e-book

Habtamu Abie, Ilias Gkotsis, Manos Athanatos,
Rita Ugarelli, Denis Čaleta, Lorenzo Lodi,
Fabrizio Di Peppo, Aleksandar Jovanović (Eds.)

Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience

Virtual Workshop, April 27–29, 2022

Steinbeis-Edition

Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience

Virtual Workshop, April 27–29, 2022

Habtamu Abie, Ilias Gkotsis, Manos Athanatos, Rita Ugarelli, Denis Čaleta,
Lorenzo Lodi, Fabrizio Di Peppo, Aleksandar Jovanović (Eds.)

Steinbeis-Edition

Imprint

2023 Steinbeis-Edition

Habtamu Abie, Ilias Gkotsis, Manos Athanatos, Rita Ugarelli, Denis Čaleta, Lorenzo Lodi, Fabrizio Di Peppo,
Aleksandar Jovanović (Eds.)

Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection
Virtual Workshop, April 27–29, 2022

1st edition, 2023 | Steinbeis-Edition, Stuttgart
ISBN 978-3-95663-285-3

Layout: Habtamu Abie, Ilias Gkotsis | Technical Editing: Steinbeis-Edition
Cover picture: Hilch / Shutterstock.com, edited by Steinbeis-Edition

The platform provided by Steinbeis makes us a reliable partner for company startups and projects. We provide support to people and organizations, not only in science and academia, but also in business. Our aim is to leverage the know-how derived from research, development, consulting, and training projects and to transfer this knowledge into application – with a clear focus on entrepreneurial practice. Over 2,000 business enterprises have already been founded on the back of the Steinbeis platform. The outcome? A network spanning over 6,000 experts in approximately 1,100 business enterprises – working on projects with more than 10,000 clients every year. Our network provides professional support to enterprises and employees in acquiring competence, thus securing success in the face of competition. Steinbeis-Edition publishes selected works mirroring the scope of the Steinbeis Network expertise.

222728-2023-02 | www.steinbeis-edition.de

Abstract

Modern critical infrastructures (or “critical entities” as now defined in 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. Addressing them successfully, need coordinated and integrated responses, which must be disseminated and exploited further to the EU funded projects' frameworks or individual research studies' reports, through raising awareness initiatives, such as the 2nd ECSCI Workshop on CIP.

This workshop presented the different approaches on integrated (i.e., cyber and physical) security in several 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, ethical and legal aspects of cybersecurity, combating hybrid threats to critical infrastructure, cyber and physical threats detection, increased automation for detection, prevention and mitigation measure, information and knowledge sharing, standards and regulations for the protection of critical infrastructures, common platforms for cascading effects on the different critical infrastructures, combined safety and security solutions, cyber security awareness, and the landscape of advanced combined cyber and physical threats.

The workshop included three opening remarks, three keynote speeches, twenty-one project presentations, two roundtable and panel discussions, twenty-one thematic presentations, and closing remarks. 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 sectors and policy makers for critical infrastructure protection.

Table of Contents

List of Figures

List of Tables

1. Organizing comittee

The 2nd ECSCI workshop organizing committee consists of the following members:

- Habtamu Abie, Norsk Regnesentral / Norwegian Computing Center,
  E-mail: habtamu.abie@nr.no
  Website: https://home.nr.no/~abie/
  OrcId ID: https://orcid.org/0000-0003-0866-5050
- Ilias Gkotsis, SATWAYS Ltd
  E-mail: i.gkotsis@satways.net
  OrcId ID: https://orcid.org/0000-0003-2228-1387
  https://www.linkedin.com/in/ilias-gkotsis-b7b84348/
- Manos Athanatos, FORTH,
  E-mail: athanat@ics.forth.gr
  https://www.linkedin.com/in/manosathanatos/
  Orcid ID: https://orcid.org/0000-0002-1182-7922
- Rita Ugarelli, SINTEF AS
  E-mail: rita.ugarelli@sintef.no
  OrcId ID: https://orcid.org/0000-0002-2096-8591
- Denis Čaleta, President of the Board, Institute for Corporate Security Studies,
  E-mail: denis.caleta@ics-institut.si
  Website: www.ics-institut.si
- Lorenzo Lodi
  E-mail: lorenzo.lodi@zanasi-alessandro.eu
  Website: https://www.zanasi-alessandro.eu
  Orcid ID: https://orcid.org/0000-0002-7600-621X
- Fabrizio Di Peppo, GFT Italia,
  E-mail: fabrizio.dipeppo@gft.com
  Website: https://www.gft.com
- Aleksandar Jovanović, Steinbeis EU-VRi
  E-mail: jovanovic@risk-technologies.com
  Website: www.eu-vri.eu and www.risk-technologies.com

2. Program Agenda

The three-day workshop program agenda includes open remarks, keynote speeches from the ENISA, ECSO, and JRC, 21 presentations on H2020 project results, 2 roundtable and panel discussions, 21 thematic presentations, and closing remarks.

