e-book

Habtamu Abie, Davide Ferrario, Ernesto Troiano,
John Soldatos, Fabrizio Di Peppo, Aleksandar Jovanović,
Ilias Gkotsis, Evangelos Markakis (Eds.)

# Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection

## Virtual Workshop, June 24–25, 2020

Steinbeis-Edition

# Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection

Virtual Workshop, June 24–25, 2020

Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo, Aleksandar Jovanović, Ilias Gkotsis, Evangelos Markakis (Eds.)

Steinbeis-Edition

# Abstract

Modern critical infrastructures ("critical entities" in the terminology of the new EU-CER Directive) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Thus, addressing cyber security and physical security separately is no longer effective, but more integrated approaches, that consider both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects, are needed to face the challenge of combined cyber-physical attacks. To face them successfully, aligned and integrated responses are needed, and this workshop has provided a great opportunity to do it: aligning and integrating not only the positions of single projects but also of many intended users of their results.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in seven different industrial sectors, such as finance, healthcare, energy, air transport, communications, industrial plants, gas, and water. The peculiarities of critical infrastructure protection in each one of these sectors have been discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies.

Specifically, novel techniques have been presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, resilience of critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures.

The workshop included two opening remarks, two keynote speeches, 11 project presentations, 2 roundtable and panel discussions and 10 thematic presentations. The audience included scientists and experts in the field of critical infrastructure protection, CISOs, CIOs, CERTs, CSIRTs, CSOs, cyber and physical security experts representing different sector and policy makers for Critical Infrastructure protection.

# Table of Contents

**Imprint**

2021 Steinbeis-Edition

Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo,
Aleksandar Jovanović, Ilias Gkotsis, Evangelos Markakis (Eds.)

Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection
Virtual Workshop, June 24–25, 2020

1st edition, 2021 | Steinbeis-Edition, Stuttgart
ISBN 978-3-95663-087-3

Layout: Steinbeis-Edition
Cover picture: Macrovector/shutterstock.com



218957-2021-10 | www.steinbeis-edition.de

# 1. Organizations

The organizing committee consists of the following members all from the FINSEC project:

- Habtamu Abie
- Davide Ferrario
- Ernesto Troiano
- John Soldatos
- Fabrizio Di Peppo

# 2. Program Agenda

The two days' workshop program agenda includes keynote speeches from the EC, ENISA, and ECSO, 11 H2020 projects results presentations, roundtable and panel discussions, and thematic presentations.

- ECSCI (European Cluster for Securing Critical Infrastructures) Workshop
- Venue: Google Meet
- Dates: June 24–25, 2020

Day 1: Wednesday, June 24th, 2020 (09:00 – 17.10)

| | |
|---|---|
| 09:00 – 09:20 | Welcome and opening remarks: Habtamu Abie (NRS) and Andrea de Candido, Head of Unit of DG HOME B4 Innovation and Industry for Security |
| 09:20 – 10:00 | **Invited Talk:** Critical Information Infrastructure Protection: The role of ENISA in the new EU policy context – Kostantinos Moulinos (ENISA) |
| 10:00 – 10:10 | Coffee Break |
| 10:10 – 10:30 | DEFENDER (https://defender-project.eu/): Energy infrastructure protection - Gabriele Giunta (Engineering) |
| 10:30 – 10:50 | SAFECARE (https://www.safecare-project.eu/): Safeguarding critical health infrastructure by Philippe Tourron (APHM – Hôpitaux universitaires de Marseille) and Isabel Praça (ISEP – Institut Superior de Engenharia do Porto) |
| 10:50 – 11:10 | FINSEC (https://www.finsec-project.eu): Securing critical financial infrastructure – Ernesto Troiano (GFT) |
| 11:10 – 11:30 | Coffee Break |
| 11:30 – 11:50 | InfraStress (https://www.infrastress.eu/): Improving resilience of sensitive industrial plants & infrastructures – Lorenzo Franco Sutton (Engineering) |
| 11:50 – 12:10 | RESISTO (http://www.resistoproject.eu/): Resilience enhancement and risk control for communication infrastructures – Bruno Saccomanno (Leonardo – Società per azioni) |
| 12:10 – 12:30 | STOP-IT (https://stop-it-project.eu/): Protection of critical water infrastructures by Rita Ugarelli (SINTEF) |
| 12:30 – 14:00 | Lunch Break |
| 14:00 – 15:00 | Physical and Cyber security integration and modelling |

| | |
|---|---|
| | • Applied to WATER critical infrastructure by Christos Makropoulos (ICCS/NTUA, Greece)<br>• FINSTIX Data Modelling by Giorgia Gazzarata (CINI)<br>• SAFECARE approach to integrated cyber-physical security for the healthcare sector by Fabrizio Bertone (LINKS Foundation) |
| 15:00 – 15:40 | Round table discussions<br>• Combining cyber and physical security management for critical infrastructure protection by Theodore Zahariadis (University of Athens)<br>• Could standardization break the silos approach in Critical Infrastructure Protection? by Denis Caleta (CS-Institut) |
| 15:40 – 16:00 | Coffee Break |
| 16:00 – 16:20 | ELSI - Panel Discussion<br>Ethical, legal, and social implications of projects by Sylvia Bach (University of Wuppertal) |
| 16:20 – 16:40 | Protect Industry 4.0 - Panel Discussion<br>How to protect Industry 4.0 Sensitive Industrial Plants from cyber and physical attacks by Luigi Romano (University of Naples "Parthenope") |
| 16:40 – 17:00 | Collaborative Risk Assessment - Panel Discussion<br>Collaborative Risk Assessment and Impacts by John Soldatos (Innov-acts) |
| 17:00 – 17:10 | Conclusions and Collaboration Planning of Day 1 |

Day 2: Thursday, June 25th, 2020 (9:00 – 15.30)

| | |
|---|---|
| 09:00 – 09:10 | Welcome and second day introduction |
| 09:10 – 10:00 | **Invited talk:** Moving towards a trustworthy and resilient European cyber security ecosystem – Roberto Cascella (ECSO) |
| 10:00 – 10:20 | Resilience of Critical Infrastructures<br>Indicators for assessing resilience of the European critical infrastructures: Wishful thinking vs. engineering challenge by Aleksandar Jovanović (EU-VRi & Steinbeis Advanced Risk-Technologies) |
| 10:20 – 10:40 | Coffee Break |
| 10:40 – 11:00 | ANASTACIA (http://www.anastacia-h2020.eu/): Security and trust assessment in CPS / IOT architectures - Stefano Bianchi (AlgoWatt Spa) |
| 11:00 – 11:20 | SATIE (http://satie-h2020.eu): Security of air transport infrastructure of Europe – Kelly Burke (DGSSPA) |
| 11:20 – 11:40 | SecureGas (https://www.securegas-project.eu/): Securing the European gas network – Ilias Gkotsis (KEMEA) |

| | |
|---|---|
| 11:40 – 12:00 | SPHINX (https://sphinx-project.eu/): Cyber-security protection in healthcare IT ecosystem – Evangelos Markakis (Hellenic Mediterranean University-HMU) |
| 12:00 – 12:20 | SmartResilience (http://www.smartresilience.eu-vri.eu/) – Aleksandar Jovanovic (Risk-Technologies) |
| 12:20 – 12:40 | Automation – Panel Discussion:<br>Increased automation for detection, prevention and mitigation measures – Evangelos Markakis (Hellenic Mediterranean University-HMU) |
| 12:40 – 13:00 | Legal and Ethical issues – Panel Discussion<br>Legal and Ethical frameworks concerning cybersecurity of critical infrastructures (with a specific focus on healthcare and medical devices) – Elisabetta Biasin (KU Leuven) |
| 13:00 – 14:00 | Lunch Break |
| 14:00 – 14:20 | Artificial Intelligence – Panel Discussion<br>Artificial Intelligence for Securing Critical Infrastructures – John Soldatos (Innov-Acts) |
| 14:20 – 14:40 | Predictive Analytics – Panel Discussion<br>AI based CCTV Analytics for Cyber-physical Security – Adrien Besse and Jürgen Neises (Fujitsu) |
| 14:40 – 15:00 | Anomaly detection – Panel Discussion<br>Applying Machine Learning algorithms to build anomaly-based cyber and physical detection systems – Juan Caubet (EURECAT) |
| 15:00 – 15:30 | Conclusions and Collaboration Planning of Day 2 |

# 3. Welcome and Opening Remarks

## 3.1 Opening Remarks

Andrea de Candido, Head of Unit of DG HOME B4 Innovation and Industry for Security

The coming months are very important for the future of infrastructure protection, with the new Security Union Strategy being adopted and a dedicated policy for CIP upcoming as part of the Commission work programme. On the side of research, the transition from Horizon 2020 to Horizon Europe is closely linked to those initiatives, since the research programme will support their implementation with targeted projects. Looking at the global landscape and the enormous challenges Europe is facing in protecting its vital infrastructures, it is evident that without such research we will not be able to respond to complex threats or keep up with the necessary technological developments that ensure strategic autonomy. Security research will play a strategic role since many of the challenges will not be solved with laws and regulations alone but are of technical nature and thus require close cooperation with experts from academia and industry.

A strong security research aimed at enhancing infrastructure protection needs an active community. As such, activities like the ones undertaken by ECSCI are very useful initiatives that complement other instruments that are used by the Commission to facilitate exchanges on innovation in security among relevant stakeholders, most notably the Community of Users for Secure, Safe and Resilient Societies (CoU). The specific focus on cross-cutting priorities which this cluster has put at the core of the work reflects the approach which the Commission also suggests for the future research on infrastructure protection: leaving behind the sectoral approach and instead identify more common challenges and solutions. This rationale combined with a strategic and foresight-oriented approach will be the guiding principles for the first work programme of Horizon Europe in the Infrastructure Protection domain.

## 3.2 The ECSCI Cluster Achievements

Habtamu Abie, Norwegian Computing Center

European Cluster for Securing Critical Infrastructures (ECSCI – https://www.finsec-project.eu/ecsci) is a cluster of H2020 projects for securing critical infrastructures. Its main objective is to bring about synergetic, emerging disruptive solutions to security issues via cross-projects collaboration and innovation. The cluster will research how to protect critical infrastructures and services, highlighting differences (approaches, sectors of interest, etc.) between the clustered projects and establishing tight and productive connections with closely related and complementary H2020 projects. To promote the activities of the cluster, ECSCI organizes international conferences, and national or international workshops highlighting the achievements within the cluster. These events involve policy makers and the public. The cluster's foreseen impacts will include stimulating the uptake of project results, the exploitation of synergies, sharing best practices, effectively executing activities of common interest (such as IPR management, standardization and policymaking), stimulating network and alliance formation for further Research and Technical Development and industrial innovation, and increasing public awareness of the cluster activities by targeted communication activities.

Figure 1 depicts the ECSCI cluster members, collaboration topics and proposed activities. ECSCI Liaison Plan. European Commission encourages collaboration among funded projects. Hence the Liaison Plan is to create the ECSCI cluster of H2020 projects dealing with cyber and physical security of critical infrastructures and underpinning complex architectures.


**Figure 1 – The ECSCI Cluster members and collaboration topics**

ECSCI's identified main high-level objectives are scientific collaboration, technical collaboration, communication, and dissemination (workshops, press, web presence), stakeholder alliance, and marketplace. The specific objectives of the ECSCI cluster are to (i) create synergies and foster emerging disruptive security solutions via cross-projects collaboration and innovation, (ii) focus on the different approaches between the clustered projects, (iii) establish tight and productive connections with closely related and complementary projects, and (iv) promote the activities of the cluster international scientific conferences/workshops and national or international stakeholders workshops, involving both policy makers, industry and academic practitioners, and representatives from the European Commission. Table 1 shows the events of the ECSCI success stories.

**Table 1 – ECSCI Success Stories: Events**

| # | Events | Organizers | Participants | Place and Dates |
|---|---|---|---|---|
| 1 | SAFECARE Awareness Event | SAFECARE | FINSEC, SATIE, SPHINX | Leuven, September 18, 2019 |
| 2 | FINSEC 2019 (1st International Workshop on Security for Financial Critical Infrastructures and Services) Co-located with ESORICS 2019 | FINSEC | DEFENDER | Luxembourg, September 27, 2019 |
| 3 | 1st ECSCI Virtual Workshop | All Cluster members | All Cluster members | Google Meet, 24-25, June 2020 |
| 4 | CPS4CIP 2020 (The 1st International Workshop on Cyber-Physical Security for Critical Infrastructures Protection) Co-located with ESORICS 2020<br><br>Check CPS4CIP 2020: https://sites.google.com/fbk.eu/cps4cip20 | FINSEC, DEFENDER, RESISTO, SAFECARE, STOP-IT | All Cluster members support the workshop | Guildford, UK, September 14-18, 2020 |

**The Open Access Book** (John Soldatos et al. 2020). The success stories in terms of collaboration and information sharing include the co-edition of Open Access Book entitled Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures by J. Soldatos (FINSEC), G. Giunta (DEFENDER), J. Philpot (SAFECARE), and consists of 23 Chapters Published by Now Publishers. It is structured in five parts: Finance, Energy, Healthcare, Communications, Sector Agnostic Topics. It was a collaboration of five (5) Projects:

- FINSEC (9 Chapters)
- DEFENDER (3 Chapters)
- SAFECARE (4 Chapters)
- RESISTO (6 Chapters)
- SPHINX (1 Chapter)

Figure 2 depicts the synopsis of the open access book.


**Figure 2 – The Open Access Book**

The Finsecurity.eu Market Platform is a single-entry point to FINSEC Solutions and promotional channels for the project's results. Recently enhanced with an "Other Sectors" Section destined to present and integrate solutions from other projects. Early Contributors are:

- DEFENDER / Energy
- STOP-IT / Water
- RESISTO / Communications

The FINSEC market platform and third parity solutions are shown in Figure 3 and Figure 4, respectively.

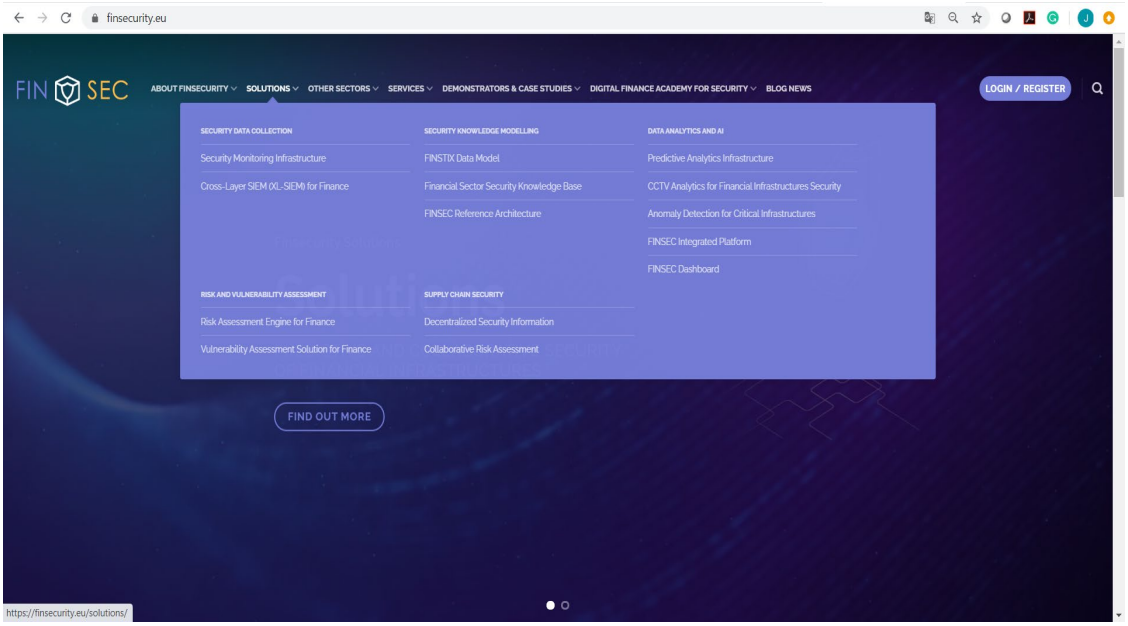


**Figure 3 – The FINSEC Market Platform**

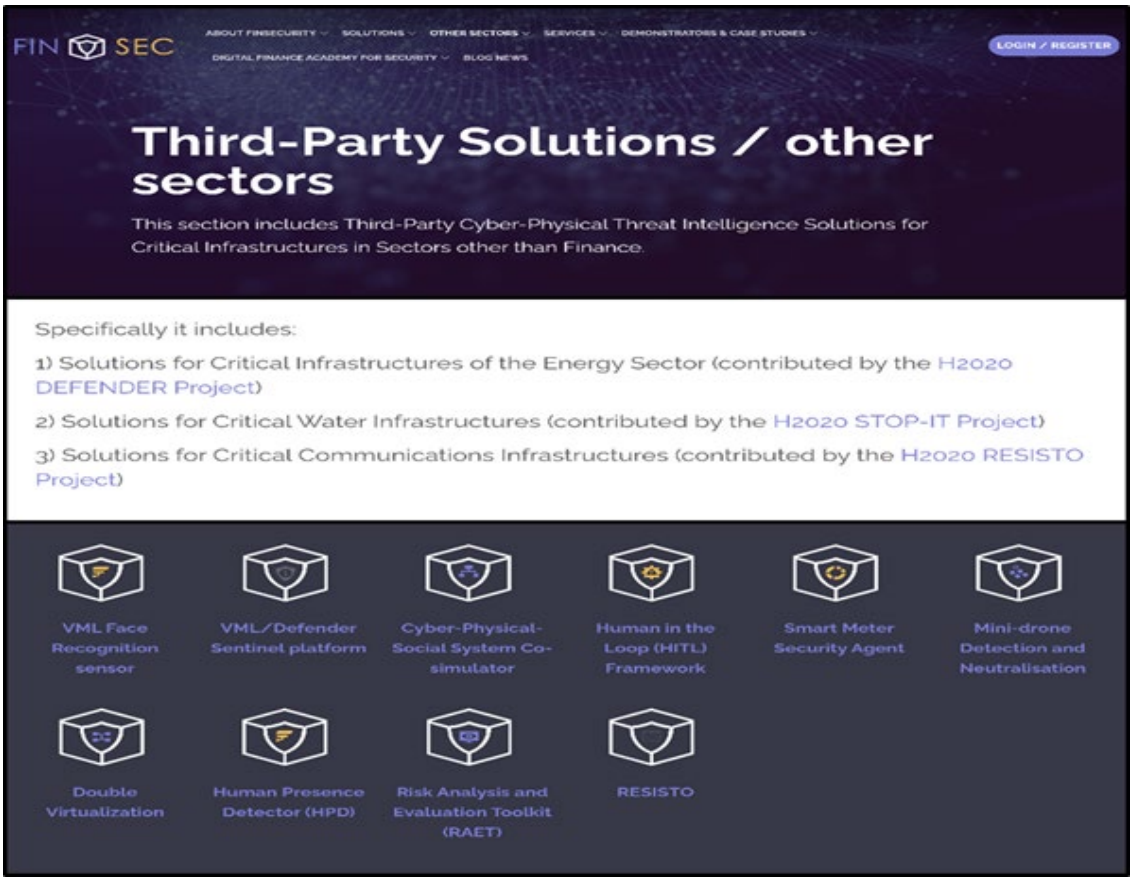


**Figure 4 – Third Party Solutions/Other Sectors**

ECSCI takeaways can be summarized as follows:

- Stimulate the uptake of project results
- Exploit synergies among the projects
- Share best practices
- Stimulate network and alliance formation
- Become a collaborative platform

## 3.3 Critical Infrastructure Protection: Main messages

Critical Infrastructure Protection: Main messages 2020 related to the EU funded research projects and activities, by Aleksandar Jovanović

The contribution was proposing to

1. Ensure that the Critical Infrastructure Protection EU projects and activities have a full portfolio of platforms needed, incl. EXPLOITATION PLATFORM helping to ensure sustainable use of project results beyond the projects' lifetime
2. Ensure right inputs & interaction for/with the new EU directive on critical infrastructures: from "critical infrastructures" to "critical functions"

When doing this, one should address some of the paradoxes of the current safety/security practices in Europe.

