveness analysis, cost benefit analysis, selected methods from Multi Criteria Decision Approaches (MCDA)). The semantic layer will be composed by a knowledge base modelled using existing ontologies as physical and cyber semantic models, geographic semantic models and social representation among others.

Innovative solutions to treat the inherent risks at operational level in the CI water sector will be the focus of WP5. The range of the proposed protections schemes will be broad, ensuring comprehensive protection of water CIs, covering physical, communications, IT and SCADA attack routes. As a first step physical threats are taken into account, and to protect water CIs from physical threats, STOP-IT proposes novel technologies listed as module 4 in Table 3.

Once the physical layer is secure, the following step is to secure communications, both wired and wireless. STOP-IT will focus on developing novel and more efficient solutions for securing wireless channels. The security of existing solutions and protocols, as LTE-M, NB IoT, Long Range WLAN (LoRa, SIGFOX), will also be analysed. Traditional IT and SCADA systems will be addressed too, through two basic approaches: (a) an innovative application of blockchain technology principles to protect high-volume, real-time data, (b) the development of two advanced control centres, one covering the management and visualisation of cyber-incidents and the other dealing with the anomaly detection for operational threats, taking special consideration to the simultaneous and combined threats that can lead a CI to its unavailability.

A modular software integrated platform to embrace the outcomes of WP4 and WP5, plus the additional modules for the immediate information of the people in the vicinity of the critical event and the improved visualisation interfaces (see modules 7-9 in Table 3), will be provided by WP6. The project will follow an iterative process both in producing the overall framework design and the integrated prototypes that will be validated in a simulation environment. The tested platform will then be deployed and integrated into a respective real-life system for further testing and validation in WP7. This WP will focus on piloting and demonstration in the four different contextual backgrounds of the project FR water utilities.

The methodological, technological and procedural advances of the project will be encapsulated into standardized, high quality knowledge and transfer products in WP8. These products will be tested and improved through the FLs in an iterative manner, allowing for a knowledge co-production process whereby the end users of the training and knowledge transfer products will be able to feedback suggestions for improvement and customisation of the knowledge products, as the training and transfer process progresses. Educational platforms, including serious games and open labs, will be developed making use of the stress testing platform developed in WP4, as engine for games and virtual environment. By using the developed relevant knowledge-transfer materials, the outputs of the project will be transferred to FL utilities, but also embedded into already operational training scheme (such as the European Network for Cyber Security (ENCS) and the EU CPSE Labs Design Centres). Since the project will work together with other institutional stakeholders (such as ENISA and the first European PPP on cybersecurity (http://europa.eu/rapid/press-release_IP-16-2321_en.htm), WP8 will foster collaboration to develop a European Certification Scheme on Cyber-Physical Security for CI.

The role of the FLs in STOP-IT is not limited to the participation to the CoPs in WP2 and to training activities in in WP8, but, in WP9, they will act as drivers to market transferability, uptake and replication of STOP-IT outcomes.

WP9 will i) create and enhance visibility of the project and its most important outputs, and ii) develop exploitation strategies and plans to foster market introduction of the key innovations of the project within the wider European community of utilities.

2.3 The STOP-IT technological outcomes

Prevention, Detection, Response and Mitigation of relevant risks at strategic, tactical and operational levels will be addressed through modular solutions (technologies, tools and guidelines), at different TRL levels, brought by the STOP-IT consortium, embedded into the STOP-IT software platform, developed up to at least TRL 7 (Table 2).

Table 2 - Modular components of the STOP-IT risk management platform

No	STOP-IT modules	Description	Foreseen TRL
1	Risk Assessment and Treatment Framework, including:	A RIDB, a step-by-step guide for vulnerability assessment, a modelling toolkit for risk analysis and evaluation, a RRMD, linked to the RIDB, recommending actions to avoid or mitigate the occurrence and consequences of risk events for water CIs, a stress-testing platform to evaluate the effectiveness of RRM and a decision support tool to guide the choice of risk treatment options.	7
2	Secure wireless sensor communications module	A secure wireless sensor communication module capable of analysing the wireless spectrum range of several technologies (from WiFi to cellular) to detect different types of radio security threats, such as Denial of Service. This module will inform about wireless channel activities affecting regular network communications. Furthermore, it will provide an innovative method to locate the identified threats geographically, so corrective actions can be implemented to challenge the security threats.	8