- ECSCI (European Cluster for Securing Critical Infrastructures) Workshop
- Venue: Virtual Meeting
- Dates: 27th-29th of April 2022

Day 1: Wednesday, April 27th, 2022 (09:00-18.00)
Invited Talks, Project Presentations & Thematic Presentations

Welcome and opening of the day *Chair: Habtamu Abie, Norsk Regnesentral*	
09:00 - 09:10	Welcome and opening remarks: Habtamu Abie (Norsk Regnesentral) and Boryana HRISTOVA - ILIEVA from DG CNECT Unit H.2 – Cybersecurity and Digital Privacy Policy
09:10 - 10:00	**Invited Talk:** Cybersecurity investments and good practices for cyber risk management in critical infrastructure by Athanasios Drougkas, ENISA
10:00 - 10:20	Coffee Break
Session 1: The results of EU research on CI protection (part 1) *Chair: Manos Athanatos, FORTH*	
10:20 - 10:40	ANASTACIA (www.anastacia-h2020.eu): Security and trust assessment in CPS / IOT architectures - Stefano Bianchi, Algowatt
10:40 - 11:00	CyberSANE (www.cybersane-project.eu): Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures by Thanos Karantjias, MAGGIOLI
11:00 - 11:20	FeatureCloud (featurecloud.eu): Privacy-preserving AI in Systems Medicine with Federated Learning by Julian Matschinske, University of Hamburg
11:20 - 11:40	EnergyShield (energy-shield.eu): Shielding the power grid from cyberattacks by Otilia Bularca, SIMAVI
11:40 - 12:00	ENSURESEC (www.ensuresec.eu): Securing the e-commerce ecosystem from cyber, physical and cyber-physical threats by Luís Júdice Sousa, INOV
12:00 - 12:20	EU-HYBNET (euhybnet.eu): Empowering a Pan-European Network to Counter Hybrid Threats by Päivi Mattila, Laurea
12:20 - 12:40	CyberSEAS (https://cyberseas.eu/): Cyber Securing Energy Data Services by Paolo Roccetti, Head of Cysec research unit, Engineering (ENG)
12:40 - 13:00	FINSEC (www.finsec-project.eu): Securing critical financial infrastructure - Fabrizio Di Peppo, GFT
13:00 - 14:00	Lunch Break
Session 2: Cybersecurity and respective ELSI *Chair and moderator: Erik Kamenjašević, KU Leuven CiTiP*	

14:00 - 15:00	**Cybersecurity and the NIS2 Directive: regulatory aspects and sectoral perspectives** Panel by KU Leuven CiTiP researchers involved in SAFECARE/ ENSURESEC/ PRAETORIAN ● Eyup Kun (ENSURESEC): Evolution of the Cybersecurity Responsibilities: From NIS-to-NIS Directive 2 and its impact on E-commerce ● Maria Avramidou and Maja Nišević (PRAETORIAN): The Cybersecurity of airports and ports under the proposed NIS 2 and CER Directives. ● Elisabetta Biasin (SAFECARE): Medical Device Cybersecurity under the NIS2 and the AI Act *Moderator: Erik Kamenjašević*
15:00 - 15:20	**Ethical and legal aspects of cybersecurity** ● By Dimitra Stefanatou (Arthur van der Wees), Arthur's Legal B.V
15:20 - 15:40	Coffee Break
Session 3: **The results of EU research on CI protection (part 2)** *Chair: Rita Ugarelli, SINTEF*	
15:40 - 16:00	IMPETUS (www.impetus-project.eu): Intelligent Management of Processes, Ethics and Technology for Urban Safety by Joe Gorman, SINTEF Digital
16:00 - 16:20	InfraStress (www.infrastress.eu): Improving resilience of sensitive industrial plants & infrastructures - Gabriele Giunta, Engineering
16:20 - 16:40	PHOENIX (phoenix-h2020.eu): Improving the cyber security of the European electrical power energy systems by Ganesh Sauba, DNV
16:40 - 17:00	PRAETORIAN (praetorian-h2020.eu): Protection of Critical Infrastructures from advanced combined cyber and physical threats by Eva María Muñoz Navarro, ETRA I+D
17:00 - 17:20	SealedGRID (www.sgrid.eu): Scalable, trusted, and interoperable platform for secured smart GRID by Christos Xenakis, University of Piraeus
17:20 - 17:40	**Conclusions and Collaboration Planning of Day 1** *Chair: Habtamu Abie, Norsk Regnesentral*

Day 2: Thursday, April 28th 2022 (9:00-17.00)
Invited Talks, Project Presentations & Thematic Presentations

Welcome and Session 1 *Chair: Ilias Gkotsis, Satways Ltd*	
09:00 - 09:10	Welcome and opening remarks: Ilias Gkotsis (Satways) and Max Brandt from DG Migration and Home Affairs - D2 Counter-Terrorism
09:10 - 10:00	**Invited talk:** Moving towards a trustworthy and resilient European cyber security ecosystem by Roberto Cascella, ECSO
Session 2: The results of EU research on CI protection (part 3) *Chair: Ilias Gkotsis, Satways Ltd*	
10:00 - 10:20	SPHINX (sphinx-project.eu): Cyber-security protection in healthcare IT ecosystem by Evangelos Markakis, Hellenic Mediterranean University-HMU
10:20 - 10:40	STOP-IT (stop-it-project.eu): Protection of critical water infrastructures by Rita Ugarelli, SINTEF
10:40 - 11:00	7SHIELD (www.7shield.eu): A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats by Gerasimos Antzoulatos, Centre for Research and Technology-Hellas – CERTH
11:00 - 11:20	Coffee Break
Session 3: The results of EU research on CI protection (part 4) *Chair: Denis Caleta, ICS-Ljubljana*	
11:20 - 11:40	SecureGas (www.securegas-project.eu): An integrated, yet installation specific, solution for the resilience of gas infrastructure against cyber and physical threats by Celina Solari (Clemente Fuggini), RINA Consulting
11:40 - 12:00	PRECINCT (www.precinct.info): Cascading cyber-physical threats and effects by Antonis Mygiakis & Aristea Zafeiropoulou, Konnecta Systems
12:00 - 12:20	RESISTO (www.resistoproject.eu): Resilience enhancement and risk control for communication infrastructures - Bruno Saccomanno, Leonardo – Società per azioni
12:20 - 12:40	SAFECARE (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)
12:40 - 13:00	SATIE (www.satie-h2020.eu): Security of air transport infrastructure of Europe by Tim Stelkens-Kobsch, German Aerospace Center (DLR)
13:00 - 14:20	Lunch Break
Session 4: Combating hybrid and cyber-physical threats *Chair: Habtamu Abie, Norsk Regnesentral*	
14:20 - 14:40	**Combating Hybrid Threats to Critical Infrastructures** ● Innovations to counter hybrid threats by Souzanna Sofou, Satways (EU-HYBNET)
14:40 - 15:00	**Cyber and Physical Detection**