- Paradox #1: (Unnaturally) Interrupted RIA/IA way to exploitation
  Market-close results from the EU-project (especially RIA projects with higher TRLs), are regularly developed at the end of the respective projects, but then, there is no time for the "final stretch", no time and money available for prepare real exploitation – the IA projects, at least those running so far, are generally not continuing the work from their RIA-predecessors.

- Paradox #2: Forced merging of different exploitation interests?
  "It feels like we are trying to push water uphill with a garden rake" (approximate quote of one of the industrial leaders coordinating an EU project), referring to try to get the "market oriented engagement" of the partners having no reals role at markets (e.g. academia or state-financed research, or even state-financed end-users); academia and R&D are more interested in new projects than in exploiting the results, and industry is often more interested in protecting these results; the interest in JOINT exploitation often only declarative.

- Paradox #3: A service can be a product, too!
  In EU projects, all prefer to talking about "innovative products" as deliverables, often forgetting that "innovative services" can be an even more useful

- Paradox #4: First response is not and cannot be the only component of a holistic response!
  First response and first responders have been in the focus of most of the projects so far: but that, as e.g. the COVID-19, has clearly shown, "bringing COVID patients quickly to the ventilator" is certainly needed, but not enough to deal with crises; one needs to scan the emerging risks horizon, one needs to look at the recovery and transformation/adaptation after a crisis.

# 4. Keynotes

## 4.1 Critical Information Infrastructure Protection: The role of ENISA in the new EU policy context

Kostantinos Moulinos, ENISA

In recent years, the cybersecurity of critical national infrastructure has become a prominent security concern. To respond to these concerns, the European Union adopted the Network and Information Security Directive in 2016. It is the first piece of EU legislation aimed specifically at improving cybersecurity throughout the Union; a very significant step towards securing the European Union's information systems. ENISA, the European cybersecurity agency, not only plays a major role in the implementation of the NIS Directive but also in supporting the Member States and private sector in achieving a higher level of cybersecurity. It has conducted numerous activities and studies on Critical Infrastructure Protection, IoT, industrial control and SCADA systems and smart grids cyber security, in close collaboration with public and private stakeholders.

## 4.2 Moving towards a trustworthy and resilient European cyber security ecosystem

Roberto Cascella, ECSO

Cyber security is an essential enabling factor for the development and exploitation of digital technologies and innovation and is, therefore, inextricably linked to future prospects for growth, job creation and Europe's response to environmental and societal goals. The significance of cyber security is an ever-growing issue with political, societal and economic implications. The talk will look at the global trends and the challenges for a trustworthy and competitive European cyber security ecosystem and for the creation of secure and resilient infrastructures.

# 5. Project Presentations

Eleven H2020 projects presentations in alphabetical order.

## 5.1 Security and trust assessment in CPS / IOT architectures

ANASTACIA (http://www.anastacia-h2020.eu/): Security and trust assessment in CPS / IOT architectures by Stefano Bianchi

ANASTACIA addressed cybersecurity concerns by researching, developing and demonstrating a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and Cloud architectures (main objective). Since the nature of Cyber Physical Systems (CPS) based on Internet of Things (IoT) and virtualised cloud architectures introduces new and unexpected risks that cannot be completely solved by current state-of-the-art security solutions, ANASTACIA's original concept was built on innovative solutions:

- to build security into the ICT system at the outset,
- to adapt to changing security conditions,
- to reduce the need to fix flaws after deploying the system, and
- to ensure the assurance that systems are constantly secure and trustworthy.

ANASTACIA developed an innovative cybersecurity and privacy framework able to take autonomous decisions on mitigation actions by exploiting **networking technologies** – such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) – **advanced monitoring methodologies and techniques**, and **intelligent dynamic security enforcement**. The proposed framework includes:

- a **security development paradigm**, based on compliance to best security practices and the use of the security components and enablers;
- a **suite of distributed trust and security components and enablers**, able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures;
- a **holistic Dynamic Security and Privacy Seal (DSPS)**, combining security and privacy standards and real time monitoring and online testing.

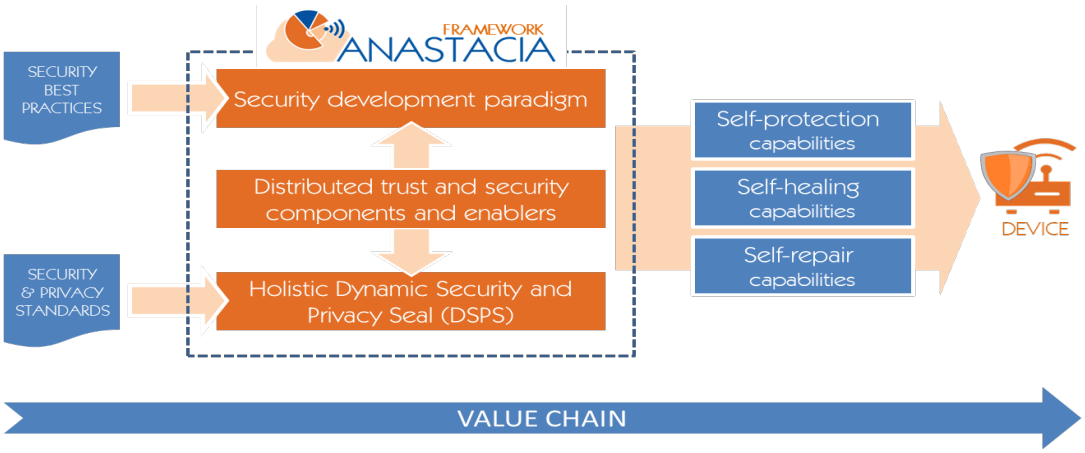


**Figure 5 – ANASTACIA framework summary and associated value chain**

The Consortium efficiently combined innovative IT approaches and business models with security and privacy solutions, creating a security framework where the end users will be able to control their security while privacy policy enforcement and application developers (SMEs in particular) will find an appealing solution for the proper securitization of the managed IoT/CPS architecture.

ANASTACIA completed the **conceptual and architectural model**, thus supporting a complete security management cycle from policy definition to orchestration, enforcement and final deployment of security solutions, based on the integration of SDN/NFV components (the approach has considered SDN/NFV standards and extended solutions for IoT controllers and legacy elements to implement the innovative approach proposed by the ANASTACIA project)

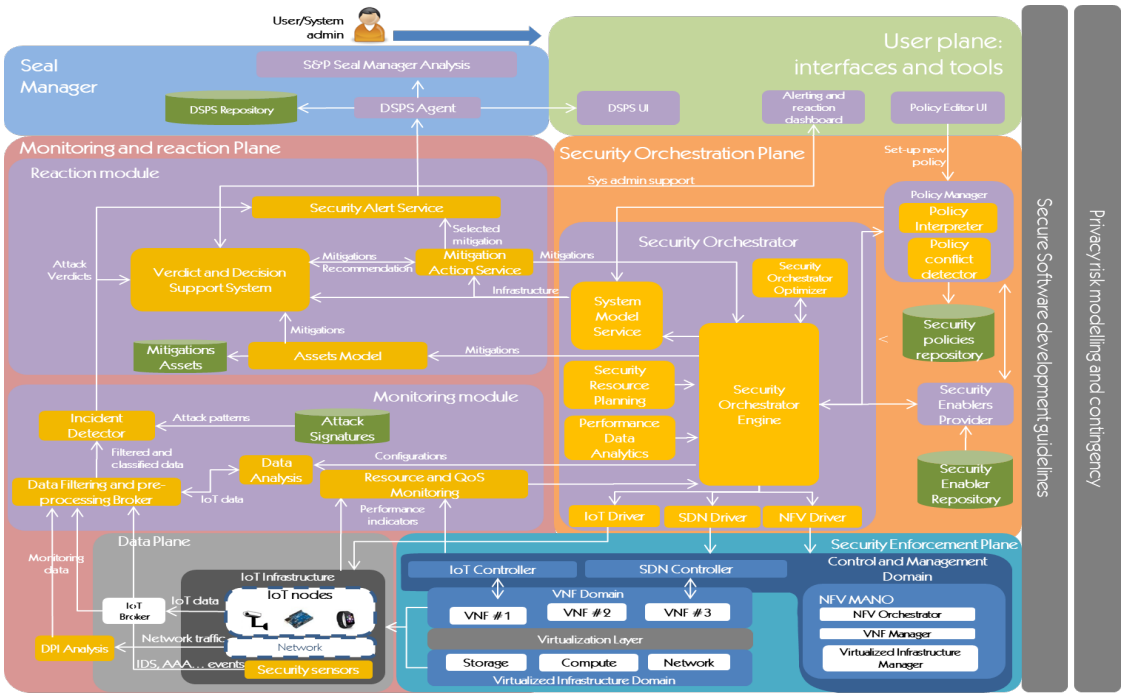


**Figure 6 – ANASTACIA reference architecture**

ANASTACIA designed, developed and integrated **several tools** (and adapted already existing ones) to cope with the different layers of the architecture (see proposed **Key Innovations** and **Key Exploitable Assets** as defined for supporting the joint and individual exploitation plans).

ANASTACIA has completed the conceptual design and the implementation of the **DSPS**, ensuring the integration with other architecture components and completing the functionalities for the envisaged end users – i.e., Chief Information Officer (CIO)/Chief Information Security Officer (CISO) and Data Protection Officer (DPO). Results associated with DSPS (WP5) will soon undergo a **patenting process** to protect IPR and allow joint exploitation by the file proposers (partners MAND, AS and DG).

ANASTACIA has achieved a full level of **integration** of the platform, allowing to setup a live demonstration that was used to assess – with Innovation Advisory Board (IAB) members and stakeholders – the quality of the results proposed to dynamically and proactively react to threats and attacks and provide information on potential issues associated to privacy.

ANASTACIA identified a specific set of **8 Research Challenges (RC)**:

- RC1 – Interoperable and scalable IoT security management
- RC2 – Optimal selection of SDN/NFV-based security mechanisms
- RC3 – Orchestration of SDN/NFV-based security solutions for IoT environments
- RC4 – Dealing with new kind of cyber-attacks in IoT

- RC5 – Learning Decision Model for Detecting Malicious Activities
- RC6 – Hybrid IoT Security Monitoring enhanced with event correlation
- RC7 – Quantitative evaluation of incidents for mitigation support
- RC8 – Developing a Dynamic Security and Privacy Seal which secures both organizational and technical data

To address these challenges the project activities focused to develop and demonstrate a set of 8 Key Innovations (KI) to advance research in holistic IoT cybersecurity and privacy:

- KI1 – Holistic policy-based security management and orchestration in IoT
- KI2 – Investigation on innovative cyber-threats
- KI3 – Trusted Security orchestration in SDN/NFV-enabled IoT scenarios
- KI4 – Dynamic orchestration of resources planning in Security-oriented SDN and NFV synergies
- KI5 – Security monitoring to threat detection in SDN/NFV-enabled IoT deployments
- KI6 – Cyber threats automated and cognitive reaction and mitigation components
- KI7 – Behaviour analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments
- KI8 – Secured and Authenticated Dynamic Seal System as a Service

## 5.2 Energy infrastructure protection

DEFENDER (https://defender-project.eu/): Energy infrastructure protection by Gabriele Giunta, Engineering

Project Number: **740898**

Project Acronym: **DEFENDER**

Project title: Defending the European Energy Infrastructures

Energy sector and in particular the subsector of electrical energy, is a central CI sector and all other CI sectors are interdependent and correlated with this central CI sector. DEFENDER provides new approaches on methodology which explains at high level elementary concepts, methods, principles and rules that enable and govern the process of security in complex electrical energy infrastructure (CEI). Such systems are dynamic, heterogeneous, distributed, discretionary and highly integrated with humans and the environment of their operation. The process of policy, doctrinal and standardization should be flexible, evolvable and dynamically managed to provide enough manoeuvrable space in countering known and unknown threats in this complex security environment.

CEI threats and risks are analysed and classified through: (i) attack trees modelling, (ii) additional approaches to risk assessment methodology and tools to determine and visualize an overall risk exposure/rate and (iii) criteria to assess the risk and classify the CEI assets, systems and segments.

In addition, a modular security architecture to protect the end-to-end CEI from cyber-social-physical accidents, incidents and attacks is designed to obtain a CEI situation awareness, perception and comprehension. Many physical sensors to gather information and drones with cameras have been used as well as cyber sensors, such as combined data from existing IDS, SCADA, Smart Meters and Advanced Metering Infrastructure (AMI), and low-cost Phasor Measurement Unit (PMU). In addition, DEFENDER aims to build a platform for incidents and countermeasures information exchange at a European level. The resulting architectural design has a clear big-data orientation and is managed via a set of state-of-the-art open-source services.

In this context, the Human-In-The-Loop paradigm plays a significant role in CEI security providing information on incidents and accidents that may have cascading effects in CEI operation, given that

their anonymity should be protected. On the other hand, trusted information should be shared from CEI authorities to the public (i.e., citizens, rescue/ security teams) in the vicinity of the CEI installation.

The proposed technological framework could conceptualize the baseline for future understanding of integrating different security technologies in common decision tools which could improve the quality of identification, mitigation and response to complex security threats.

In addition, DEFENDER creates a Culture of Security, where trusted information exchange between trained employees and volunteers will complement cyber-physical protection, while preserving the privacy of the citizens involved. The promotion of the results of DEFENDER at the level of scientific research, with a clear industry focus is one of the main goals of the project.

Finally, within the European legal framework, several desirable and relevant regulatory directives address very similar issues. DEFENDER consortium strongly recommends that the overall policy framework regarding Critical Infrastructure Protection and all related areas, such as cyber security, is reviewed with a holistic approach and focus to decrease the number of regulatory acts to a minimum level appropriate for providing all strategic and operational security environment and processes. DEFENDER experiences and best practices aims at rationalizing the whole EU CIP regulatory picture in order to be sustainable across all the Member States and Companies by applying the principles of "hierarchy" (starting from a general act towards the domain specific one) and "inheritance" (the compliance to part of the framework of higher hierarchy transitively applies also to the following ones with lower hierarchy) and adopting a single format of representations of the relevant information to the relevant EU authorities.

## 5.3 Securing critical financial infrastructure

FINSEC (https://www.finsec-project.eu/): Securing critical financial infrastructure by
Fabrizio Di Peppo, GFT

FINSEC develops and demonstrates an integrated (Physical + Cyber), intelligent, collaborative and predictive approach to the security of critical infrastructures in the financial sector.

FINSEC (Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures) has been conceived for H2020 Programme in Innovation Action submitted to REA (Research Executive Agency) of EC with a duration of 36 months, from May 01, 2018 until April 30, 2021. It is a result of a joint effort of 23 partners with security experts, research centers, technology providers, academia, and financial organizations.

FINSEC considers the critical infrastructures of the financial sector as large-scale cyber-physical systems, which must be protected based on a holistic approach that considers both physical security risks (e.g., robberies, riots, terrorist attack) and cyber-security risks (e.g., malware, ransomware, phishing, DDoS), along with their interrelationships, interactions, and cascading effects across the financial services supply chain. Furthermore, FINSEC introduces, validates, and promotes a predictive and collaborative approach to the security of critical infrastructures in the financial sector.

FINSEC's predictive approach is based on the collection and analysis of security-related data as a means of anticipating security incidents before they actually occur. This predictive approach enables financial organizations to plan for mitigation activities earlier and in the proper context.

At the same time FINSEC's collaborative approach is based on stakeholders' collaboration across the financial services supply chain in the identification, assessment and mitigation of risks, including their cascading effects. FINSEC provides tools that facilitate the collaboration among different organizations.

FINSEC's Reference Architecture (RA) will be available for the systems that will support its predictive and collaborative approach to integrated (cyber/physical) security of critical infrastructures in the

financial sector. This RA is driven by proven security standards, which provides the means for specifying and implementing appropriate security measures and policies. At the same time, it is driven by applicable rules and regulations, as a means of boosting compliance and certification of the critical infrastructures against these regulations. A prototype implementation of the FINSEC RA has been released, based on background technologies of the partners. In particular, a collection of technologies for risk identification, assessment and mitigation has been adapted to the FINSEC architecture and bundled within a security toolbox that will underpin the implementation of the architecture. This implementation is used as a basis for the validation of the project concept in the scope of pragmatic, user driven use cases involving cyber-attacks against popular banking systems (e.g., the SWIFT system, Peer-to-Peer Payment systems, blockchain systems), asymmetric physical attacks against physical assets (e.g., buildings, data centers, ATM networks), as well as their combination.