3	Toolbox of technologies for securing IT and SCADA	Technologies for SCADA and IT systems to monitor and protect their integrity, both against intentional attacks or malfunction. They include a blockchain-based scheme to assure the integrity of all the data generated during a CI operation (logs, sensor data, etc.)	7
4	Toolbox of technologies for protecting against physical threats in CI, including:	Coordinated network cameras: computer vision tools for automated surveying of the large-area of the water utility	7
		XACML Authorization Engine: service-oriented attribute-based access control mechanism that employs user specified policies to determine who can access which resources and for what purpose in CI restricted environments.	7
		Human presence detection using WiFi signals reflection in human body to detect the presence of persons in restricted areas	7/8
		Water quality monitoring technologies for the early detection and impact minimization of contamination events (intentional attacks) based on an optimization-simulation framework using measurements provided by quality sensors placed at strategic placements	7
		Access control system based on intelligent electronic locks and dedicated applications to service employees and to central management system.	8/9
5	Cyber Threat Incident Service	A cyber Threat Incident Centre collecting data feeds from incidents and related vulnerabilities and providing preventive actions.	8/9
6	Real-Time anomaly detection system	A system to detect unknown anomalies, with automatic learning abilities for RT anomaly detection of combined threats and attacks.	7/8
7	PWS-Secure Information Exchange Technologies	An optimized Public Warning System (PWS) module as a blend of the best attributes of all of the existing technologies, adapted to the particular demands of water CI and the country or territory in question (different use cases).	8/9
8	Reasoning Engine	Continuous assessment of the risk exposure of an organisation by executing specific reasoning (rule based) algorithms.	7
9	Enhanced Visualisation Interface	Visualization module operable in mobile environment, as well as to the control centre of the water utilities. It will act as a Common Operational Picture (COP).	7

3 International cooperation in STOP-IT

STOP-IT, coordinated by SINTEF, is conceived as a cooperative project, which will strengthen the EU international cooperation by involving (eight) water utilities, (six) private companies (ATOS, PNO, Aplicatzia, World Sensing, RISA, Mnemonic) and (seven) R&D partners (SINTEF, IWW, CETaqua, KWR, EURECAT, Technion, ICCS) from seven EU and H2020 associated Countries: Belgium, Germany, Greece, Israel, Norway, Spain and The Netherlands. To further enhance EU competitiveness and support EU external policy objectives, STOP-IT includes the European water platform (WssTP) as partner to foster collaborative, innovative and integrated European research and technologies development and ensure the European growth and competitiveness of the water sector. Furthermore, STOP-IT will collaborate with key cyber-physical security research partners, such as the Sandia National Laboratories in the USA, through their strong involvement in the project's advisory board.

As very first collaborative action STOP-IT has joined the ICT4WATER cluster (www.ict4water.eu/) in September 2017.

4 Conclusions

Water infrastructures are essential for human society, life and health. They can be endangered by physical or cyber threats with severe societal consequences. To address this, the H2020 funded STOP-IT project brings together a strong team of water utilities, industrial technology developers, high tech small and medium-sized enterprises and top research & development providers from all across Europe to develop solutions to the most pressing threats. In STOP-IT, prevention, detection, response and mitigation of relevant physical and cyber related risks at strategic, tactical and operational levels will be addressed through modular solutions (technologies, tools, training material and guidelines), at different TRL levels, embedded into the STOP-IT software platform, developed up to at least TRL 7. To ensure the development of sound solutions, all the STOP-IT technologies will be tested and validated by the FR operators, with the involvement of different users (security officers, terminal operators, facility operators, associated technology providers, and more) through interactions with researchers. STOP-IT has also included four FL water utilities that will undertake training and knowledge transfer exercises with a focus on the experimentation, interactive learning and transferability and scalability of solutions provided by the project. The FLs will contribute to the definition of user requirements along dedicated events of the project CoPs and will allow evaluating the market uptake and replication of STOP-IT outcomes.

5 Acknowledgment

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. The paper has been written by the STOP-IT Scientific and Technical Committee on behalf of the STOP-IT Consortium.

References

ISO (2009). ISO 31 010:2009 Risk management. Risk assessment techniques. International Standards Organization.

Rozos, E. and C. Makropoulos. "Source to tap urban water cycle modelling. "Environmental modelling & software 41 (2013): 139-150.