	● PRAETORIAN (praetorian-h2020.eu): Risk scenarios modelling and assessment in a combined attack approach by Frederic Guyomard, EDF Labs Paris (EDF)
15:00 - 15:40	**Round table discussions** ● Frederic GUYOMARD, EDF Labs Paris (EDF) ● Nineta Polemi, University of Piraeus *Moderator: Christos Tselios, Citrix*
15:40 - 16:00	Coffee break
Session 5: Increased automation and information sharing *Chair: Ilias Gkotsis, Satways Ltd*	
16:00 - 16:20	**Increased automation for detection, prevention and mitigation measures** ● Vasileios Mavroeidis, University of Oslo
16:20 - 16:40	**Information sharing techniques, rules, and repository to exchange knowledge** ● Decentralized Identities and the role of this technology in CI protection and information sharing by Michele Nati, IOTA
16:40 - 17:00	**Conclusions and Collaboration Planning Day 2** *Chair: Ilias Gkotsis, Satways Ltd*

Day 3: Friday, April 29th 2022 (9:00-17.00)
Invited Talk & Common Thematic Presentations

Welcome and Session 1 *Chair: Habtamu Abie, Norsk Regnesentral*	
09:00 - 09:10	Welcome and opening remarks - Giannis Skiadaresis from DG Migration and Home Affairs, Unit B4 - Innovation and Security Research
09:10 - 10:00	**Invited talk**: The evolution of security and resilience of critical infrastructures in a challenging environment by Georgios Giannopoulos, JRC
Session 2: Standards and regulations *Chair: Loredana Mancini, Inlecom Systems*	
10:00 - 11:20	**Standards and Regulations for the Protection of Critical Infrastructures** ● PHOENIX – Industrial Cybersecurity Testing Methodology on LSPs by Ganesh Sauba, DNV ● Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released by CISA and NIST in the United States by Ilesh Dattani, Assentian ● Standards and NIS compliance by Argyro Chatzopoulou, TÜV TRUST IT GmbH ● InfraStress: New DIN 91461 standard SPEC document on stress-testing resilience of critical infrastructures by A. Jovanović, Steinbeis EU-VRi, G. Giunta, Ch. Grunewald
11:20 - 11:40	Coffee break
Session 3: Platform for cascading effects *Chair: Isabel Praça, GECAD/ISEP*	
11:40 - 13:00	**Common Platform for Cascading Effects on the Different Critical Infrastructures** ● SmartResilience: A methodology and a platform for indicator-based self-generation of cascading scenarios in infrastructure-of-infrastructures by Aleksandar Jovanović (Steinbeis EU-VRi) ● Synergies and Challenges towards the integration of Safety and Security requirements in Critical Infrastructure Protection: Examples from the SecureGas and Infrastress projects by Clemente Fuggini (RINA Consulting) ● Simulation Framework for Cascading Effects among Urban Critical Infrastructures by Stefan Schauer (AIT Austrian Institute of Technology GmbH) ● Mitigating attacks in Collaborative Manufacturing Environments by Adrien Bécue (Head of Innovation, Airbus Cyber Security)
Session 4: Safety and security, a holistic approach *Chair: Rita Ugarelli, SINTEF*	
13:00 - 14:00	**Combined Safety and Security for European Critical Infrastructures** ● Hybrid threats and critical infrastructure protection by Päivi Mattila, Laurea ● Integrated Security, Safety and Risk Assessment for CIs and will be made by Antonis Kostaridis (SATWAYS) ● Pan-European cybersecurity information and incidents sharing and management for Energy Infrastructures by Sofia Tsekeridou (Netcompany-Intrasoft)
14:00 - 14:40	Lunch Break

Session 5: Cybersecurity awareness *Chair: Habtamu Abie, Norsk Regnesentral*	
14:40 - 15:40	**Cyber Security Awareness** ● Framework for Cybersecurity Awareness in the Industrial Domain at EDF by Frederic Guyomard (EDF Lab Paris) ● Meta-computing in Cybersecurity by Arasaratnam Arasilango (Tech Inspire LTD) ● Cyber security awareness in critical infrastructures by Christos Angelidis (konnektable)
Session 6: Cyber and physical threats *Chair: Isabel Praça, GECAD/ISEP*	
15:40 - 16:40	**Advanced Combined Cyber and Physical Threats** ● Visible and Emerging Vulnerabilities in Critical Energy Infrastructures by G. Stergiopoulos (Univ. of the Aegean), D. Gritzalis (Athens Univ. of Economics & Business) ● Modeling cyber and physical threats in IT&OT integrated systems by Sokratis Katsikas (Director Norwegian Center for Cybersecurity in Critical Sectors (NORCICS), Norwegian University of Science and Technology - NTNU) ● Risk Methodology Approach for Combined Cyber and Physical Threats by M. Mohamed (HIBTI)
16:40 - 17:00	**Conclusions and Collaboration Planning Day 3:** Giannis Skiadaresis from DG Migration and Home Affairs, Unit B4 - Innovation and Security Research *Chair: Habtamu Abie, Norsk Regnesentral*

Enhancing resilience is a team effort…

Thank you for your participation!