FINSEC REFERENCE SECURITY ARCHITECTURE MAIN RESULTS

FINSEC introduces a novel, standards-based Reference Architecture (RA) for combined cyber and physical security of critical infrastructures in the financial services industry, as a means of facilitating the implementation, deployment, and wider uptake of security solutions in this sector. The main features of the FINSEC RA will be as follows:

- **Integrated**, as it will consider critical infrastructures as cyber-physical systems, while integrating technologies and measures for cyber and physical security.
- **Standards-based**, since it will be driven by standards for cyber-security and physical security in general (e.g., the ISO 27000 and ISO 28000 family of standards) and financial services standards (e.g., ISO/TC 68/SC 2) in particular.
- **Data Modelling**, FINSEC has introduced an integrated standard-based data model for CIP knowledge in the finance sector, namely FINSTIX, which is based on OASIS STIX. FINSTIX boosts the interoperability and harmonization of different risk assessment platforms and threat intelligence system.
- **Adaptive and Dynamic**, as it will define mechanisms for intelligent and adaptive monitoring and data collection, taking into account the physical or cyber-security context.
- **Anomaly detection and prediction,** family of analytics techniques that learn typical properties of the system and reports significant deviations from the typical system's properties as outliers
- **Collaborative and Participatory**, as the architecture will consider all participating stakeholders allowing them to collaborate in vulnerability assessment, risk analysis, threat identification, threat mitigation and more.
- **Potential Contribution to PSD2**, FINSEC implements a range of tools for security in Open Banking and PSD2 environments, including Auditing and Certification tools, vulnerability assessment tools, as well as relevant Authentication and Authorization services. Based on the use of these tools policy brief for security in PSD2 environments will be prepared.

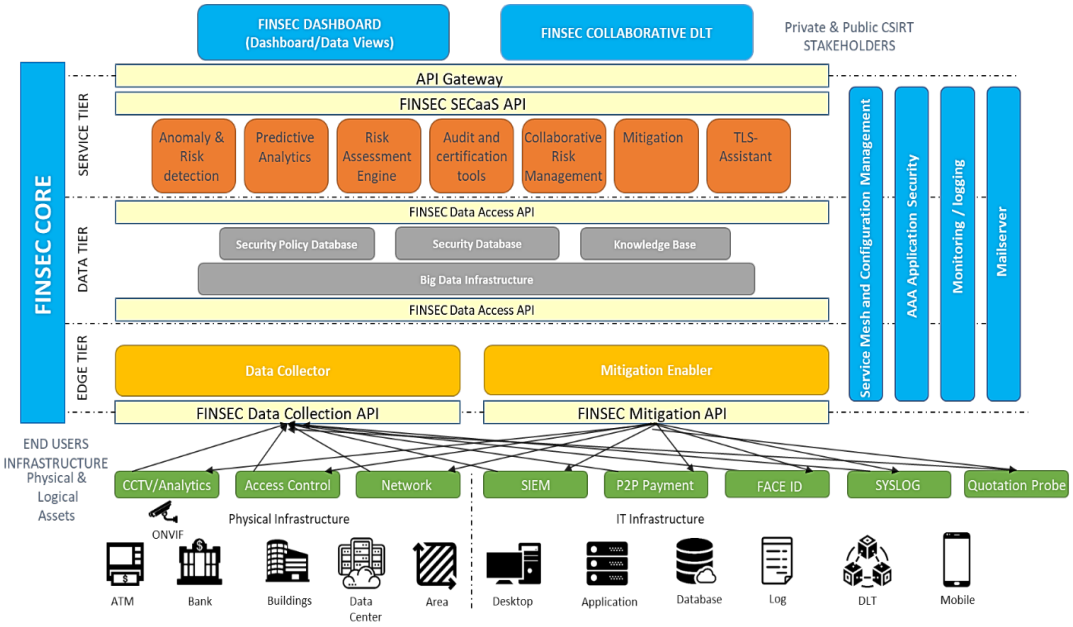


**Figure 7 – FINSEC Reference Security Architecture Main Results**

Hence, the Reference Architecture will represent a blueprint for security systems for critical infrastructures protection within a financial organization, based on an integrated, predictive and collaborative approach.

## 5.4 Improving resilience of sensitive industrial plants and infrastructures

InfraStress (https://www.infrastress.eu/): Improving resilience of sensitive industrial plants & infrastructures by Lorenzo Franco Sutton, Engineering

Project snapshot

- Topic: "Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe"
- Start date: June 1st, 2019, End date: May 31st 2021
- Overall budget: € 10 137 674, EU contribution: € 7 999 623
- Team: 27 partners of excellence from 11 countries

InfraStress addresses resilience and cyber-physical (C/P) security of **Sensitive Industrial Plants and Sites (SIPS)** Critical Infrastructure (CI) to improve resilience and protection capabilities of SIPS exposed to large scale, combined, C/P threats and hazards, and guarantee **continuity of operations**, while minimizing **cascading effects** in the infrastructure itself, the environment, other CIs, and citizens in vicinity, at reasonable cost.

Today, the term "**Critical Infrastructure**" is well known not only to security experts and researchers, but also to European citizens and professionals from many different fields. **Threats and reported attacks** to Critical Infrastructure have recently made it into several headlines in mainstream news. Indeed, we are now much more aware of the importance of those systems and assets, which are vital for running our countries and guaranteeing the key services needed for our everyday lives. However, Critical Infrastructure includes many different **assets and installations** with a great variety in terms of security and safety challenges and including key economic and strategic sectors such as energy, transportation, communication, supply systems, emergency and industrial plants.

Currently, most Industrial Critical Infrastructure (the SIPS we are mainly addressing in InfraStress), have high levels of safety (most are 'Seveso' plants). At the same time, the rise of **the 'digital**

**everywhere' paradigm** (think of how we use our smartphones for almost anything, how our cars have an on-board computer, or our houses are protected by an electronic alarm system), poses new challenges. In particular, the **borderline between physical and cyber security** is thinner and thinner and with so many digital systems and technology diving industrial plants and related infrastructure there is an increased risk of complex, mixed security threats. In InfraStress we aim to have a holistic approach to addressing both physical and cyber threats in SIPS while improving their resilience, minimising cascading effects and actively involving stakeholders, including citizens and communities.

To achieve the above, InfraStress pursues the following technical, scientific and strategic goals:

- **Improve** the **resilience** and the **protection** capabilities of Sensitive Industrial Plants and Sites (SIPS) exposed to large-scale, combined, cyber-physical threats and hazards
- **Guarantee continuity of operations**, while minimizing cascading effects in the infrastructure itself, the environment, other Critical Infrastructures (CIs), and the citizens in vicinity, at reasonable cost
- Improve the resilience of single SIPS, through an adaptive, **flexible**, and **customizable** set of innovative and configurable security measures and tools.
- Enable effective **collaboration** among SIPS operators, in order to impede the propagation of cascading effects.
- Deliver an **open Framework** that allows future evolution to easily integrate additional detection technologies, data feeds, analysis and decision support services, and most importantly to effectively integrate existing solutions already deployed at the SIPS CI side.
- Enable **full exploitation of the technological innovation** potential by supporting a culture of EU SIPS Critical Infrastructure Protection and implementing a human-centric approach that effectively combines decision support and human expertise.

In terms of proposed **innovation**, InfraStress aims to progress the state of the art by firstly concentrating on SIPS, which are generally not the specific focus of current research, or at least not at the level of detail and specificity InfraStress is addressing. Differently from several current approaches, we are addressing **multiple threats and cascading impacts**, in particular by proposing an open, integrated, yet adaptable Framework providing integrated Cyber/Physical situational awareness (based on resilience indicators), supporting effective decision-making across the full CIP lifecycle and support/tools for stress-testing. To this end InfraStress is utilizing and adapting for SIPS innovative capabilities and tools for cyber threats detection. InfraStress also aims to provide not only integrated technological solutions but also foster a **culture of shared collaboration**, participation, and trust in the protection of CI.

## 5.5 Resilience enhancement and risk control for communication infrastructures

RESISTO (http://www.resistoproject.eu/): Resilience enhancement and risk control for communication infrastructures by Bruno Saccomanno

In May 2018, RESISTO project was successfully launched to provide holistic (cyber/physical) situation awareness and enhanced resilience for Communication Critical Infrastructures (CI), that play a fundamental role in the economic and social well-being of the citizens and on operations of most Critical Infrastructures. RESISTO is a three-year EU research project led by LEONARDO (key player in Aerospace, Defence and Security) and co-funded by EU H2020 Research and Innovation Programme. It brings together end users, practitioners, research centres and industries from Cyprus, Estonia, Germany, Greece, Italy, Portugal, Romania, Spain and the United Kingdom.

*RESISTO Architecture*

The logical architecture of RESISTO integrates two control loops both running on top of the Communication Infrastructure and interlinked with each other that implement the five core security

functionalities introduced by the USA National Institute of Standards and Technology (NIST) in the "Framework for Improving Critical Infrastructure Cybersecurity".

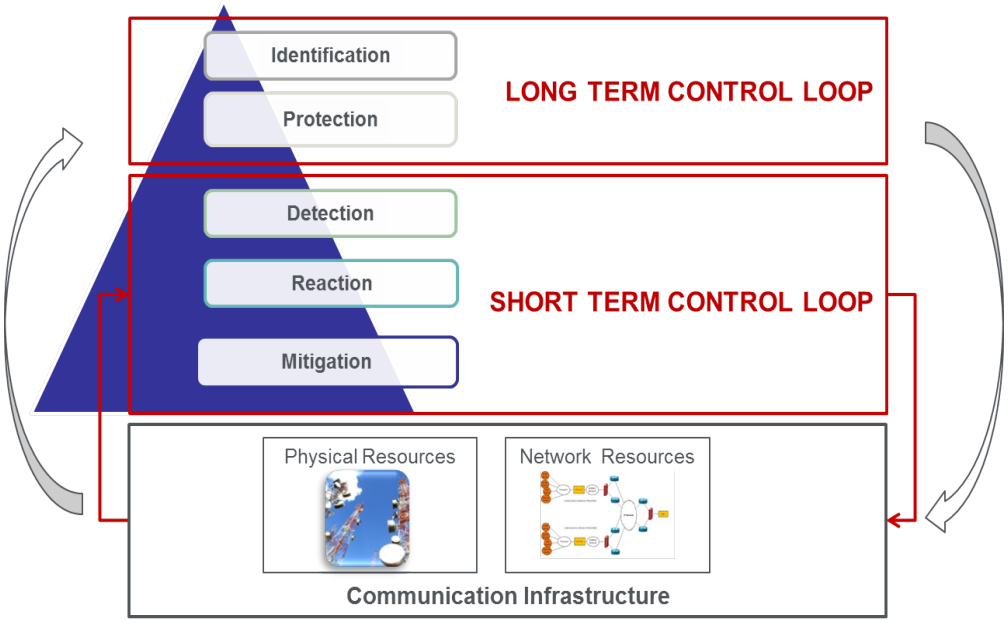


**Figure 8 – The RESISTO Long-term Control Loop and Short-term Control Loop**

The Long-term Control Loop (LTCL) is an offline activity, following a well-defined methodology and supported by advanced tools, aimed to identify infrastructure vulnerabilities and cyber and physical security threats and, consequently, to define asset configuration and interventions to improve CI's resilience and robustness. For each loop cycle, a set of Resilience Indicators (RIs), relevant to critical threat event typologies, are estimated and stored in a Knowledge Base (KB). An LTCL cycle is performed on a periodic basis or when particular events take place (new threats or discovery of previously undetected vulnerabilities). It is typically conducted annually, quarterly, or even monthly.

The Short-term Control Loop (STCL) is the runtime component of the platform. It promptly responds to detected cyber/physical attacks and events that may impact the operational life of the system. It enhances situation awareness and provides operators with a Decision Support System cockpit able to implement the best response to an identified adverse event with the aim of mitigating the event's effects and recovering standard operating conditions.

While facing adverse cyber/physical events, some actual RIs values are measured and stored in the KB. Moreover, LTCL and STCL are strongly interlinked with each other. In fact, comparison between target RIs estimated by the LTCL and their actual values measured by the STCL facing run-time threat events establishes a higher-level global control loop able to continuously review and improve infrastructure resilience and methods.

RESISTO proposes a complete and integrated framework to cover offline Identification and Prevention activities as well as Detection, Response, and Recovery on-line activities. Specifically, RESISTO:

- promotes a unified approach to face physical, cyber, as well as combined physical/cyber threats to Communication CIs to provide a complete situation awareness and impacts evaluation allowing resources optimization and improving recovery actions efficiency.
- encompasses security analysis in a wider Risk and Resilience analysis and management integrating both physical and cyber aspects.
- also includes a wide set of physical and cyber threatening events detectors based on state-of-the-art technologies (Machine Learning, blockchain, etc.); they could be employed in different contexts as stand-alone components as well as in integrated configurations.

Its approach is scalable, developed in the context of Communications but easily applicable to different kinds of CIs. The proposed framework is modular and based on very versatile technologies so easily adaptable to face the continuous evolution of physical and cyber threats and continuously improve the CI resilience.

*Implementation status*

The project has made significant progress both in the use cases definition and user requirements specification - thanks to the significant presence of TELCO Operators - and in all the RESISTO technical solutions, to deliver an innovative platform for optimized decision support in the face of physical, cyber and combined cyber-physical threats, taking account of critical schemes of infrastructures, functions and services and possible (cascading) event trajectories.

In more details, the user requirements have been collected, the main cyber-physical threats have been analysed and, correspondingly, the possible countermeasures identified. At the same time, an in-deep assessment of existing key performance indicators has been carried out in order to select the most suitable ones. The mitigation/reaction engines have been designed and their ability to adapt to the different scenarios analysed.

The resilience concept has been evaluated in more detail, by improving and adopting awareness tools (i.e., penetration test) specialized for the communication scenario by also taking into account, since the initial assessment phase, the available resources. At the same time, current efforts are devoted to measuring the resilience of systems.

After the use cases definition and user requirements specification, all the platform components are almost completed and we are setting up the integration environment (in the Cloud) to test the core applications: it will be shortly interfaced to the testbeds at Telco Operators premises (Telecom Italia Mobile, British Telecom, Hellenic Telecommunications Organization, Orange Romania, Retevision, Altice Labs), in order to perform the end user validation of the platform, in the three planned scenarios - current Telco Infrastructures, interconnected Critical Infrastructures, future 5G Telco Infrastructures - in order to show the first real results.

We are on the right path to help Communications Infrastructures Operators to take the best countermeasures and reactive actions, exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domain by RESISTO the physical security operators and the cyber security experts will finally work together.

## 5.6 Safeguarding critical health infrastructure

SAFECARE (https://www.safecare-project.eu/): Safeguarding critical health infrastructure
by Philippe Tourron and Isabel Praça

The goal of SAFECARE is to bring together the most advanced technologies from the physical and cyber security spheres to achieve a global optimum for systemic security and for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects. The project focus on health service infrastructures and will work towards the creation of a global protection system, which will cover threat prevention, detection, response and, in case of failure, mitigation of impacts across infrastructures, populations and environment. SAFECARE proposes and demonstrates 13 innovative elements, which will optimise the protection of critical infrastructures under operational conditions. These elements are interactive, cooperative and complementary (reinforcing in some cases), aiming at maximising the potential utilisation of the individual elements.

SAFECARE architecture and innovation elements

SAFECARE includes a set of modules with physical and cyber solutions that are integrated through a data exchange layer and deliver a set of tools combining cyber and physical security awareness like: a Threat Response and Alert system, an Impact Propagation and Decision Support tool, a Risk Management Module and a Hospital Availability Management System.

The physical security layer brings modules as the Suspicious Behavior Detection System, Intrusion and Fire detection system, Ubiquitous services for integrated alert system, and a Data Collection from physical sub-systems that are integrated into a Building Threat Monitoring System. The building monitoring system will centralise security events from the suspicious behaviour detection system, intrusion and fire detection system, access management system, air cooling system, power supply system. It will allow building security agents to monitor physical assets on a building representation and it will give access to the video streams. The building monitoring system will also have the ability: to report security events on physical assets; to manage manual acknowledgement of security events; to forward acknowledged incidents to the central database; to set rules based on related impacts coming from the central database; to trigger response and mitigation plans concerning the impacts.

The set of cyber solutions includes an IT Threat Detection System, an Advanced File Analysis system, an OT oriented threat detection system and analytics tools to improve cyber security, and a medical security analytics module. These modules are available through the Cyber Threat Monitoring System. The cyber threat monitoring system collects cyber security events from multiple security assets: probes, IDS, IPS, SIEM, firewall. It mainly focuses on threat detection and incident response along the crisis lifespan.

The database and data exchange layer will be designed to standardize data exchange between the different project bricks. Incidents stored in the database will be previously validated by security operators (building security agents or SOC operators), thus reducing the amount of false positive alerts. By implementing standardized data models, by implementing relevant processes (correlation between incidents, impacts and responses), the central database will return relevant data and optimize decision support. Furthermore, work on the standardized exchange layer will pave the way for interconnected health services to improve security and defence strategies at national and European level. The analysis and comparison of individual scenarios, in three different European sites, will provide additional information about the behaviour of different environments in healthcare structures across Europe. Information coming from the three scenarios evaluation, via the platform, will allow security staff to positively impact the security of their facilities and, above all, the people in their care.

Figure 9 illustrates the global architecture of SAFECARE and how the different modules are integrated.

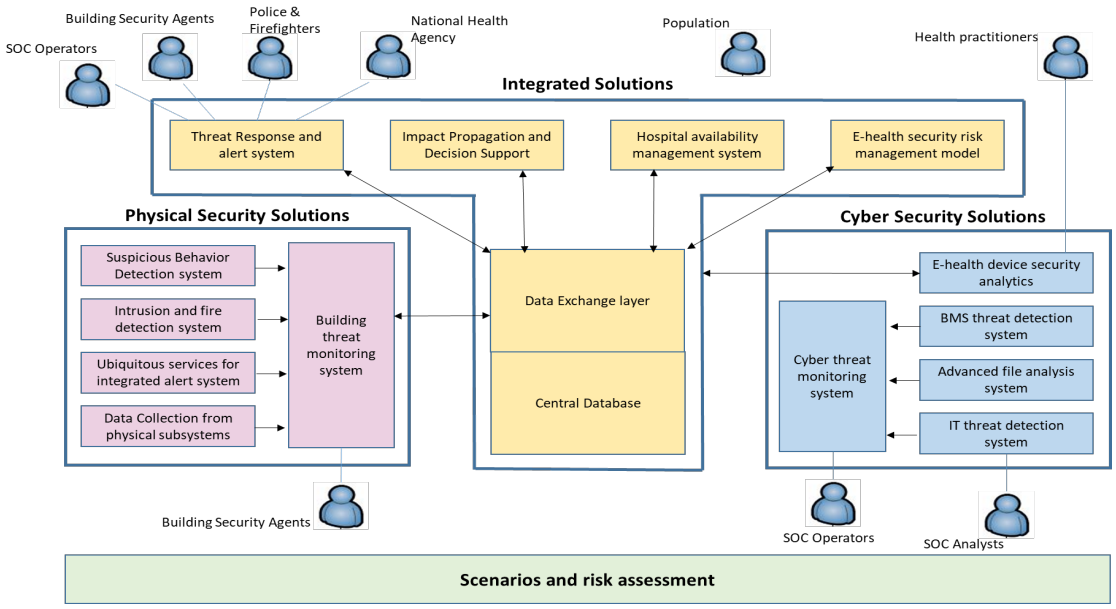


**Figure 9 – SAFECARE global architecture and interconnections**

A simulation platform is built on the top of Airbus CyberRange, where all solutions are integrated, and the threat scenarios will be tested prior to their demonstration on the hospital pilots. Following the demonstration step, 3 demonstrations in 3 different countries will be carried out in the hospitals:

A full pilot project will be deployed in the AP-HM (Assistance Publique des Hôpitaux de Marseille), located in 80, rue Brochier 13005 Marseille. AP-HM offers the highest standards of clinical skills and nursing care. 2,000 physicians are committed to providing excellent and accessible health services to everyone within a full range of specialties and advancing care through pioneering hospital-based research programs and educating future healthcare professionals with the University School of Medicine.

A quasi-full pilot project will be deployed in the ASLTO5 (Azienda Sanitaria Locale Torino 5) three hospitals. ASLTO5 Local Public Healthcare Provider in Piedmont, is serving 310,292 citizens (continuously increasing year by year) in 40 municipalities, with 35 facilities interconnected in an area of 600 square kilometers, South-East of Turin metropolitan area. ASLTO5 is divided in four administrative healthcare districts and includes three hospitals (Chieri, Moncalieri e Carmagnola).

The issue of safety of medical devices will be tested and demonstrated in the Academic Medical Centre, University of Amsterdam in the Netherlands (AMC).

The AMC is the first university medical centre of the Netherlands and currently the second-largest one.

## 5.7 Security of air transport infrastructure of Europe

SATIE (https://satie-h2020.eu/): Security of air transport infrastructure of Europe
by Kelly Burke, DGS S.p.A

Airports are among the most complex and largest systems and are recognized as critical infrastructure when it comes to the security of society. Airports are actually system-of-systems, though. For example, the Flight Information Display System that passengers view is composed of various systems together: the public announcement system, the airport database, the baggage handling system, and others which all contribute to the one function. With this complexity, airports are extremely data driven. They rely on accurate and timely information for efficient operation, they utilize seamless information

exchange across integrated systems, and support real-time decision-making for the benefit of all aviation stakeholders. This increased connectivity has enabled airports to manage resources more efficiently, overcome irregular operations faster, and avoid disruptions. However, increased reliance on data and increased integration also increases the risk of malicious cyber-physical attacks that can disrupt and bring airport operations to a halt.

The number of cyber-attacks is increasing each year and cost up to €1M/hour for disruptions at major European airports, along with the fact that the average time to detect a malicious or criminal attack is 170 days, with 90% of large organizations reporting a security breach at some point. Therefore, it is vital to the successful operation, financial outcome and potential safety of all people involved, for airports to avoid cyber- and physical-security breaches as much as possible. While airports have cyber-security teams these days and specialized personnel, because of the complexity of the stakeholders involved and the complex system-of-systems, there does not exist a method to bring together data and information from physical assets as well as from cyber assets and to use correlation approaches and quickly and easily detect a potential threat, even sharing necessary situational awareness information to security personnel and first responders.

Therefore, it is SATIE's goal to improve the correlation of cyber- and physical threats to facilitate human analysis and decision-making. Demonstrations will be carried out at TRL7 in five realistic complex cyber-physical threat scenarios at three international airports across Europe, which include varying subsets of different airport operations: the Flight Information Display System, the Baggage Handling System, the Baggage Registration Service, the Airport Operation Center, the Public Announcement system, passenger control, passport and border control, the airport operation database, resource management system, and gate management and stand allocation. SATIE will demonstrate an efficient and cost-effective solution to improve dynamic airport security standards.

SATIE adopts a holistic approach about threat prevention, detection, response, and mitigation in the airports, while guaranteeing the protection of critical systems, sensitive data and passengers. Critical assets are usually protected against individual physical or cyber threats, but not against complex scenarios combining both categories of threats. In order to handle it, SATIE develops an interoperable toolkit which improves cyber-physical correlations, forensics investigations and dynamic impact assessment at airports. A shared situational awareness can help security practitioners and airport managers to collaborate more efficiently to the crisis resolution. Emergency procedures can be triggered simultaneously through an alerting system to reschedule airside/landside operations, notify first responders, cybersecurity and maintenance teams towards a fast recovery.

At this point, the project is around the half-way point. The platform on which the toolkit will be built is ready, with each SATIE tool deployed. The combination of tools included gathers data from the various systems and puts them together in an intelligent manner to better correlate anomalous data or coincidental incidences which could indicate a potential threat occurring. The tools include a vulnerability management system, risk assessment, threat impact propagation, a business process intrusion detection system, secured IoT communication on the baggage handling system, secured air traffic management data services, among others. Preliminary assessments have been performed, including a gap analysis, harmonization of security procedures across the airports, a preliminary risk assessment, an ontology developed for inter-system operability, threat propagation model templates created, technical tests of each tool on the platform, and the validation plan is being created to ultimately evaluate the usefulness and usability of the tool for Security Operations Center and Airport Operations Center personnel.

Innovative solutions will be integrated on a simulation platform to improve their interoperability and to validate their efficiency. Then the three demonstrations will be conducted at different corners of Europe (Croatia, Italy and Greece) in order to evaluate the solutions in operational conditions. Results and best practices will be widely disseminated to the scientific community, standardization bodies, security stakeholders and the aeronautic community. Finally, SATIE paves the way to a new generation of Security Operation Centres that will be included in a comprehensive airport security policy.

## 5.8 Securing the European gas network

SecureGas (https://www.securegas-project.eu): Securing the European gas network
by Ilias Gkotsis, KEMEA

SecureGas focuses on the 140.000 km of the European Gas network covering the entire value chain from production to distribution to the users, providing methodologies, tools and guidelines to secure existing and incoming installations and making them resilient to cyber-physical threats. Three business cases (including upstream, midstream and downstream facilities) addressing relevant issues for the Gas sector, have been identified so that they ensure the delivery of solutions and services in line with clear needs and requirements, focused on: risk-based security asset management of gas transmission and distribution networks; impacts and cascading effects of cyber-physical attacks on interdependent and interconnected European Gas grids; integrity and security, through the operationalization of resilience guidelines, of strategic installations across the EU Gas network.

SecureGas tackles these issues by implementing, updating, and incrementally improving extended components, integrated according to a High-Level Reference Architecture (HLRA) built upon the SecureGas Conceptual Model; a blueprint on how to design, build, operate and maintain the EU gas network, in terms of cyber and physical security and resilience. These components include the following technologies

a) Situational Awareness and Decision Support
b) Information processing and management
c) Detection, identification and early warning
d) Joint cyber-physical security risk management and resilience modelling

All SecureGas extended components are contextualized, customized, deployed, demonstrated, and validated in each business case, according to the scenarios defined by the end-users. Related services provided by SecureGas will be offered to the end-users via a Platform as a Service (PaaS), that allows modularity, flexibility, cooperation, and third-party interoperability, thus securing a long-lasting impact, supporting the project exploitation strategy.

A multidisciplinary consortium (Gas operators, technology providers, research institutions, sector-related associations), supports the project implementation across Construction, Demonstration and Validation phases, as well as a Stakeholder Platform (including Gas CIs, Energy companies, Public and Regulatory Authorities, etc.) ensures inputs, advise, and a wider Diffusion of the project outcome, focusing on replication opportunities on other CIs and concepts, and significant contribution in policy making procedures.

## 5.9 Resilience of Smart Critical Infrastructures

SmartResilience (http://www.smartresilience.eu-vri.eu/): Smart Resilience Indicators for Smart Critical Infrastructures (DRS14, 2016-2019) by Aleksandar Jovanović, Risk-technologies

**The challenge:** Modern critical infrastructures are becoming increasingly “smarter” (e.g., cities). Making the infrastructures “smarter” usually means making them smarter in normal operation and use: more adaptive, more intelligent. But will these smart critical infrastructures (SCIs) behave equally

"smartly" and be "smartly resilient" also when exposed to extreme threats, such as extreme weather disasters or terrorist attacks? If making existing infrastructure "smarter" is achieved by making it more complex, would it also make it more vulnerable? Would this affect the resilience of an SCI as its ability to anticipate, prepare for, adapt, and withstand, respond to, and recover?

**Project Objectives**: In order to match the challenge, the project has pursued the main objectives including (a) identifying existing indicators suitable for assessing resilience of SCIs, (b) identifying new "smart" resilience indicators (RIs) – including those from Big Data, (c) developing a new advanced resilience assessment methodology based on smart RIs, (d) developing the interactive "SCI Dashboard" tool, and (e) applying the methodology/tools in 8 case studies, integrated under one virtual, smart-city-like, European case study.

**Results:** The project has collected, analysed and produced a large set of 5,000 "classic" and the smart big/open data-based resilience indicators, defined the indicator-based methodology for assessing, monitoring and predicting resilience of the infrastructures and applied the methodology in 27 large infrastructure case studies, including health system (e.g., 122 hospitals in Austria), energy and water supply, transportation networks, etc. The project has significantly improved the possibilities to assess and manage resilience of critical infrastructure, within a holistic approach, including human factors, and societal and economic aspects. SmartResilience will therefore provide solutions that are suitable to enhance the societal resilience in European countries and the organisational resilience among European infrastructure providers.

**Assessing resilience practically:** The SmartResilience project provides a new methodology to cope with possible adverse scenarios/events that can potentially lead to significant disruptions in its operation/functionality. Examples of scenarios are, for instance, terrorist attacks stopping airport operation or cyber-attacks destroying the financial systems. Coping with these scenarios means preparing for them, being able to absorb/withstand their impacts, recovering optimally from their impacts and adapting to the continuously changing conditions. In practice, an end-user essentially wants to know answers to those questions and can reach these answers by following the resilience assessment workflow to create their own case study. The resilience assessment result is the "Resilience Level" (a number) that allows to compare one infrastructure with other infrastructures (do the "benchmarking") and/or to monitor changes in resilience over the operation time. This part of the assessment normally does not concern any particular scenario but covers issues and indicators applicable in general. The resilience level can be monitored in operation time and/or compared among different infrastructures, as well as during the course of the adverse/disruptive event ("scenario time"), the result showing the functionality of the infrastructure after the event, e.g., "as before", "better", "worse" or "lost". (Figure 10).

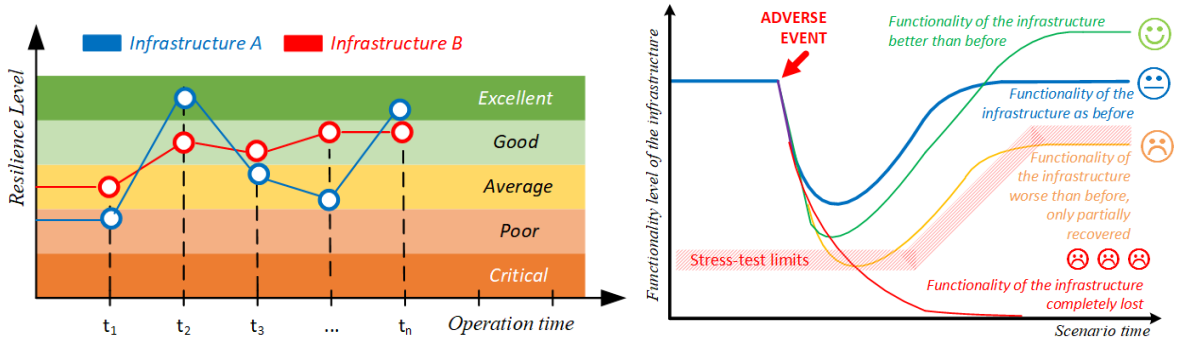


**Figure 10 – Assessing resilience over operating time (l) and during an adverse event (r)**

SmartResilience allows to look at interdependencies between infrastructures to understand how, in a case of a problem on one of them, the functionality of the others can be impacted. The assessment is based on issues and indicators: the issues and indicators that are shared by different infrastructures

indicate lines of interconnectedness and interdependency (Figure 11). The same type of the assessment can be done in order to check if the behaviour of the infrastructure is within the prescribed limits, e.g., the loss of function smaller than the maximum allowed, e.g., following the stress-test definition. Finally, it allows optimizing the resilience decision-making: e.g., for the case when various "resilience improvement portfolios". Different criteria can be taken into account (e.g., implementation time, cost, robustness improvement), but the main one is the Resilience Level Improvement (RLI).

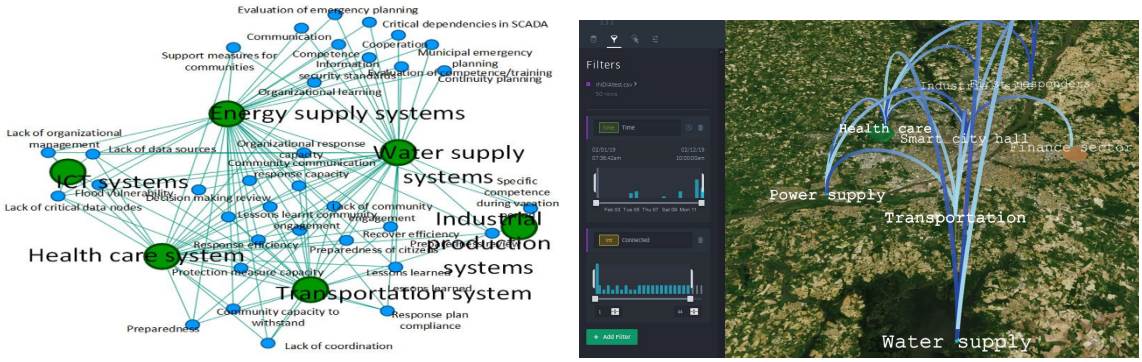


**Figure 11 – Modelling and visualizing interdependencies among SCIs in SmartResilience**

**Standardizing approach and using results beyond the project:** The project approach is being embedded in the new ISO 31050 ("Managing emerging risks in order to enhance resilience"). The project results and the ResilienceTool have stayed available, free of charge for the registered ERRA members, also after the project end, and the concept and the tools are developed further in the project InfraStress.

## 5.10 Cyber-security protection in healthcare IT ecosystem

SPHINX (https://sphinx-project.eu): Cyber-security protection in healthcare IT ecosystem
by Evangelos Markakis, Hellenic Mediterranean University-HMU

On behalf of SPHINX H2020, Dr. Evangelos Markakis presented the main scope of SPHINX that aims to introduce a health tailored Universal Cyber Security Toolkit, thus enhancing the cyber protection of the Health and Care IT Ecosystems and ensuring patients' data privacy and integrity.

Hospitals and Care Centres are prime targets of cyber criminals, especially concerning data theft, ransomware, man-in-the-middle and phishing attacks. This reflects the need of Healthcare Institutions for a Holistic Cyber Security vulnerability assessment toolkit (Markakis et all.), that will be able to proactively assess and mitigate cyber security threats known or unknown, imposed by devices and services within a prorate ecosystem.

SPHINX aims to introduce a Universal Cyber Security Toolkit, thus enhancing the cyber protection of Health IT Ecosystem and ensuring the patient data privacy and integrity. It will also provide an automated zero-touch device and service verification toolkit (Nikoloudakis et al.) that will be easily adapted or embedded on existing, medical, clinical or health infrastructures.

The SPHINX Toolkit will be validated through pan-European demonstrations in three different scenarios at different countries (Romania, Portugal and Greece). Hospitals, care centres and device manufacturers participating in the project's pilots will deploy and evaluate the solution real-life situations and emergency situations across various use case scenarios.

## 5.11 Protection of critical water infrastructures

STOP-IT: Protection of critical water infrastructures by Rita Ugarelli, SINTEF

The ultimate goal of STOP-IT project is to 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.

The delivered technologies and solutions are scalable, which might be adopted from small utilities to large ones; adaptable, including various modules addressing different needs, with expandability for future modules; and flexible, which means that the water utility managers can decide how to use it and it can be exploit by different user's profiles e.g., by experts, novices, and even non-technical staff.

The STOP-IT solutions are integrated in the STOP-IT fully operational and technically evaluated platform in the form of 9 modules designed to cover most of the utilities' needs. The high variety of modules provide solutions to real-time operational needs and decision making, but also supports strategic/tactical planning and post action assessment (Figure 12).


**Figure 12 – Conceptual visualization of the integrated STOP-IT platform**

At strategic and tactical level, the project has developed Module I, including the comprehensive Risk Analysis and Evaluation Toolkit (RAET); consolidated a cyber-physical risk management ontology to link risks, consequences and their corresponding mitigation actions; and provided also an organizational stress testing platform, in the form of a board game, to stress test the level of preparedness of water utilities in case of crisis management. The RAET gives access to several integrated components supporting the water utilities in performing a complete risk management process at strategic/tactical level (Figure 13) (see also 7.1.1 below).