3. Welcome and Opening Remarks

3.1 Opening Remarks

Max Brandt from DG Migration and Home Affairs - D2 Counter-Terrorism

It is commonly accepted in EU policymaking that the resilience of CIs is of paramount importance, nevertheless, in the last years, the environment of security has changed, with cybersecurity gaining more attention, as well as geopolitical, hybrid and systemic threats. Such complex risks highlight the increased importance of policy development and implementation, thus several policy documents have been published in the last months, such as the strategic compass of security and defence, which clearly reference the need of enhancing the resilience of CI.

A lot of work has been done in this direction, with one of the most important achievements being that of launching the proposal for a new framework, the legislative framework for the non-cyber resilience of critical entities (CER Directive), in 2020. Due to the significant importance of establishing such a legislative framework, especially in the last months, a series of negotiations are taking place between several MS and the EU parliament on the final version of the text. A final agreement is expected to take place in the coming months, providing substantial provisions to the sectors in scope (energy, transport, digital, banking, financial markets, drinking water, wastewater, health, public administration, space and food) and also making a clear reference to research conducted on the resilience of critical entities and their infrastructures.

The CER directive points to the CER group which will be the main cooperation body between the commission and the MS, having as one of its tasks to integrate relevant R&I activities, and acting as a significant opportunity to cooperate with the projects funded by H2020 and HEU, and other cluster activities like ECSCI. In a nutshell, the role of research in CER is acknowledged and closer collaboration is expected, exploiting the results, findings and lessons learned.

Giannis Skiadaresis - Coordinator of Resilient Infrastructure Research (INFRA) / Unit F2 - Security Research and Innovation, DG HOME

Countering security threats is one of the most complex challenges the European Union and its Member States are facing. The EU response aims to enhance situational awareness, boost resilience in all critical sectors, provide for adequate response and recovery in case of crisis. While Member States remain predominantly responsible for building resilience, detecting, preventing and responding to these threats, actions at EU level support and complement national efforts. The Security Union Strategy identifies the protection of critical infrastructures as one of the main priorities for the EU for the coming years. Specific reference is established to growing interconnectivity as well as emerging and complex threats. Another very important initiative is the proposal for a Critical Entities Resilience (CER). The CER-Directive covers natural and man-made non-cyber threats and will be coherent and complementary with the NIS-2 directive on cybersecurity. Both legislations combined will provide a comprehensive framework for resilience of critical entities against new complex hybrid threats.

On the side of security research, the transition from Horizon 2020 to Horizon Europe was closely linked various policy initiatives since the research programme supports their implementation with targeted projects. Under the last EU framework programme for research and innovation Horizon 2020 (2014-2020) we have been invested around 3 billion EUR and more than 700 projects since 2007, which is almost 50% of public spending on civil security R&I in the EU. This is why initiatives like the ECSCI are bringing high added value by clustering research projects. The specific focus on cross-cutting priorities which ECSCI has put at the core of the work, reflects the approach which the Commission also suggests for the future research on infrastructure resilience against hybrid threats: 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 work programme of Horizon Europe in the Infrastructure Resilience domain. 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 the fostering of the Resilience of our Infrastructure.

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 in this cluster - 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. Therefore, 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 EU Strategic Autonomy.

3.2 The ECSCI Cluster Achievements

Habtamu Abie, Norwegian Computing Center/Norsk Regnesentral

The European Cluster for Securing Critical Infrastructures (ECSCI) is a cluster of EU funded R&D projects, kicked off during the H2020 Work Programme, derived by the needs and interests of projects and experts conducting research and innovation on critical infrastructures protection (CIP) and resilience. Its initial objective and driving force are to create synergies and foster emerging disruptive solutions to security issues via cross-project collaboration and innovation.

The ECSCI cluster shares experiences and best practices about CIP in different sectors, consolidates and reflects a European approach for Cyber-Physical and Hybrid Threat Intelligence in the CIP domain, and focuses on research that protects and secures critical infrastructures and services respecting the differences between individual projects, such as the different approaches, sectors of interest, or target groups, while establishing tight and productive connections with closely related or complementary H2020 and HEU projects. Members of the cluster engage in various activities: (i) Scientific collaborations, in the form of joint workshops and conferences, co-writing of academic publications, (ii) Technical collaborations, such as sharing approaches on cyber-physical security, risk assessment, and predictive analytics, (iii) Communication and dissemination of information about the cluster’s activities and outputs through common web and social media presence as well as joint events, (iv) Building and fostering stakeholders’ alliances, allowing for the mobilisation of local ecosystems, and (v) Marketplace extensions of members and their products/services across various sectors. Figure 1 shows the 25 ECSCI member projects and collaboration activities.