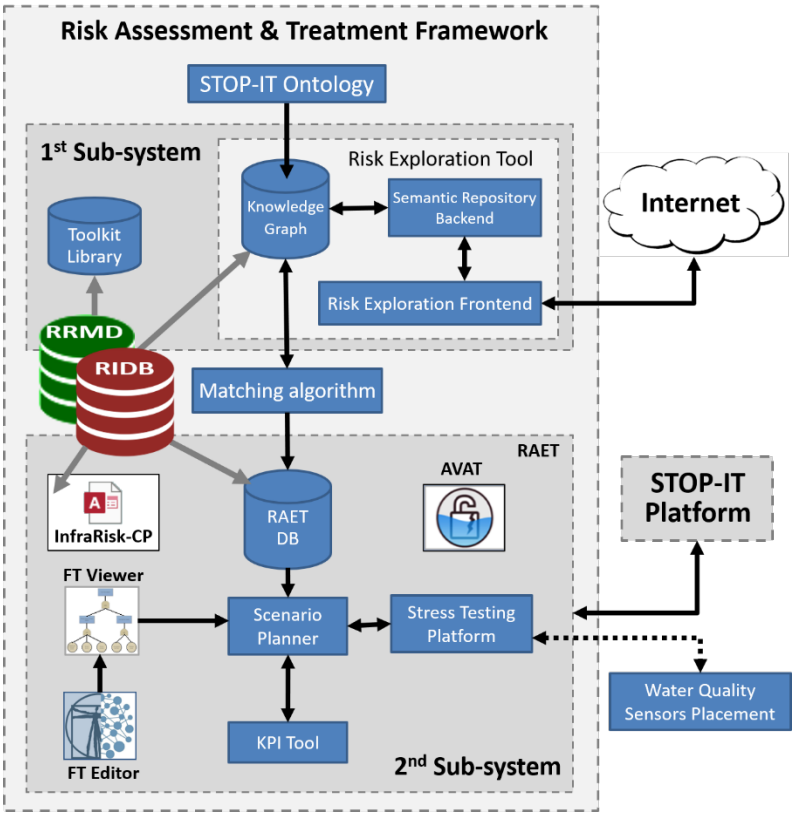


**Figure 13 – The STOP-IT Risk Assessment and Treatment Framework integrated solutions**

At operational level, the project has provided innovative solutions for risk treatment (prevention, detection, mitigation, and recovery) of water CIs (see also section 7.10). The range of the proposed protections schemes has been broad and comprehensive covering the full spectrum, from communications to IT and SCADA systems and to physical protection. These solutions are: the Module II, designed as a jammer detection with improved functionalities; solutions for the "IT and SCADA security" including (Module III): the Fault-tolerant Control Strategies for Physical Anomalies affecting the SCADA system (FTCS), the Network Traffic Sensors and Analysers (NTSA) and the Real-Time Sensor Data Protection (RSDP); solutions for "physical protection of water infrastructure" comprising (Module IV): the Access Control System using Electronic Locks (Smart Locks), the Computer Vision Tools (CVT), the Fine-grained Cyber Access Control (FCAC), the Human Presence Detector (HPD) using WiFi signals and the Water Quality Sensor Placement Tool; Module VI, providing the Real-time Anomaly Detection System (RTAD and XL-SIEM), and the Module V Cyber Threat Sharing System (Figure 14).

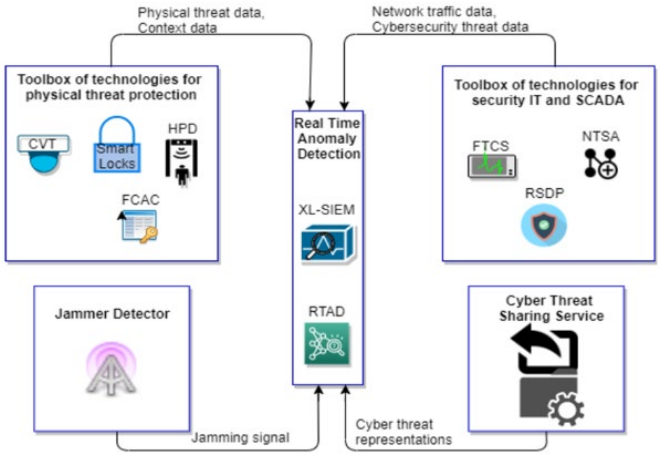


**Figure 14 – The STOP-IT solutions at operational level and their interaction**

Further, the project has produced Module VII, the Public Warning Notification System; Module VIII, the Reasoning Engine and Module IX, the Enhanced Visualisation Interface for Water Utilities.

STOP-IT solutions are co-created and demonstrated through a front-runner/follower approach where 4 advanced utilities, Aigües de Barcelona (ES), Berliner Wasserbetriebe (DE), MEKOROT (IL) and Oslo VAV (NO) are twinned with 4 ambitious ones to stimulate mutual learning, transfer and uptake (EMASAGRA (ES), Hessenwaser (DE), Bergen City (NO) and DeWatergroep (BE)).

But STOP-IT is not only about technologies, but also collaboration and training.

To contribute to the development of the project products, with a multi-stakeholder perspective, three levels of Communities of Practice (CoPs) have been launched to ensure the required levels of confidentiality for the information to be exchanged and with different roles in the project:

- Local CoP: one for each of the 4 water utilities involved Front Runner (FR), treating technical aspects in a confidential environment; they involve selected actors for each of the FR cases (water utility operators, the associated technical solutions providers and the R&D experts);
- Project CoP: designed to establish a network of different groups of stakeholders on the project and open to a broader audience (i.e., FL water utilities, national water associations, first aid associations);
- Trans-project CoP: crossing boundaries between different CI sectors, involving international networks and non-project expert groups (the ECSI cluster is an example of the result of the Trans-project activities).

To ensure the development of sound solutions, all the STOP-IT technologies are tested and validated by the Front Runner (FR) operators, with the involvement of different users (security officers, terminal operators, facility operators, associated technology providers, and more) through interactions, and feedback loops, with the technology developers.

Building on this solid basis STOP-IT also delivers high impact through the creation of hands-on training and best practice guidelines, contributes to policies on critical infrastructure protection, as well as by fostering market opportunities, leveraging the EU water technology platform's multi-stakeholder network.

# 6. Round tables and Panel Discussions

## 6.1 Artificial Intelligence

Artificial Intelligence for Securing Critical Infrastructures by John Soldatos, Innov-Acts

The panel was focused on the use of Artificial Intelligence (AI) for Critical Infrastructure Protection (CIP). It consisted of a short introduction and four target interventions on AI related topics. The introductory presentation set the scene for AI in CIP: It presented the potential benefits (i.e., automation, speed, discovery of hidden patterns of security and resilience) and sample use cases (e.g., AI for Intelligent Access Control, AI for Intelligent Perimeter Protection, AI for Predictive Maintenance of physical assets, Cyber-Physical Threat Intelligence, Safe Production). However, it also discussed why AI for CIP is challenging with emphasis on the lack of data for training algorithms, the transparency and trustworthiness of the AI systems, and the lack of a digital/AI culture inside security organizations.

The three thematic presentations that followed presented AI security use cases on the following areas:

- Predictive Analytics for Cyber-Physical Threat Intelligence (CPTI) in the Financial Sector. This presentation outlined the algorithms used, the benefits validated, and the challenges faced when applying predictive analytics for CPTI in the context of the FINSEC project. The presentation was given by John Soldatos (FINSEC Project).
- Situational Awareness for Critical Infrastructures with emphasis on ensuring long-term resilience. The presentation was given by Alexander Jovanović (CEO/Director of Steinbeis Advanced Risk Technologies (R-Tech) and lead contributor to various projects/initiatives like SmartResilience, InfraStress, Encircle and ISO 31050).
- Resilience of critical infrastructures (such as railway networks) against natural hazards. The presentation was given by Mauro Rossi from CNR, who presented a practical case of the use of machine learning for image analysis towards anticipating and managing natural hazards in Italy, including planning of proper response.

## 6.2 ELSI – Ethical, legal, and social implications of project

Ethical, legal, and social implications of projects by Sylvia Bach (University of Wuppertal)

During the ELSI Round Table ELSI, we heard about the approaches of three projects to this topic: DEFENDER, FINSEC and RESISTO. Afterwards, there was a short, but lively discussion between the panellists. The topic raises interest and awareness and is surely one not to be overlooked in a project.

RESISTO

In RESISTO, there are two pillars for addressing and monitoring ethical and societal impacts of the project. First, work package 11 concludes all guidelines and templates for the consortium to work with. This includes templates for the informed consent and information sheets as well as opinions / approvals of ethics committees (or other competent authorities) on the research with humans. Each member of the consortium had to announce a Data Protection Officer and had to check if a declaration on compliance for collecting and processing personal data is needed. A DPIA (Data Protection Impact Assessment) had to be carried out, as well as a risk assessment on measures to prevent the misuse of the research findings throughout the project.

Additionally, there were pre-grant requirements the consortium had to fulfil regarding specific tasks that might have ethical or data protection issues.

Secondly, there is an ethical monitoring process implemented in the project, as part of WP 1. When starting a task, the task leader has to answer a short survey regarding data protection and ethical impact of the specific work planned. After having finished the task, a second survey monitors if the planned work went accordingly or if other issues might have occurred.

In the case of any issues – mentioned in the first OR second survey, the SSHERC (Social Sciences, Humanities and Ethical Review Committee) of RESISTO would react and provide the consulting needed to carry out the research according to the law and all internal guidelines.

Also, there was a public survey launched to get an idea about the impact of a communication service breakdown on a personal level. Even though this survey will not hold representative results, it will hopefully be interesting to compare the results from the different countries, because it has been shared via the consortium members spread throughout Europe.

DEFENDER

Over the past decade, there have been unprecedented advancements in the field of computer vision by adopting AI-based solutions. In particular, cutting-edge computer vision technology based on deep-learning approaches has been deployed with an extraordinary degree of success. The ability to extract semantic concepts from continuous processing of video stream in real-time has led to the investigation of such solutions to enhance the operational security of critical infrastructure against intruders. Despite the success of computer vision technologies validated in a laboratory environment, there still exist several challenges that limit the deployment of these solutions in operational environment. To facilitate the adoption of computer vision technologies for enriching security, the DEFENDER project has developed an advanced framework relying on the integration of key technical innovations that satisfies the operational requirements of critical infrastructure. One such requirement relates to data privacy and citizen rights, following the implementation of General Data Protection Regulation across Europe for the successful adoption of video surveillance for infrastructure security. The video analytics solution developed in the project, integrates privacy preserving technologies, high-level rule engine for threat identification and a knowledge model for escalating threat categories to human operators. The various components of the proposed framework have been validated using commercially available graphical processing units for detecting intruders

# 7. Thematic Presentations

## 7.1 Physical and Cyber security integration and modelling

### 7.1.1 Applied to WATER critical infrastructure

Christos Makropoulos, ICCS/NTUA, Greece

Every vital sector of organized societies, such as energy, water, waste, healthcare, transportation or communication and other industries, relies on Critical Infrastructures (CI) to continuously and safely produce and distribute services as designed. Recent advances in the information and communication technology (ICT) sector, networked machines, and Internet of Things (IoT) created a “fertile soil” for the digital transformation and allowed CIs to evolve by merging physical processes with computational systems and form new, cyber-physical systems (CPSs) (Lee, 2008). In that hybrid architecture, the physical operations are monitored and controlled by a networking/computing core through feedback loops between the layers. However, as the physical systems harvest the potentials of the digital transformation, they inherit the vulnerabilities as well, creating new risk sources for adversaries to exploit. With access to a range of malwares and tools through the Darknet, attacks beyond the adversary’s actual know-how are possible, while more advanced cyberattacks can manipulate the system design and infringe upon the physical domain through communication or computational infrastructures, thereby evolving into cyber-physical threats (Moraitis et al., 2020). The systems, thus, by progressively relying on the intricate interplays between the cyber and the physical domains to efficiently achieve objectives in their daily operations, have expanded their attack surface to include cyber-physical threats like denial of service (DoS) attacks, hacking, data manipulation and sabotage. As a result, the models and tools used to simulate and represent the system behaviour based solely on the physical layer operations, are no longer valid. As the two domains are no longer isolated, continuing to think and treat them in silos can lead to misguided perceptions over the system’s security and resilience, with potentially heavy impacts.

Adopting this principle for critical water infrastructures, in the context of the STOP-IT project (see also section 5.11), we argue that since the cyber and physical systems interact continuously, and cascading effects between them are not easy to track (or back-track to improve designs or identify sources of attacks) we need to combine cyber and hydraulic engineering knowledge to develop novel cyber-physical security concepts and robust tools (Makropoulos and Savíc, 2019). However, converging cyber and physical security, assessing cyber-physical threats, and subsequently preparing against them can be a daunting task that requires multidisciplinary approaches and information from multiple sources that span from expert judgment to state-of-art models.

To assist the sector in overcoming this barrier, the Risk Assessment and Evaluation Toolkit (RAET) was produced, as a solution for cyber-physical water systems security at strategic and tactical level within STOP-IT (Ugarelli et al., 2018). RAET is directly supporting the broad objectives of Critical Infrastructure Protection programs and is consistent with the main standards and approaches enhancing cyber-physical resilience of the water sector. RAET supports the utilities in the steps of a) identifying, b) analysing c) evaluating cyber-physical scenarios and d) selecting suitable risk mitigation actions while evaluating their effectiveness, in a systematic and standardized way, through various components that serve an overarching framework inspired by ISO risk management standards. The platform supports the overall process at multiple levels, considering the end-user perspective and implementing different analysis procedures, based on the needs as well as on data availability. The core components of RAET are the following:

- The **Fault Tree Viewer** (FT Viewer) which enables FT analysis and supports the identification and selection of risks for further use
- The **Scenario Planner** (SP) which supports the creation and management of threat scenarios and the investigation of relevant risk reduction measures

- The **Key Performance Indicator Tool** (KPI Tool), that helps analyse and evaluate simulation results in detail
- The **Stress Testing Platform** (STP) for the simulation of a single scenario or multiple variations of a given scenario in a single process
- The **RAET database** (RAET DB) is used to store all data produced by other RAET components and to integrate a generic cyber-physical risks DB and related risk mitigation measures DB.

To properly represent both cyber and physical threats and their combination, the toolkit relies on formulating the identified risks and considering system interactions through the rigorous Fault Trees (FT) architecture. This allows the dedicated RAET component, the FT Viewer, to capture the cyber-physical relationships/dependencies between events that help determine and analyse factors that can contribute to a failure incident. Through capabilities like editing or adding FTs, RAET enables different users to constantly renew and enhance the information structure and directly communicate risks of different origins in a common view. In addition to the explicit relationship structure, it also provides an interactive and dynamic visual representation of the converged cyber-physical threat landscape, for users to explore and gain awareness of the situation.

Supported by the intuitive functionalities of the Scenario Planner component, the user-identified cyber-physical threats can be transformed from FT events into network-specific threat scenarios. In a standardised, stepwise approach, all required key characteristics that render the potential threat event to be explored, are introduced to a specified scenario structure. This way, the SP component acts as a wrapper for all the scenario data, hiding underlying model specific input data and taking care of the modifications that are needed in the related files accordingly. By creating, editing and managing the cyber-physical scenarios under a unified, structured process, the RAET ensures consistent structure and a unique interpretation of any scenario.

To ensure a resilience-based assessment (Makropoulos et al., 2018) and preparedness against the complex cyber-physical threat landscape, it is necessary to rethink water systems as CPS in stress-testing procedure (Nikolopoulos et al., 2019). Thus, for water CIs to prepare against events that may cascade from the cyber to the physical layer and vice versa, appropriate stress-testing environments are required that can realistically model those dynamics. RAET is designed to support and host various tools through the STP which incorporates different modelling engines for single and multiple cyber-physical scenarios simulations to serve the needs and purposes of the risk analysis. Seamlessly integrated within the overall RAET workflow, the user can utilise state-of-art solutions for more sophisticated CPS simulations, like RISKNOUGHT. RISKNOUGHT (Nikolopoulos et al., 2020a) is a recently developed, stand-alone stress-testing and modelling platform for water cyber-physical distribution networks. It is based on a simulation approach, able to represent information flow, control logic and interconnections of the cyber layer with the physical processes in a higher fidelity, realistic and extensible way, aiding in risk management practices. It is designed to address both quality and quantity related scenarios and realistically represent pressure deficiency effects, often occurring during system failure, by facilitating pressure-driven demand (PDD) hydraulic equations throughout the simulation of the threat scenario (Nikolopoulos et al., 2020b). This tool may also be utilised to explore variations of a cyber-physical scenario, through the multiple scenario simulation in a single batch procedure, similarly to a sensitivity analysis. This STP component functionality allows water experts to explore in detail the effects that a range of parameters, used to define a cyber-physical threat scenario (e.g., duration, occurrence time etc.), has on the system behaviour, and rank scenarios or detect “black-swan” scenario configurations. The very nature of cyber-physical threats (i.e., uncertainty, non-repeatability, unknown adversaries, high impact etc.) makes the stress-testing methodology essential in understanding CPS behaviour under attack and the resulting consequences.

As each system requires a unique scenario set-up to perform analysis and/or stress-testing, so does for the evaluation of the analysis output to quantify consequences, based on its unique risk criteria that define the utility’s risk attitude, the legal, regulatory and operating environment. Recognizing the need to uniquely interpret and communicate the stress testing results, a common quantification

framework has been adopted and seamlessly operationalised though SP and the Key Performance Indicators tool (KPI tool) component (Moraitis et al., 2020). The tool is designed specifically for water CIs under cyber-physical threat and is adjustable to any internal and external operating environment of a water utility. It enhances data-driven emergency preparedness and planning, while accounting for critical parts of the network and the society. RAET also assists users in their aim to find suitable mitigation measures for a given risk, through the consolidated ontology that links risks, consequences, and their corresponding mitigation actions from the embedded Risk Reduction Measures Database. By sorting the relevant mitigations for a given risk, the user can easily detect, evaluate and subsequently prioritize relevant measures that can be adopted to different regions and under various conditions.

Based on the results of this work, water utilities are now able to a) gain a clearer understanding of their strengths and vulnerabilities in a cyber-physical oriented way b) analyse promising interventions and countermeasures and stress test them against the same or other attacks c) investigate low probability - high impact scenarios and d) quantify costs and benefits which will eventually support them develop strategies to better prepare for risks that may occur in the future. As such, RAET and its components (e.g., RISKNOUGHT) set the example of how cyber and physical security approaches for contemporary CIs can converge and be integrated under a common, flexible and scalable platform to preserve data integrity and ensure a continuous, relevant information flow between multidisciplinary processes and multiple users.

### 7.1.2 FINSTIX Data Modelling for Financial Critical Infrastructures

FINSTIX: a Cyber-Physical Data Model for Financial Critical Infrastructures by Giorgia Gazzarata, CINI, University of Genoa

Cyber-physical security of financial institutions is a critical and sensitive topic. In the last few years, the number of cybersecurity incidents against financial institutions has been growing. It is then clear that financial institutions must increase their robustness against attack vectors. In the financial services industry, cyber and physical security measures usually act in isolation, thus entailing inaccurate vulnerability assessment and risk analysis and, in general, poor-quality security guarantees. In this context, the FINSEC project aims to design and build a reference architecture for integrating physical and cyber security of financial institutions.