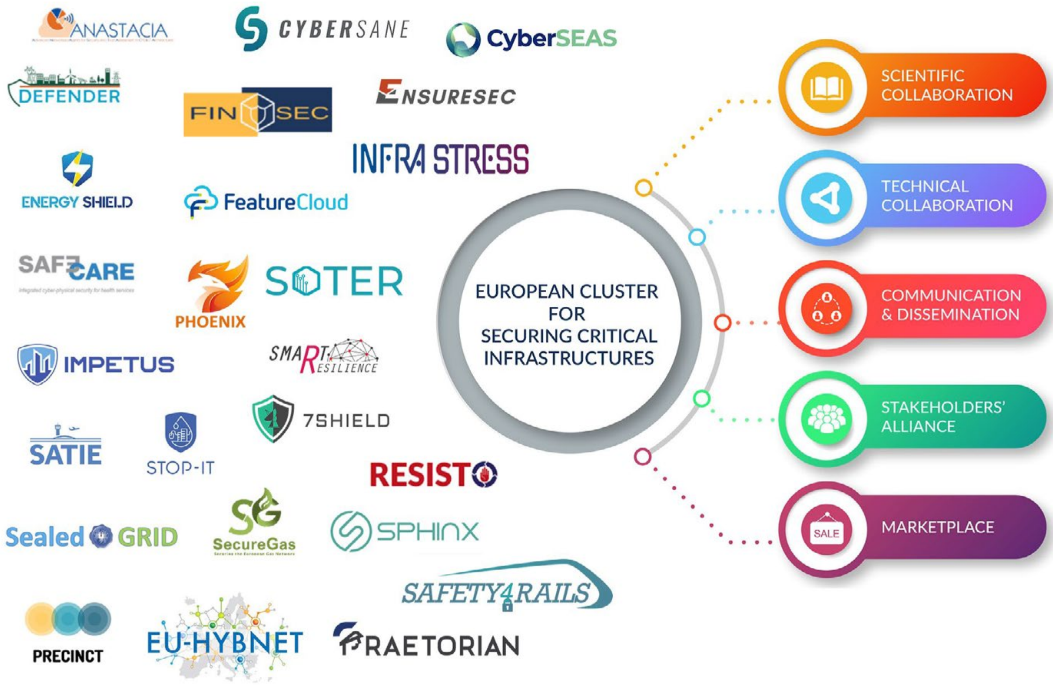


Figure 1 - ECSCI 25 member projects and collaboration activities

During its lifetime, the ECSCI cluster organized and participated in five events and stakeholders' workshops: SAFECARE awareness events (2019), the first ECSCI workshop (2020), the second ECSCI workshop (2022), ENSURESEC Final conference (2022), and EnergyShield final event (2022). It also organized a series of scientific workshops co-located with ESORICSv (European Symposium on Research in Computer Security): FINSEC 2019 (1st International Workshop on Security for Financial Critical Infrastructures and Services), CPS4CIP 2020 (1st International Workshop on Cyber-Physical Security for Critical Infrastructures Protection), CPS4CIP 2021 (2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection), CPS4CIP 2022 (3rd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection).

In the area of collaboration, the ECSCI cluster members co-edited two Open Access Books and contributed to book chapters:

(i) Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures, Editors: J. Soldatos (FINSEC), G. Giunta (DEFENDER), J. Philpot (SAFECARE), published by Now Publishers, structured in five parts: Finance, Energy, Healthcare, Communications, and Sector Agnostic Topics, based on the results of five (5) Projects: FINSEC (9 Chapters), DEFENDER (3 Chapters), SAFECARE (4 Chapters), RESISTO (6 Chapters), and SPHINX (1 Chapter).

(ii) Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry, Editors: John Soldatos (University of Glasgow, UK and INNOV-ACTS LIMITED), Isabel Praça (Institute of Engineering of the Polytechnic of Porto (ISEP)), and Aleksandar Jovanović (Steinbeis Advanced Risk Technologies Group), published by Now Publishers, structured in seven (7) parts: Air Transport, Water, Gas, Healthcare, Finance, Industry and Smart Resilience, based on the results of eight (8) projects: InfraStress (5 chapters), STOP-IT (4 chapters), SATIE (3 chapters), SecureGas (4 chapters), SAFECARE (3 chapters), SPHINX (1), FINSEC (2 chapters), and SmartResilience (1 chapter)

In the area of information sharing, the Finsecurity.eu Market Platform, which is a single-entry point to FINSEC Solutions and promotional channels for the project's results, has been enhanced with an "Other Sectors" Section destined to present and integrate solutions from other projects such as DEFENDER (Energy), STOP-IT (Water), RESISTO (Communications). Access to respective material is available through a simple and quick registration process provided through the platform (Finsecurity.eu) to the CIP community.

Further to the above, the ECSCI cluster has contributed to the following Proceedings and Newsletters:

- Consolidated Proceedings of the 1st ECSCI Workshop on Critical Infrastructure Protection based on the 1st ECSCI Virtual Workshop, held online on the 24th-25th of June 2020
- Consolidated Proceedings of the 2nd ECSCI Workshop on Critical Infrastructure Protection (under preparation) based on the 2nd ECSCI Virtual Workshop, held online on the 27th-29th of April 2022
- Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE
- Cyber-Physical Security for Critical Infrastructures Protection
- Computer Security: ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC
- ESORICS 2022 Workshops (ADIoT, CDT&SECOMANE, CPS4CIP, CyberICPS, EIS, SecAssure, SECPRE, SP-MIoT, SPOSE) under preparation
- Two articles in the Newsletter on Critical Infrastructure Resilience:
    - The European Cluster for Securing Critical Infrastructures (ECSCI)
    - Report on the 2nd ECSCI Workshop on Critical Infrastructure Protection

Based on the above and the scope of the cluster, ECSCI has and will continue supporting the uptake of project results, encouraging the exploitation of synergies and the sharing of best practices, stimulating network and alliance formation, and serving as a collaborative platform for all CIP projects and practitioners.

4. Keynotes

4.1 Cybersecurity investments and good practices for cyber risk management in critical infrastructure

Athanasios Drougkas, ENISA

Since 2020, ENISA, the EU Agency for Cybersecurity, has been publishing the NIS Investments report, which aims to provide insights into how operators in critical sectors invest their cybersecurity budgets and how recent EU policies - primarily the NIS Directive - have influenced these budgets. The 2021 NIS Investments report [NIS 2021] includes data collected from 947 operators in critical sectors and illustrates the positive impact of the NIS Directive on their information security. The report also provides substantial insights into aspects related to the cost of cybersecurity incidents - highlighting the banking and health sectors as the sectors most impacted in that regard - as well as to how information security is organised in operators in critical sectors documenting investments in CISOs, certifications and cyber insurance among other topics.

In the context of supporting critical sectors, ENISA has also published over the past couple of years several reports with good practices for cyber risk management in different NIS Directive sectors. The 2021 report on cloud security for healthcare services [ENISA 2021] aims to provide Cloud security practices for the healthcare sector and identify security aspects, including relevant data protection aspects, to be taken into account when procuring Cloud services for the healthcare industry. The report builds on the procurement guidelines for hospitals report which was also published as an online tool in 2021 [ENISA-1]. Another online tool to support operators in critical sectors published in 2021 is the tool on cyber risk management for ports [ENISA-2], which aims to enable port operators to select and prioritise security measures based on a selection of assets to be protected and primary threats. Finally, for operators in the rail sector, ENISA published a report with good practices for cyber risk management approaches [ENISA 2021-2] and developed together with the European Railway ISAC (ER-ISAC) to give guidance on building zones and conduits for a railway system [ENISA 2022].

4.2 The evolution of security and resilience of critical infrastructures in a challenging environment

Georgios Giannopoulos, JRC

During the last 15 years, there is a huge amount of work which has taken place since the first efforts to establish a programme at EU level for the protection of critical infrastructures. In the meantime, the concepts have evolved, and we are focusing more on the resilience of entities and services while we see a completely different level of complexity in terms of the threats that infrastructures and critical services are facing. At policy level the landscape has changed completely with the adoption of the Security Union Strategy, which takes a much more comprehensive vision of security in which critical infrastructures are important pillars. In the future data, early warning, and strategic communication will play a very important role in order to improve the security and resilience of critical infrastructures and critical entities.

5. Project Presentations

Twenty-one H2020 project presentations in alphabetical order.

5.1 Security and trust assessment in CPS / IOT architectures

ANASTACIA: Security and trust assessment in CPS / IOT architectures by Stefano Bianchi

Project Number: 731558

Project Acronym: ANASTACIA

Project title: Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures

The main objective of the ANASTACIA project was to address cyber-security concerns by researching, developing and demonstrating a holistic solution enabling trust and security-by-design for Cyber-Physical Systems (CPS) based on Internet of Things (IoT) and Cloud architectures.

The heterogeneous, distributed, and dynamically evolving nature of CPS based on IoT and virtualised cloud architectures introduce new and unexpected risks that cannot be solved by current state-of-the-art security solutions. For this, new paradigms and methods are required in order i) to build security into the ICT system at the outset, ii) to adapt to changing security conditions, iii) to reduce the need to fix flaws after deploying the system, and iv) to assure that the ICT system is secure and trustworthy at all times.

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.

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 released a fully functional **conceptual and architectural model**, supporting a 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)