To integrate Cyber and Physical security, the security services must process information on both cyber and physical systems. This information must follow a strict semantic to enable automated processing and information exchange among different security services. For these reasons, it is fundamental to make use of a proper data model that considers both cyber and physical aspects. While standard formats for Cyber Threat Intelligence do exist, standard formats for Cyber-Physical Threat Intelligence do not exist and must be defined.

After a brief description of the FINSEC Reference Architecture, FINSTIX is introduced. FINSTIX is the data model used to enable the semantic interoperability among the different services of the FINSEC Platform. In particular, it enables the interactions between the FINSEC platform and third parties, and the interactions among the different services within the FINSEC platform. FINSTIX is an extension of the OASIS STIX version 2, which is one of the most used Cyber Threat Intelligence standards. In addition to all the objects already defined by STIX (OASIS), FINSTIX introduces new custom objects to cope with both Logical and Physical incidents. Among the others:

- Organization is an object used to represent an organization;
- Asset is used to describe an organization valuable asset, such as a PC, an ATM, an application, or whatever is crucial for the organization;
- An Area of Interest is a logical or physical area, such as a server room;
- A Probe is a monitoring infrastructure that generates events and/or observed data;

- The Event object is used to represent an event produced by a probe;
- Attack describes a cyber-physical attack. It considers both cyber and physical attacks, thus enabling an integration among cyber and physical scopes;
- The Cyber-Physical Threat Intelligence object is the result of the analytic tools. One or more CPTI objects are used to generate the output of the intelligence process, which is a report about ongoing or possible future attacks on one or more assets belonging to the infrastructure.

The custom objects include information relevant to the financial institution to enable the integration of cyber and physical security measures.

Following the illustration of FINSTIX and its main features, an example of use of FINSTIX is presented. The example shows how FINSTIX is used to model the infrastructure of an imaginary bank, SuperBank. Moreover, it presents the FINSTIX objects generated and treated within the FINSEC platform to detect and mitigate an attempt of Jackpotting attack to a SuperBank ATM.

### 7.1.3 SAFECARE approach to integrated cyber-physical security for the healthcare sector

Fabrizio Bertone, LINKS Foundation

Hospitals are complex environments characterized by a high presence of external people and large-size structures, peculiarities that constitute complications for the implementation of effective physical security. At the same time, thousands of networked devices, potentially accessible to unauthorized persons, are connected to the internal ICT networks and to systems used to manage the daily activities of the hospital, involving cybersecurity aspects that have to be taken into consideration.

SAFECARE is building an architecture that integrates various modules for the monitoring of cyber and physical threats, the storage of security events and the management of incidents. Figure 15 represents a schema SAFECARE architecture (Bertone et al., 2020).

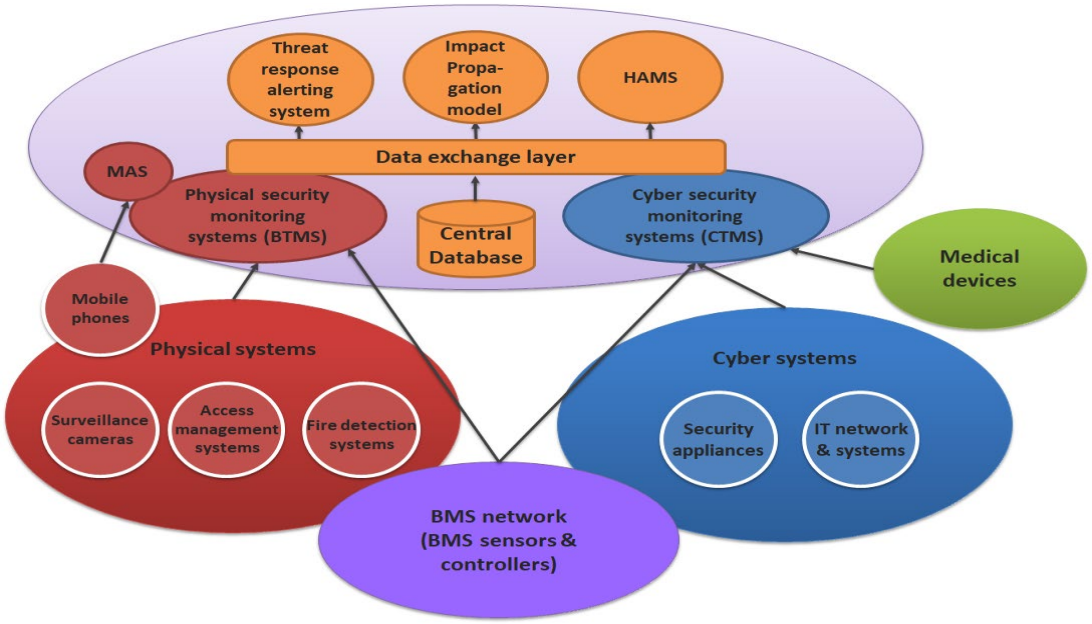


**Figure 15 – SAFECARE integrated architecture**

All the modules communicate through a common channel called Data Exchange Layer, using the standard MQTT protocol. Security events that have been identified as incidents, either automatically by algorithms or manually by human operators, are stored in a common Central Database and received by other modules for further elaboration.

The *Impact Propagation Model* (Atigui et al., 2020) contains information about links between assets, both physical (e.g., because they share the same location) and cyber (e.g., because they are connected to the same network). With this knowledge, the platform is able to infer probable cascading effects to other assets not directly involved in the incident, enabling an enhanced awareness of the global status of the hospital.

The *Hospital Availability Management System* (HAMS) (Lubrano et al., 2021; Stirano et al., 2020) is the module dedicated to crisis management, where operators have a real-time graphical view of all assets status, with the possibility of manually updating information if required. Furthermore, hospital availability information can be exported in EDXL-HAVE standard format (O'Donnell et al., 2019), enabling centralized management of patients between multiple hospitals in case of emergency.

Another module called *Threat Response and Alerting System* is in charge of automatically alerting relevant staff or external officers depending on the kind of incident that occurred. The alert process is carried on using multiple channels, like phone calls, SMS and a mobile app specifically developed during the SAFECARE project.

In order to better design the modules, initial threat analysis and risk assessment were done to collect information about the context. Several realistic mixed cyber-physical attack scenarios have then been conceived and will be later used to verify the solution by simulating them (Maia et al., 2020).

## 7.2 Standardization in Critical Infrastructure Protection

Could standardization break the silos approach in Critical Infrastructure Protection? By Dr. Denis Caleta, *President of the Board*, Institute for Corporative Security Studies (Slovenia)

Security is of key importance for the development of an individual and the society. Particularly the means for and the forms of an organized provision of security have changed dramatically throughout history, influenced significantly by new technologies and scientific evidence. The globalization of the world, and thus indirectly of security, poses serious dilemmas to modern society about how to continue basing its development on the fundamental requirements related to the free movement of goods, services and people, and, on the other hand, about how to keep threats at an acceptable risk level. The emergence of asymmetric forms of threat to national and international security is based on completely different assumptions and perceptions which were used in the past, based on the static approach of managing conventional threats. The changing social conditions and tensions caused by the rapid technological development found particular social environments totally unprepared for confronting the new global security situation and, above all, the newly emerging complex security threats. Dynamic changes and unexpected technological development have contributed to even greater complexity of this dimension. The fact that the modern society depends entirely on the functioning of technology makes this society even more vulnerable in terms of security. Energy, and in particular electricity, is in this respect even more important for normal functioning of modern society based on technology. Moreover, it makes individual threats and risks related to the proper functioning of infrastructure even more uncontrollable. Certain infrastructure segments, especially the sector of electrical power, are so important for the functioning of the society that their non-functioning or limited functioning could have serious consequences or cause serious trouble for that society (Čaleta, 2011).

Critical infrastructure and business-core applications can be attacked by means of many different vectors. Expanding on the previous analysis, it should be kept in mind that CI is, at an operative level, ordinary business with all the typical weaknesses that this implies.

We also need to face the fragmented landscape of operational approaches for CIP:

- Limits in the threat scope (e.g., either cyber or physical threats)
- Limits in the coverage of the energy value chain (from generation to consumer, from operation to market)
- Limits within the organisation, silos (e.g., technical, operations, business)
- Rarely involving human dimension (citizens or workers)
- Little systematic relationship between Power Network Operators and Security Operators/Service Providers and/or Law Enforcement Agencies
- Interaction and underlying procedures for linking Power Network Operators with Computer Emergency Response Teams (CERTs) and Information Sharing & Analysis Centres (EE-ISAC) still challenging at both governance and technological levels

DEFENDER as First-of-this-kind EU-scale solution for cyber-physical protection and security fully tailored to cover the complete value chain of smart Critical Energy Infrastructures. Bringing citizens and CEI stakeholders' workforce at a centre stage, as key elements of the proposed solution (human dimension). One of the very first attempts to bring together in a systematic way electrical energy network operators and Law Enforcement Agencies (LEAs) at the same table.

Standardization could break the silos approaches in CIP but should be carefully developed through the prism of processes complexity in organizations and take into consideration the landscape of threats from the security environment!

## 7.3 Collaborative Risk Assessment

Collaborative Risk Assessment and Impacts by John Soldatos, Innov-acts

This presentation introduced the importance and value of sharing security related information across stakeholders of the financial supply chain. This information sharing was motivated by recent security incidents in the finance sector (e.g., SWIFT network attacks) that could have been avoided if proper information sharing and information analysis services were in place. In this context, the presentation referred to state of the art infrastructures for sharing and analysing security information across stakeholders of the financial services supply chain, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).

The challenges of sharing and analysing information across stakeholders were also discussed, including security, data protection, interoperability, and trust challenges. For example, most financial organizations are not willing to share information about attacks against their infrastructures or vulnerabilities of their assets, since this could harm their brand image. Following the discussion of the information sharing challenges, a decentralized approach to sharing and analysing security information across financial organizations was introduced, along with its implementation based on distributed ledger technologies. Specifically, the presentation illustrated a blockchain-based approach for information sharing across financial organizations and other security stakeholder, which leveraged a permissioned blockchain infrastructure. The benefits of the approach include its ability to operate without the need for a trusted third party, i.e., based on decentralized trust. The blockchain infrastructure has been implemented in the scope of the H2020 FINSEC project.

Leveraging on the distributed ledger approach for sharing information, the FINSEC platform (developed in H2020 FINSEC) enables the secure and trusted flow of information across various financial sector stakeholders, as well as across relevant financial organizations. On top of the blockchain infrastructures a collaborative risk assessment application has been implemented. The application was described in detail as part of the presentation. It uses shared security information to trigger and to perform risk assessments. The presentation discussed the condition under which a new risk assessment is triggered. Furthermore, the risk scoring methodology and criteria were presented.

Overall, the presentation discussed a novel approach for collaborative risk assessment in the financial supply chain, which took advantage of a blockchain infrastructure for secure and trusted information sharing. This novel approach boosts the preparedness of security teams (CERTs/CSIRTs) within financial organization and contributes to increased resilience for the critical infrastructures of the financial sector. Indeed, some of the recent security incidents against financial organizations could have been avoided based on information sharing and collaboration across the different financial organizations that were affected by these incidents.

The presentation ends up with a prompt to the audience to register to the finsecurity.eu marketplace to access information, demonstrations, and training presentations about the FINSEC project in general and its collaborative risk assessment solution in particular.

## 7.4 Protect Industry 4.0

How to protect Industry 4.0 Sensitive Industrial Plants from cyber and physical attacks by Luigi Romano (InfraStress Technical Manager)

Cyber-security is key in Sensitive Industrial Plants and Systems (SIPS), since: i) attacks to Industrial Control Systems (ICS) of SIPS cost money, reputation, and even human lives, and ii) domino effects in the physical world could arise from cyber-attacks, causing environmental disasters or serious damage to production lines.

As an example, a combined cyber-physical attack to a SIP may result in environmental impact, as illustrated in Figure 16.

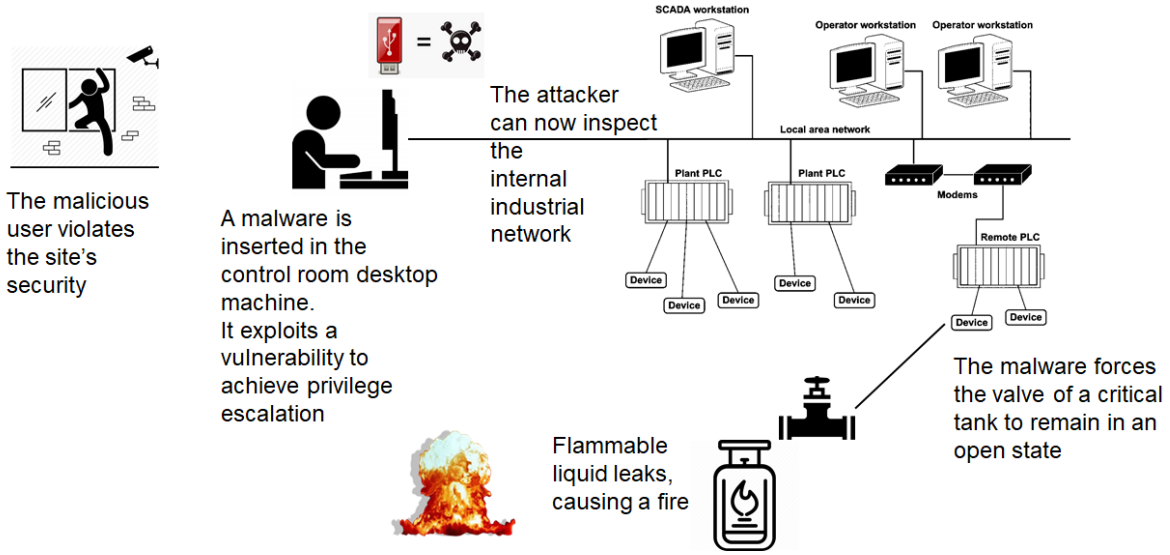


**Figure 16 – Storyboard of combined cyber-physical attack to a SIP resulting in environmental disaster**

In the specific context of Industry 4.0, a cyber-attack may impact the production process. A relatively easy to implement attack with dramatic impacts on the production line is as follows: 1) an insider attacker injects a malicious G-code in a CAD machine and in the product control system; 2) the CAD machine uses the malicious G-code with specifications which are not compliant to correct design of the product; 3) the final effect is that the entire product line is compromised.

The InfraStress project is developing advanced mechanisms to protect Industry 4.0 SIPS from these types of attacks. Project solutions will be validated in the specific context of a case study related to medical prosthesis production, contributed by project partner DePuy. The basic idea is to correlate

events from the OT and the IT worlds to timely spot attacks. The solution is being implemented in an advanced SIEM (Security Information and Event Management) tool.

## 7.5 Cyber and Physical Security management

Dr. Theodore Zahariadis, H2020 DEFENDER Technical Coordinator

In the last couple of years, technical innovations and developments in digital information and telecommunications dramatically increased interdependencies among the critical infrastructures. The energy infrastructure provides essential fuel to all critical infrastructure sectors, and without energy, none of them can operate properly. In turn, it depends on other critical infrastructure sectors, such as communications and information technology. Figure 17 provides a simplified illustration of inter-dependencies among 16 critical infrastructure sectors, including the 4 critical sectors (i.e., Energy, Water, Communications, and Transportation) that provide lifeline functions to all critical infrastructure sectors.

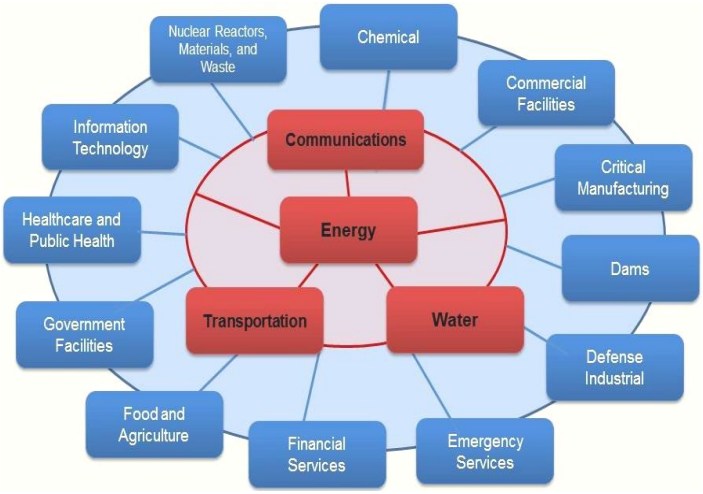


**Figure 17 – Critical Infrastructure Interdependencies**

H2020 project DEFENDER has played the role of a cross-sector critical infrastructures security facilitator, as a) it contributes to the resilience and uninterrupted operation of all other critical infrastructures by protecting the energy infrastructure directly and b) many DEFENDER achievements (including protection from both cyber-physical-social attacks and access to the pan-European I2SP) may apply to other critical sectors, such as water and transportation infrastructures.

In more details, DEFENDER has modelled Critical Energy Infrastructures (CEIs) as distributed Cyber-Physical Systems for managing the potential reciprocal effects of cyber and physical threats. Moreover, it has deployed a novel security governance model, which leverages on lifecycle assessment for cost-effective security management over the time. Finally, it has empowered citizens in vicinity and CEI employees to act as virtual sensors for threat detection, as first level emergency responders to attacks, or by considering workforce as potential threats.

During the project a broad threat analysis and classification has been conducted, providing a holistic threat and threat agent's taxonomy as a further basis for threat modelling and analysis of unknown threats. A final risk analysis and CEI assets, systems and segments classification according to their trustworthiness has been conducted and the Risk Analysis process has been elaborated. In the first reporting period, also a study, analysis and validation of the DEFENDER key design objectives, namely CEI Security Lifecycle Assessment by design, Resilience by design, CEI Survivability by design and CEI Data Privacy by design has been conducted.

DEFENDER platform offers incidents of mitigation via several technology innovations. The DEFENDER framework is able to detect and mitigate threats, providing a clear set of models for manage incidents and countermeasures, including a threat extraction tool for the detection of attack and threats and a repository suited for storing the new and old threats analysed by the DEFENDER Incidents Detection Support System. Moreover, the DEFENDER CEI Security Control Centre allows CEI operators to overview the security state of the CEI areas of their responsibilities and react, while the Incidents

Mitigation Decision Support System proposes a number of mitigation actions and technological countermeasures taking into account priorities in order to minimize downtime and cascading effects.