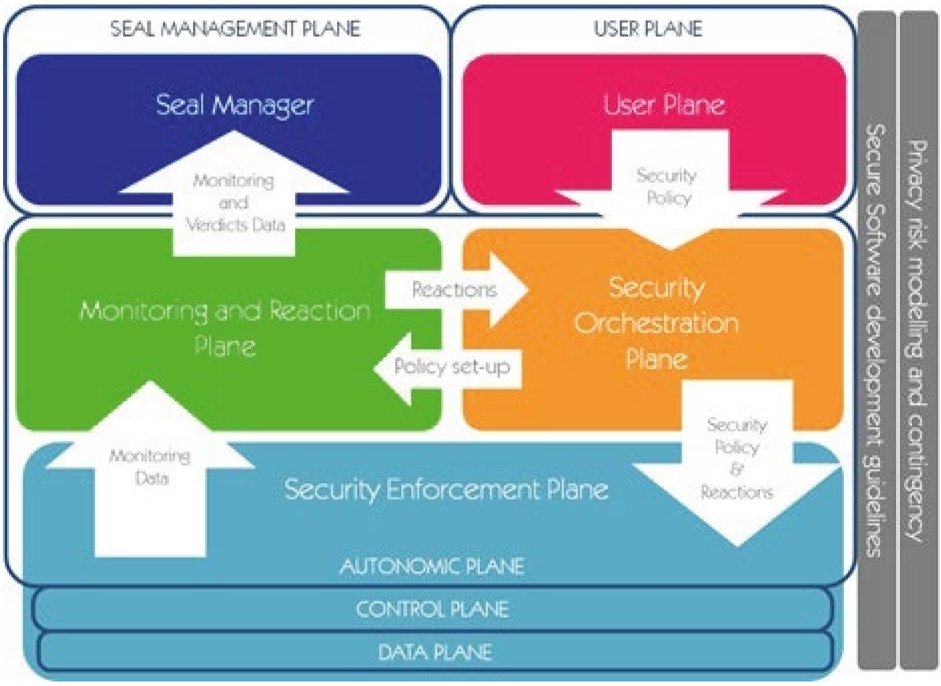

SEAL MANAGEMENT PLANE
USER PLANE
Seal Manager
User Plane
Monitoring and Verdicts Data
Security Policy
Reactions
Monitoring and Reaction Plane
Security Orchestration Plane
Policy set-up
Monitoring Data
Security Enforcement Plane
Security Policy & Reactions
AUTONOMIC PLANE
CONTROL PLANE
DATA PLANE
Secure Software development guidelines
Privacy risk modelling and contingency

Figure 2 - ANASTACIA high-level conceptual architecture

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

ANASTACIA also 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 are currently undergoing a **patenting process** to protect IPR and allow joint exploitation by the file proposers. 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.

Answering **8 Research Challenges (RC)**, i.e.:

- 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 kinds 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

ANASTACIA 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

The final ANASTACIA integrated prototype was finally tested in real lab premises hosted by the University of Murcia, involving interconnected IoT devices and physical assets, in a challenging, multi-level threat scenario, with evidence of attacks and associated mitigations up to the multipurpose DSPS (public video available on the project's public YouTube channel at https://www.youtube.com/watch?v=eEQNAcGiMFE).

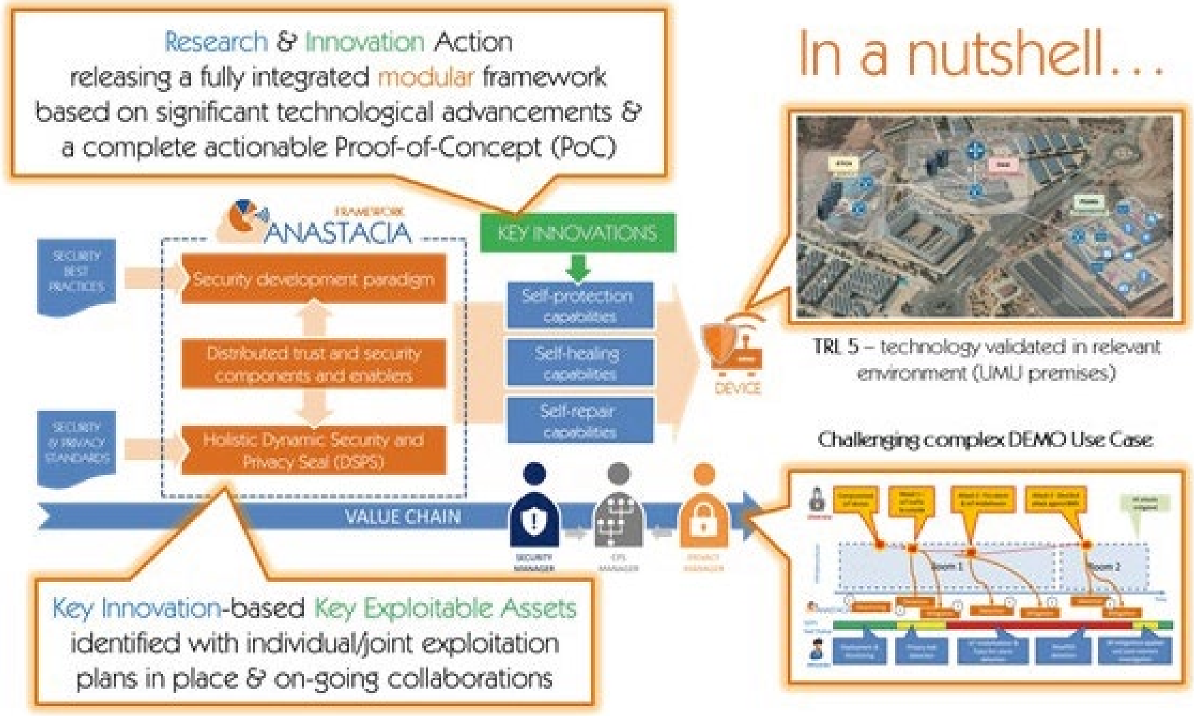

Research & Innovation Action
releasing a fully integrated modular framework
based on significant technological advancements &
a complete actionable Proof-of-Concept (PoC)
In a nutshell...
FRAMEWORK
ANASTACIA
SECURITY BEST PRACTICES
SECURITY & PRIVACY STANDARDS
Security development paradigm
Distributed trust and security components and enablers
Holistic Dynamic Security and Privacy Seal (DSPS)
KEY INNOVATIONS
Self-protection capabilities
Self-healing capabilities
Self-repair capabilities
DEVICE
TRL 5 – technology validated in relevant environment (UMU premises)
Challenging complex DEMO Use Case
VALUE CHAIN
SECURITY MANAGER
CPL MANAGER
PROJECT MANAGER
Room 1
Room 2
Key Innovation-based Key Exploitable Assets
identified with individual/joint exploitation
plans in place & on-going collaborations

Figure 3 - ANASTACIA integration, demonstration and exploitation in a nutshell

5.2 Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures

CyberSANE (www.cybersane-project.eu): Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures by Thanos Karantjias, MAGGIOLI