Finally, DEFENDER has created a Pan-European CEI Security Stakeholders Group (CEIS-SG) to share information on CEI risks, incidents, threats and countermeasures, exchanging reliability best practices.

## 7.6 Resilience of Critical Infrastructures

Indicators for assessing resilience of the European critical infrastructures: Wishful thinking vs. engineering challenge, by Aleksandar Jovanović, Steinbeis R-Tech / EU-VRi

Almost 100,000 projects in the EU CORDIS database contain words “security” and/or “safety”, over 10,000 “resilience”, and about as many deals with “infrastructure”. Their results contain several thousands (sic!) proposed “frameworks”, more than 100 proposing to be the “European ones”. More recently several representative EU projects have developed probably more than 10,000 indicators (over 5,000 of them only in the SmartResilience database). And yet, the EU does not have ONE resilience framework, allowing to assess its critical infrastructure, and does not have ONE set of commonly agreed and accepted resilience indicators. The same can be said for the plethora of tools delivered by the projects: having one main thing in common - they are not part of one common European system. The keynote suggested some possible ways forward, including the “OneResilience” concept, covering also new and emerging “x-threats”, and practical application of the project results in beyond-the-project use.

## 7.7 Increased Automation

Increased automation for detection, prevention, and mitigation measures, by Dr. Evangelos Markakis, Hellenic Mediterranean University

Dr. Evangelos Markakis from Hellenic Mediterranean University introduced the main areas of Automation needed in cyber security named (i) Automate Process (ii) Security Control (iii) Sieving through mountains of Data iv) Detecting anomalous activity v) Time intensive task associated (iv) Public Key Infrastructure and (v) Forensics investigation (Stoyanova et al., 2020). Afterwards, he presented the idea of automation with a fast review in current state of the art, showing the various focus areas and solutions for specific threats with special emphasis on how artificial intelligence benefits the data processing collection and reporting. Moreover, the main requirements in cybersecurity automation in the areas of Detection, Prevention, Mitigation, Recover and Reporting were described.

An automated framework for Vulnerability assessment as a service was introduced showing how the current advancement in virtualization and Software defined networking can automate the near real-time assessment of existing and newly introduced entities within a network. Special focus was given in the lack of interoperability in cybersecurity, hardening the ability of multiple “smart” toolsets to interoperate.

Finally, the presentation focused on what will be the future of Automation in cybersecurity with emphasis in Artificial intelligence, Security Orchestration, and Interoperability of toolsets.

## 7.8 Legal and Ethical issues

Issue: Healthcare critical infrastructures protection and cybersecurity in the EU: regulatory challenges and opportunities by Elisabetta Biasin, KU Leuven Centre for IT & IP Law (Biasin, 2020)

The year 2020 marks a crucial year for the EU agenda on critical infrastructure protection and cybersecurity, as EU policymakers, which will have to re-consider key pieces of legislation on the

matter. By applying a particular focus on healthcare, this contribution aims at providing key perspectives on the upcoming regulatory challenges, based on the research carried out in the SAFECARE project.

### 7.8.1 Introduction

Healthcare critical infrastructures are essential services for the security and well-being of individuals. The protection thereof should ensure their continuous functioning to impede disruptions and serious consequences for society from which it depends. In Europe, this kind of protection is currently regulated at the EU and national level – and in the upcoming months, these rules may be revised by the EU legislator. This workshop paper outlines the main regulatory challenges concerning the regulation of healthcare critical infrastructures in 2020, leveraging upon the research carried throughout the SAFECARE project. To do so, this paper gives a brief contextualisation of the matter (§2); it outlines the relevant frameworks (§3); and regulatory challenges concerning the European Critical Infrastructures Directive (ECI Directive, 2008)(§4); the Network and Information System Directive (NIS Directive, 2016)(§5). In light of this brief analysis, conclusive remarks (§6) will provide key takeaways on the regulatory challenges and opportunities that EU policymakers should consider for the healthcare critical infrastructures and their cybersecurity.

### 7.8.2 Context

Ensuring the protection of healthcare infrastructures is becoming a great disquiet for organisations and professionals worldwide. Physical attacks are a common source of insecurity for healthcare facilities. Attacks may deprive people of urgently needed care, endanger healthcare providers and undermine health systems (WHO, 2020). These concerns embrace cybersecurity, too. The last few years have seen an increasing rate of IT security incidents and data breaches for many healthcare ecosystems. Disrupting attacks to healthcare facilities, such as Wannacry and NotPetya underlined the necessity of keeping the level of those infrastructures adequate to security risks. This concern did not diminish after the COVID19 outbreak, which, on the contrary, led to an increase of cyber-attacks in healthcare (INTERPOL, 2020). At the same time, physical threats remained a critical factor to monitor in hospitals as the shortage of medical products caused thefts and security incidents in a wide range of cases (Philpot, 2020).

### 7.8.3 Setting the framework

Modern society is characterised by a strong interdependency between processes, resources and the correct functioning of infrastructural systems, whose interruption, damage or unavailability may cause economic damages for the society and may imply domino effects also in the provision of services and social development (Rinaldi et al., 2001). That is why critical infrastructures must be protected.

The protection of critical infrastructures in Europe requires the consideration of two distinct yet intertwining frameworks: first, the Critical Infrastructures Protection (CIP) framework and second, the Critical Infrastructures Protection (CIIP) – most commonly referred to as ‘cybersecurity’. CIP is a matter of national regulation due to the EU subsidiarity principle. At the EU level, the protection of critical infrastructures is regulated under the European Critical Infrastructure Directive (ECI Directive), whose implementation is embraced under the European Programme for CIP (EPCIP) and the CI Warning Network. Cybersecurity is a field that in recent years received growing attention by the EU legislator within the framework of the European Commission’s 2013 Digital Single Market Strategy. Such impulse led to the adoption of the first piece of legislation on cybersecurity, the NIS Directive, which was followed by other hard and soft laws, including the Cybersecurity Act (2019).

### 7.8.4 Regulatory challenges and opportunities for the CIP in healthcare: the ECI Directive

As research carried out in SAFECARE showed, the CIP framework envisages two opportunities and challenges upfront. The first one concerns the applicability of the ECI Directive to the healthcare sector. As widely known, the ECI Directive applies only to the energy and transport sector. In the past, this choice appeared already not fully aligned with EPCIP guidance documents which outlined the necessity to protect also other sectors concerning the critical infrastructures (Commission, 2018). This inconsistency was highlighted as well by some authors, which explained that the result of the ECI Directive should have been regarded as a temporary result, a compromise that has been reached at EU level to reach as fast as possible a common strategy among the Member States for the protection of critical infrastructures (Franchina, 2012). The ECI Directive itself indicated that it 'should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, among other things, the information and communication technology ('ICT') sector (ECI Directive, recital 5). Following this path, in 2019 the European Commission (in its working document on the ECI Directive evaluation) went further and noticed that 'the limited sectoral scope of the Directive means that it does not fully account for growing cross-sectoral interdependencies (Commission, 2019). This eventuality represents a crucial challenge and thus, opportunity for the ECI Directive revision. In this regard, possible scenarios for the ECI Directive would imply expanding its scope either maintaining a sector-specific approach or adopting a cross-sectorial one. Both scenarios would represent a positive opportunity for ECI protection in the EU. If this might prove right, caution should be paid, however, in order not to result in overlapping with the NISD.

The second challenge is inherently linked to the previous one concerns the consideration at a national level of healthcare within the critical infrastructures sectors. Member States adopted different approaches in their national CIP strategies – from sectors, to cross-sectors to critical processes. This has impacted healthcare, too. As the research in SAFECARE showed (Biasin et al. 2019), the Member States across Europe have adopted different approaches towards healthcare CIP, and some Member States do not consider healthcare as a critical sector. The study of the CIP framework for the SAFECARE pilot cases (France: Assistance Publique-Hôpitaux de Marseille (AP-HM); the Netherlands: Academisch Medisch Centrum (AMC); and Italy: Azienda Sanitaria Locale Torino 5 (ASLTO5)) underlined this evidence. By way of example, the SAFECARE D3.9 report outlined that, while France included healthcare in its twelve sectors for critical infrastructures, the same does not appear for the Netherlands, which recently reformed its CIP framework changing from a 'sector approach' to a 'process approach'. These views are further corroborated by previous EU projects in the field of healthcare critical infrastructures (THREATS, 2014), who found that Member States' protection level for healthcare CI remains uneven. The review of the ECI Directive could play a role in ensuring a convergent approach by Member States for CIP.

### 7.8.5 Regulatory challenges and opportunities for CIIP in healthcare: the NIS Directive

The NIS Directive is relevant for SAFECARE as the users of the technology to be developed will be healthcare providers. According to the NIS Directive, healthcare providers may be identified by at a national level as 'Operators of Essential Services', which have to ensure the security of their networks and information systems (NIS Directive, art 4(4)). Throughout the project, we have analysed the key aspects of the NIS Directive and its implementation in Europe. In light of these, several challenges were enlisted (Biasin et al., 2019). This section reports some of these. A first challenge relates to the implementation of the NIS Directive. The NIS Directive is an EU regulatory instrument that – likewise the ECI Directive – needs an implementation act by the Member States (MS). Namely, NIS Directive's objective is to provide minimum harmonisation for the protection of network and information systems with a margin for the Member States to develop further requirements on a national level (NIS Directive, art 1). After being approved in 2016, the NIS Directive had to be transposed across the Member States before May 2018. However, the NIS Directive was not timely implemented in all MS

before the May 2018 deadline. This brought adverse effects for many stakeholders willing to put in place the necessary measures foreseen by the EU law and national law (see NIS Directive, 148). Another challenge resides in national-level methodologies chose by the Member States for the identification of OES. Member States adopted different methodologies, which led to the incoherent application of the NIS Directive within the Union (Commission, 2019). As the European Commission put it, such a scenario may have possible consequences for the whole internal market and the effective handling of cyber-dependencies (ibid.). Finally, having regard to sector-specific legislation, it is worth recalling new challenges posed by medical devices cybersecurity regulation in the EU (Biasin & Kamenjašević, 2020). Risks of duplication with medical devices legal requirements on serious incidents (e.g., see Medical Device Regulation, article 87) and the General Data Protection Regulation (GDPR) (e.g., article 33) data breach requirements may arise. In this regard, it should be observed that simplification and cooperation mechanisms amongst competent authorities should be strengthened, to diminish burdens for healthcare organisations, as well as manufacturers (Biasin & Kamenjašević, 2020).

### 7.8.6 Conclusions

The purpose of this contribution was to outline healthcare CIP regulatory challenges for policymakers for the year 2020. The results achieved through research carried out for the SAFECARE project showed a wide array of challenges and opportunities. Concerning CIP: in the revision of ECI Directive, EU policymakers should consider whether to include healthcare in the scope of the Directive; or, if a cross-sector approach is chosen, they should be careful in avoiding risks of overlapping with the NIS Directive. Concerning cybersecurity: the effectiveness of implementation and coordination efforts at a national level needs to be monitored closely, to avoid risks of diverging application of the NIS Directive, and thus detrimental effects to the internal market. Finally, concerning healthcare-specific legislation (notably, medical devices law): more substantial alignment is needed with new cybersecurity pieces of legislation – such as the NIS Directive, and the others containing further cybersecurity requirements.

## 7.9 Predictive Analytics

AI based CCTV Analytics for Cyber-physical Security, by Jürgen Neises, Fujitsu

The presented solution for AI based CCTV Analytics is part of the physical security intelligence of the cyber-physical threat intelligence FINSEC platform.

Major motivation of FINSEC is the combination and integration of physical and cyber-security in automated Security event management, anomaly detection and threat prediction by the FINSEC platform unifying the analysis of physical and cyber events. The FINSEC CCTV Analytics System (FCAS) shall preserve privacy in physical threat monitoring by anonymous tracking and events. During the project, it has been validated in common Data Centre and ATM security scenarios. COVID-19 generated further related application scenarios for this technology in Public Safety & Security.

How does the solution work?

Starting from a CCTV video feed body parts are detected and tracked in bounding boxes. These body parts constitute human bodies from a configurable list of body parts. This way, a body can be constituted by different parts.

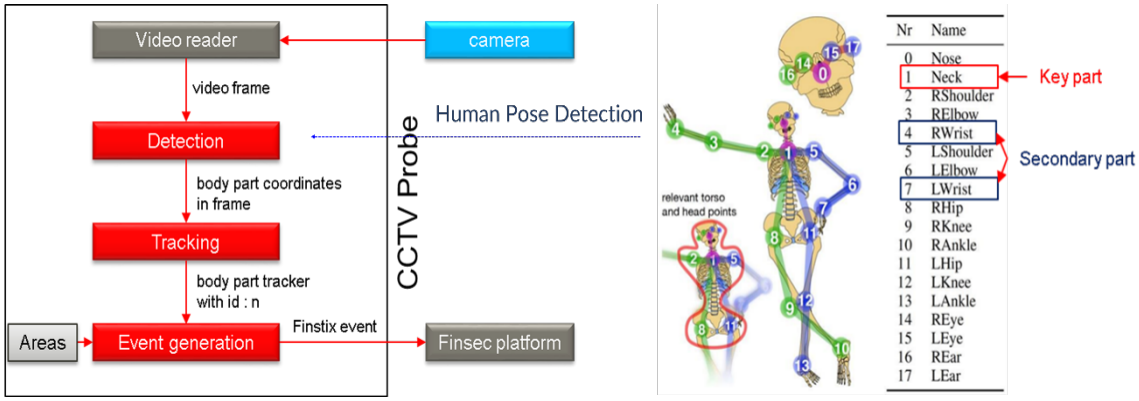


**Figure 18 – High Level Architecture and body model for pose estimation (Image source: Platte, 2018)**

Using the body model only anonymous human bodies are identified and tracked within a scene. In further steps, the human bodies are subject to human pose analysis, which enables the generation of events like entering a marked area, approaching people, speeding or trajectories. These anonymous events are issued in an open format called **FIN**SEC's **S**tructured **T**hreat **I**nformation e**X**pression (FINSTIX). In the FINSEC dashboard the events can be correlated and analysed.

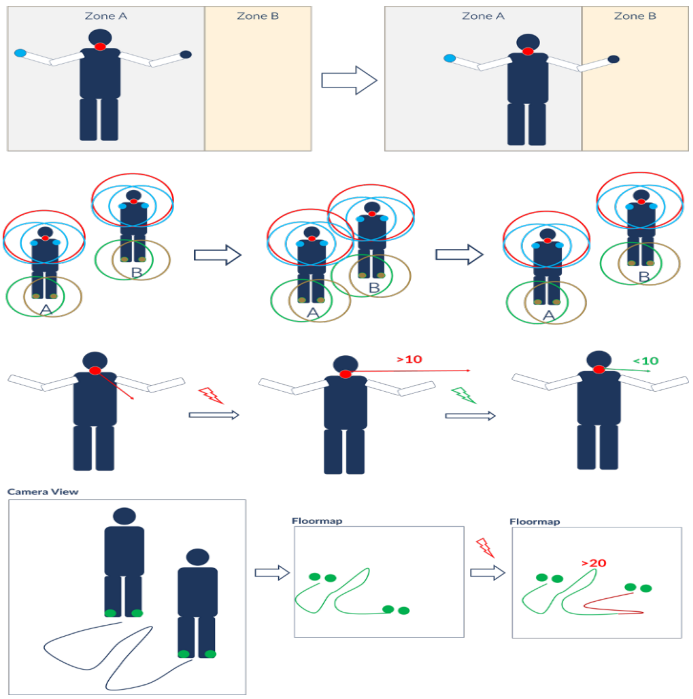


**Figure 19 – FCAS Events: Enter/Exit, Approaching/Distancing, Speeding/Slow-down, Trajectory Length**

The development starting point was applying existing technology based on a system with a powerful GPU, e.g., an X64 system and at least an NVIDIA 1080GTX. In a further step the NVIDIA Jetson platform, namely the Jetson AGX Xavier, has been evaluated as a first step towards edge and an intelligent sensor, e.g., inside an ATM. These common issues occurred. For instance, the TensorRT framework published by NVIDIA replaced the common TensorFlow. Even requiring further redevelopment, e.g., for Human Pose Detection this is advantageous for both hardware environments (edge and server). This way an optimization is achieved for both computing environments by this pose estimation implementation.

## 7.10 Anomaly detection

Applying Machine Learning algorithms to build anomaly-based cyber and physical detection systems, by Juan Caubet, EURECAT

Nowadays, security in physical and logical layers on an infrastructure is essential, even more so in ICS environments, where physical alterations like sensor manipulations or not authorized access are one of the most worrying actions that a malicious attacker can perform.

STOP-IT project is developing advanced tools to detect anomalies both in cyber and physical infrastructures based on the use of Machine Learning algorithms. Some examples of these tools are the three tools described below.

**Human Presence Detector (HPD)**. The HPD is a movement detector which can detect the movement of a person in a delimited area just by using the signals generated by at least one commercial Wi-Fi device. The system takes advantage of the physical layer of the Wi-Fi protocol by processing all the input signals of the Channel State Information (CSI) and taking a decision whether there is a person or not. Thanks to the Wi-Fi properties, the system can work through-the-wall and in any conditions of light and it is not required that the person carries any device with him/her because it is based on the variation of movement of the human body.

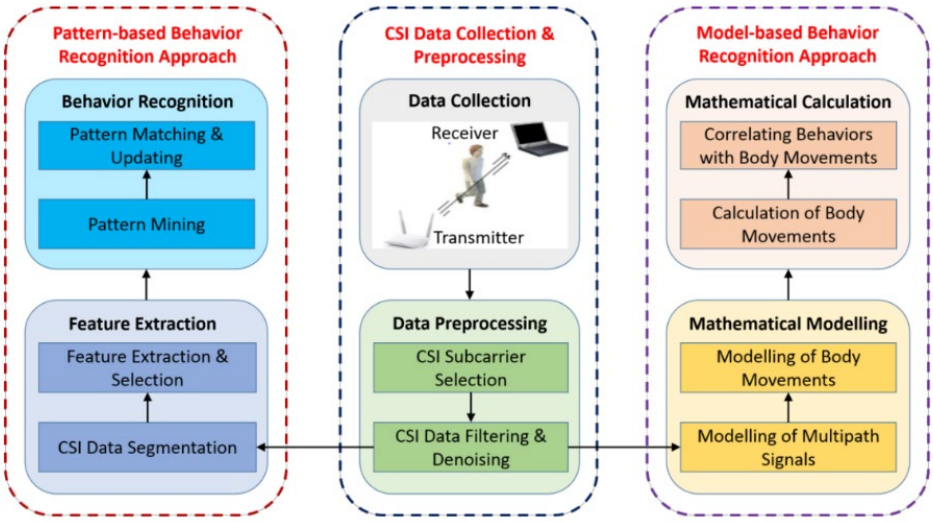


**Figure 20 – Scheme of the two ML-based schemes used by the HPD to detect the presence of a person.**

**Computer Vision Tools (CVT)**. The goal of the CVT is to survey large-scale utility areas using an existing network of cameras detecting any suspicious behaviour. The CVT utilises deep learning techniques and computer vision algorithms to provide an automatic assessment of actions and behaviours caught on cameras. The system attempts to "predict" the next frame based on the current input and the training set. When the difference between the prediction and the "true" frame is beyond a threshold, the situation is considered suspicious. The tool creates a model that can utilise inputs from multiple cameras, thermal cameras, and even other sources of information, and can detect (classify) movements as normal, i.e., movements that are usually occurring in the space we monitor, or abnormal, i.e., outliers of what is normally happening.

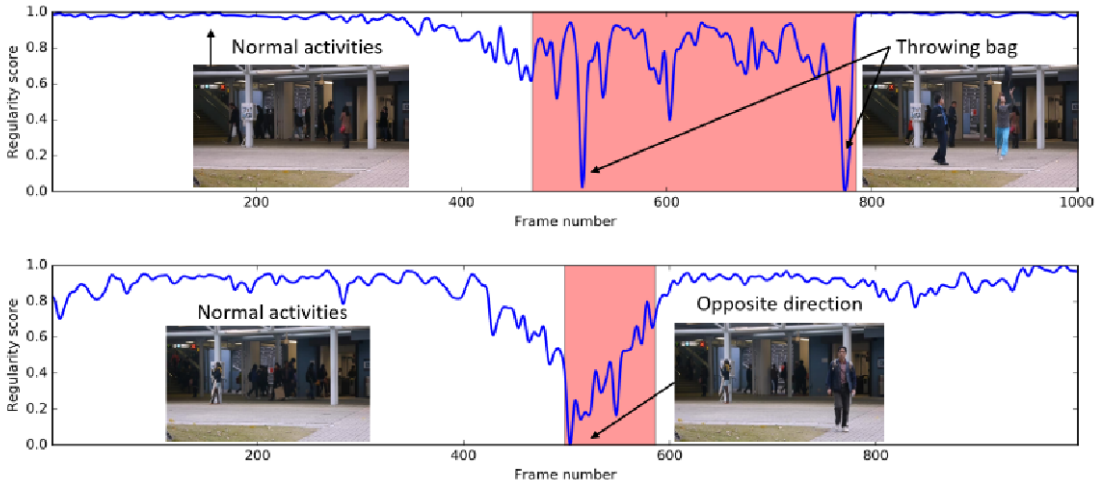


**Figure 21 – Example of abnormal situations detected by the CVT**

**Real Time Anomaly Detector (RTAD)**. The RTAD is an ML-based software tool, specialized in ICS environments, that analyse both the physical and logical layer of the environment, collecting information about traffic, final data values and events. The final goal of RTAD is to be able to detect logical and physical malicious actions as well as malicious behaviour with combined physical and logical actions. To this end, the RTAD consists of a big data platform and ML algorithms for detecting unusual situations as a result of the combination of physical and logical suspicious actions as well as known logical attacks and anomalies, unauthorized modifications to critical data, anomalies in the behaviour of data transmitted by the ICS applications, deviations in the behaviour of the previous month, among other types of infrastructure information.

# 8. Concluding Remarks and Planning

## 8.1 Day 1 and Day 2

**In Day 1,** the Opening remark**s** from the EC were encouraging and instructive opening remarks and connecting the activities of the cluster to various EC initiatives such as CoU". The keynote addressed the prominent security concern of cybersecurity of critical national infrastructures and the key takeaway is "Collaboration is Everything".

Projects presentations were in the energy (DEFENDER), healthcare (SAFECARE), finance (FINSEC), communication (RESISTO), and industrial (InfraStress), and water (STOP-IT) sectors highlighting the integration of cyber-physical security, (ii) thematic presentations were in the areas of cyber-physical security integration and modeling, standardization, collaborative risk assessment, protecting Industry 4.0, and cyber-physical security management, and (iii) a panel discussion on Ethical, legal, and social implications of projects. In the planning session the following issues were discussed: writing a consolidated proceedings report to be published (e.g., in International Journal of Critical Infrastructure Protection), stimulating the uptake of project results through raising awareness among stakeholders, exploiting the synergies by sharing best practices, collaboration (roadmap the different networking initiatives, meet the high expectation, and the ECSCI collaborative platform), and organization of 2nd ECSCI Workshop. The final decision was to keep ECSCI to populate all projects in CIP and continue with a series of ECSCI workshops. The ECSCI initiative is very important!

**In Day 2**, the keynote addressed the significance of cyber security as an ever-growing issue with political, societal, and economic implications. The talk looked at global trends and the challenges for a trustworthy and competitive European cyber security ecosystem and for the creation of secure and resilient infrastructures. The welcoming talk on resilience of Critical Infrastructures addressed the indicators for assessing resilience of the European critical infrastructures: Wishful thinking vs. engineering challenge.

Project presentations were in the cross-sectors (ANASTACIA) and (SmartResilience), and in the air transport (SATIE), gas (SecureGas), and healthcare (SPHINX) sectors highlighting the integration of cyber-physical security and resilience of critical infrastructures, (ii) thematic presentations were in the areas of (a) increased automation for detection, prevention and mitigation measures, (b) legal and ethical frameworks concerning cybersecurity of critical infrastructures (with a specific focus on healthcare and medical devices), (c) AI based CCTV analytics for cyber-physical security, and (d) applying machine learning algorithms to build anomaly-based cyber and physical detection systems, and (iii) a panel discussion on artificial intelligence for securing critical infrastructures. In the planning session the following issues were discussed: ensure a full portfolio of platforms needed (including exploitation), exploitation platform (sustainable beyond Projects' lifetime), and ensure right inputs & interaction to EU directive on CI. The following questions were also raised and discussed (i) in what ways does integrating cyber-physical security help improve the protection critical infrastructure, specifically in prevention, detection, response and mitigation? How AI contributes to this?, (ii) how can the ECSCI cluster best contribute to the new EU directive on critical infrastructures?, and (iii) how can we catalyze a common communication and information exchanges platforms? The key takeaways were: (i) organize the 2nd ECSCI Workshop on how each project deals with combined treats physical and cyber and risk assessment methodology, tools and list of risk identified as representative samples (not classified information), and (ii) use and relay on the results from the projects, e.g., by creating a Project Liaison Group of high-level representatives from the projects.

## 8.2 Closing Remarks

By Max Brandt, Area Coordinator Infrastructure Protection, Directorate General for Home Affairs, Unit B4: Innovation and Industry for Security

Security research and other innovation activities are the tools which the European Commission deploys to provide strategic knowledge to the operational actors, as well as policy makers on all levels. This is in few areas as evident as in Infrastructure Protection. When looking at the current landscape of risks and vulnerabilities, we can conclude that the major challenge is one of ensuring technological capabilities and allowing for multi-stakeholder cooperation. Research projects- like the ones that have been presented during this session- are key to achieving both. For the European Commission, their contribution is not only in generating research results and deploy new solutions with the industry. It is the extraction of the specific strategic advice which they can give, as well as their feedback to ongoing policy initiatives which needs to be stimulated with different activities.

ECSCI does part of this important work and is a perfect example of the strength of the infrastructure protection research community. The degree of self-organisation and networking is on a very high-level. When it comes to research on the security of infrastructures, we are facing many obstacles, mainly due to the rapidly changing international landscape, the high technological complexity of the matter and also the significant costs that successful deployment implies. But we also have on the other hand also many chances, since we combine in the projects public and private operators, academia and the relevant industry. If the process is steered, the potential for uptake of solutions that come out of EU-funded security research in this area is huge. To enhance such uptake and to ensure maintaining the already high quality of projects also under Horizon Europe, we are very much looking forward to continuing following the work of ECSCI and benefit from its outcomes.

## 8.3 Concluding Remarks

The ECSCI 2 days Virtual workshop is getting to the closing time. At the end of this workshop, on behalf of the organizing committee, we would like to say many thanks for your all kindness and efforts to participate in this workshop and getting along with the tough schedule. Special thanks to the EC for the encouraging and instructive opening remarks, two keynote speakers for their stimulating talks,

and to the great project presenters, thematic presenters, panelists for their excellent presentations. We Max Brandt for his inspirational closing remarks.

Our final suggested core messages of the workshop are that future work in the EU projects should ensure that

1. the Critical Infrastructure related EU projects and activities have a full portfolio of platforms needed, incl. the platform for exploitation of project results beyond the projects' lifetime (we currently have the CoU, the CEN-CENELEC Sector Forum on Security, ECSCI…, but we still miss an exploitation platform, such as ERRA proposed by SmartResilience and InfraStress), and
2. that they ensure right inputs & interaction for/with the new EU directive on critical infrastructures, including the envisaged shift from "critical infrastructures" to "critical functions". The new Directive should possibly cover interdependencies, the "x-threats" (multiple/new/unknown/ emerging threats) and, above all ensure that it includes the results and experience from the numerous projects (e.g., by creating a Project Liaison Group of high-level representatives from the projects).

This workshop has been proactive with important and stimulating talks such as two keynotes in the areas of (1) Critical Information Infrastructure Protection: The role of ENISA in the new EU policy context, Kostantinos Moulinos, ENISA and (2) Moving towards a trustworthy and resilient European cyber security ecosystem, Roberto Cascella, ECSO, presentations of 11 H2020 project results, 12 thematic presentations, and 2 panel discussion sessions. We wish to express our gratitude to you all for joining the ECSCI workshop and sharing your experiences and thoughts, and we hope you all stay safe!

## Acknowledgements

Part of this work has been carried out in the scope of the FINSEC project (contract number 786727), ANASTACIA (contract number 731558), DEFENDER (contract number 740898), InfraStress (contract number 833088), RESISTO (contract number 786409), SAFECARE (contract number 787002), SATIE (contract number 832969), SecureGas (contract number 833017), SmartResilience (contract number 700621), SPHINX (contract number 826183), STOP-IT (contract number 740610), which are co-funded by the European Commission in the scope of its H2020 program. The authors gratefully acknowledge the contributions of the funding agency and of all the project partners. In closing, the authors wish to thank all the authors for their insights and excellent contributions to this report.

# References


Lee, E.A., 2008. Cyber Physical Systems: Design Challenges, in: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC). IEEE, pp. 363–369. https://doi.org/10.1109/ISORC.2008.25

Makropoulos, C., Nikolopoulos, D., Palmen, L., Kools, S., Segrave, A., Vries, D., Koop, S., van Alphen, H.J., Vonk, E., van Thienen, P., Rozos, E., Medema, G., 2018. A resilience assessment method for urban water systems. Urban Water J. 15, 316–328. https://doi.org/10.1080/1573062X.2018.1457166

Makropoulos, C., Savíc, D.A., 2019. Urban hydroinformatics: Past, present and future. Water (Switzerland) 11. https://doi.org/10.3390/w11101959

Moraitis, G., Nikolopoulos, D., Bouziotas, D., Lykou, A., Karavokiros, G., Makropoulos, C., 2020. Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats. J. Environ. Eng. 146, 04020108. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001765

Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., Makropoulos, C., 2020a. Cyber-Physical Stress-Testing Platform for Water Distribution Networks. J. Environ. Eng. 146, 04020061. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001722

Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., Makropoulos, C., 2020b. RISKNOUGHT: Stress-testing platform for cyber-physical water distribution networks HS5.2.3-Water resources policy and management: digital water and interconnected urban infrastructure. https://doi.org/10.5194/egusphere-egu2020-19647

Nikolopoulos, D., van Alphen, H.J., Vries, D., Palmen, L., Koop, S., van Thienen, P., Medema, G., Makropoulos, C., 2019. Tackling the “new normal”: A resilience assessment method applied to real-world urban water systems. Water (Switzerland) 11, 330. https://doi.org/10.3390/w11020330

Ugarelli, R., Koti, J., Bonet, E., Makropoulos, C., Caubet, J., 2018. STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber- physical Threats, in: La Loggia, G., Freni, G., Puleo, V., Mauro, D.M. (Eds.), HIC 2018. 13th International Conference on Hydroinformatics. EasyChair, Manchester, pp. 2112–2119.

Markakis, E., Nikoloudakis, Y., Pallis, E., & Manso, M. (2019, April). Security assessment as a service cross-layered system for the adoption of digital, personalised and trusted healthcare. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 91-94). IEEE.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, 22(2), 1191-1221.

Nikoloudakis, Y., Pallis, E., Mastorakis, G., Mavromoustakis, C. X., Skianis, C., & Markakis, E. K. (2019). Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case. Peer-to-Peer Networking and Applications, 12(5), 1216-1224.

John Soldatos (ed.), James Philpot (ed.), Gabriele Giunta (ed.) (2020), "Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures", Boston-Delft: now publishers, http://dx.doi.org/10.1561/9781680836875

Čaleta, D. (2011). A Comprehensive Approach to the Management of Risks Related to the Protection of Critical Infrastructure: Public-Private Partnership. In: Čaleta, D. & Paul Shemella (Eds.). Counter terrorism challenges regarding the process of Critical Infrastructure Protection (pp. 15-26). Ljubljana, Monterey: ICS, Centre for Civil Military Relations.

Council Directive 2008/11/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75 (ECI Directive).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1 (NIS Directive).

WHO 'Stopping attacks on health care' (WHO) <https://www.who.int/activities/stopping-attacks-on-health-care> accessed 30 September 2020.

INTERPOL 'Cybercriminals targeting critical healthcare institutions with ransomware' (INTERPOL, 4 April 2020) <https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware> accessed 30 September 2020.

Philpot, J., 'Security Incidents in Healthcare Infrastructure during COVID-19 Crisis' (SAFECARE, 25 September 2020) <https://www.safecare-project.eu/?p=588> accessed 30 September 2020.

Rinaldi, SM., Peerenboom, JP., and Kelly, TK., 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies' [2001] IEEE Control Systems Magazine 11.

E. Biasin, D. Bresic, P. Notermans, E. Kamenjasevic, SAFECARE Deliverable: D3.9 Analysis of ethics, privacy, and confidentiality constraints (2019), https://www.safecare-project.eu/?p=465, 42-50.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the Euro-pean Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L 151/15 (Cybersecurity Act).

Commission Staff Working Document on the ex post evaluation of the 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks" 2007-2013 Programme (CIPS). Accompanying the document Report from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ex post evaluation for the period 2007 to 2013 of actions financed by the 'Prevention and fight against crime' programme (ISEC) and the 'Prevention, Prepared-ness and Consequence Management of Terrorism and other Security related risks' programme (CIPS) SWD (2018) 331 final Annex 8.

Luisa Franchina, 'Le infrastrutture critiche nazionali ed Europee' [2012] Quaderno n. 3 I quaderni del Network AIAS.

Biasin, Elisabetta and Kamenjasevic, Erik, Cybersecurity of Medical Devices: Regulatory Challenges in the EU (September 30, 2020). The Future of Medical Device Regulation: Innovation and Protection, Cambridge University Press, 2020, Available at SSRN: https://ssrn.com/abstract=3855491 or http://dx.doi.org/10.2139/ssrn.3855491

Commission, 'Evaluation of Council Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection' SWD (2019) 308 final (Commission Evaluation Report).

THREATS, 'An Analysis of Critical Infrastructure Protection Measures Implemented within the European Union: Identifying which European Member States includes the Health Sector as part of Critical National Infrastructure and which facets of Health Infrastructure are considered Critical' [2014] Report No: DR/1/001 <http://www.threatsproject.eu/WP1%20D1%20final.pdf>.

Biasin et al., SAFECARE D3.9 Analysis of ethics, privacy, and confidentiality constraints (SAFECARE, 2018) <https://www.safecare-project.eu/?p=465> accessed 30 September 2020.

Commission, ‘Report from the Commission to the European Parliament and the Council assessing the con-sistency of the approaches taken by Member States in the identification of operators of essential services in ac-cordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems’ COM (2019) 546 final.

E Biasin, E Kamenjašević ‘Cybersecurity Of Medical Devices. Regulatory challenges in the EU’ [forthcoming, 2020]; E Biasin ‘Medical devices cybersecurity a growing concern?’ (CiTiP Blog, September 2019) <https://www.law.kuleuven.be/citip/blog/medical-devices-cybersecurity-a-grow-ing-concern/> accessed 30 September 2020.

Maia E et al., ‘Security Challenges for the Critical Infra-structures of the Healthcare Sector’ in J Soldatos et al (eds), Cyber-Physical Threat Intelligence for Critical Infra-structures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures (Now Publishers 2020) 142–165.

EU Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1 (MDR).

EU Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and re-pealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016.

OASIS STIX Version 2.1, Structured Threat Information Expression (STIX) - language for expressing cyber threat and observable information <https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html>

Modern critical infrastructures (“critical entities” in the terminology of the new EU-CER Directive) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Thus, addressing cyber security and physical security separately is no longer effective, but more integrated approaches, that consider both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects, are needed to face the challenge of combined cyber-physical attacks. To face them successfully, aligned and integrated responses are needed, and this workshop has provided a great opportunity to do it: aligning and integrating not only the positions of single projects but also of many intended users of their results.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in seven different industrial sectors, such as finance, healthcare, energy, air transport, communications, industrial plants, gas, and water. The peculiarities of critical infrastructure protection in each one of these sectors have been discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies.

Specifically, novel techniques have been presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, resilience of critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures. The workshop included two opening remarks, two keynote speeches, 11 project presentations, 2 roundtable and panel discussions and 10 thematic presentations. The audience included scientists and experts in the field of critical infrastructure protection, CISOs, CIOs, CERTs, CSIRTs, CSOs, cyber and physical security experts representing different sector and policy makers for Critical Infrastructure protection.

978-3-95663-087-3

Steinbeis-Edition