Grant Agreement Number: 833683

Project Acronym: CyberSANE

Topic: "SU-ICT-01-2018: "Dynamic countering of cyber-attacks"

In the digital era, Critical Infrastructures (CIs) are operating under the premise of robust and reliable ICT components, complex ICT infrastructures and emerging technologies and are transforming into Critical Information Infrastructures (CIIs) that can offer a high degree of flexibility, scalability, and efficiency in the communication and coordination of advanced services and processes. The increased usage of Information Technology (IT) in modern CIIs may have increased their performance and quality of services. Nevertheless, they have become more vulnerable to cyber-attacks posing new threat vectors due to their inherent cyber-dependencies. In particular, they have attracted the attention of hackers and cyber criminals, such as hacktivists (e.g., Anonymous, LulzSec), role-players (e.g., cyber-spies) and other perpetrators of cyber-related crime (cyber criminals). Several recent research studies have shown that the cyber threat landscape is growing immensely as adversaries are continuously evolving their skills and tactics in terms of persistence and technical sophistication. In fact, they utilize next-generation malware toolkits available in various locations on the internet (e.g., Deep Web, Dark Web) and new data exfiltration methods that give them an asymmetric quantum leap in capability. Since malware and malware-as-a service is cheap and approachable, they use a variety of advanced techniques and tools (e.g., social engineering techniques and zero-day exploits programs) to launch advanced targeted attacks that enable them to bypass organizations' security mechanisms and infiltrate the networks of the cyber-dependent CIIs. Towards this background, there is a pressing need for devising novel systems for efficient CIIs incident handling and support a thorough and common understanding of cyber-attack situations in a timely manner. In this context, appropriate incident handling solutions are necessary to support and facilitate the detection and analysis of cyber-attacks and threats on CIIs and raise the knowledge of CII operators on cyber risks.

CyberSANE EU H2020 research project aims to enhance the security and resilience of CIIs with the provision of a dynamic collaborative, warning and response system (CyberSANE system) to support and guide security officers and operators (e.g., Incident Response professionals) to recognize, identify, dynamically analyze, forecast, treat and respond to Advanced Persistent Threats (APTs) and handle their daily cyber incidents utilizing and combining both structured data (e.g., logs and network traffic) and unstructured data (e.g., data coming from social networks and Dark Web). The main objectives of the project are the following:

- Optimisation of collaboration and the promotion of effective interaction among CII operators.
- Development of Advanced Persistent Threats taxonomy and models for CIIs.
- Uniting Web crawling and data aggregation technologies for necessary semantic structure, representation, convention and tool creation for data pulling, cleansing, analysis and interlinking.
- Development of Correlation Techniques for optimisation of automatic analysis of huge quantities of events, information and evidence combining both structure and unstructured data in a privacy-aware manner for malicious action identification in cyber assets such as abnormal behavior.
- Specification of appropriate forecasting procedures and models which assist CII operators and security experts.
- Establishment of a Simulation Environment allowing investigators to design, model and execute simulations for the detection, analysis, visualization, containing and eradication of security events and propagation effects.
- Enabling identification and standardization of required information for sharing with relevant parties.
- Promotion and facilitation of trusted, secure and privacy aware data communication, maintenance and storage of forensic artifacts and evidential data.
- Integration of CyberSANE components into the CyberSANE system
- Deployment and Validation of the CyberSANE system in real operational environments.

To this end, the CyberSANE system targets at improving, intensifying and coordinating the overall security efforts for the effective and efficient identification; investigation, mitigation and reporting of realistic multi-dimensional attacks within the interconnected web of cyber assets in the CIIs and security events. From a technical perspective, the system collects, compiles, processes and fuses all individual incident-related information to ensure their integrity and validity following the generic phases of ISO/IEC 27035:2016 Information Security Incident Management. In contrast, from a cognitive point of view, the decision makers should be able to understand the technical aspects of an attack and draw conclusions on how to respond. The CyberSANE system consists of the following main and core structural elements /components:

- **The Live Security Monitoring and Analysis (LiveNet)**. It operates as the interface between the underlying Critical Information Infrastructure and the CyberSANE platform, combining security information and event management functions into one security management system. It undertakes the responsibility of preventing and detecting threats, providing to security professionals and experts both insights into and a track record of the activities within their IT environment. To achieve this, it monitors, analyses and visualizes their live network traffic in real time by collecting, in an organized manner, event data from various systems (i.e., installed devices, network/storage/streaming protocols, etc.). LiveNet provides operations, such as Attack Patterns Registration and Update, Live Monitoring, Security Event Classification and Notification, Signature Generation, etc.
- **The Deep and Dark Web Mining and Intelligence (DarkNet)**. It monitors the Dark and Deep Web in order to grasp and analyze the big picture of global malware/cybersecurity activities. It allows security professionals and experts to identify attacks before they even happen, giving them the opportunity to manage and close vulnerabilities in their organizational infrastructure, or even strengthen technical controls preemptively. Moreover, it allows the exploitation and analysis of security, risks and threats related information, embedded in the User Generated Content (UGC) via the analysis of both textual and meta-data content available from various electronic streams. It embeds operations, such as Incidents and Attack Techniques Identification, Tools for Advanced Cyber-Attacks detection, etc.
- **The Data Fusion, Risk Evaluation and Event Management (HybridNet)**. It provides the intelligence needed to perform effective and efficient analysis of security events on the information produced internally within the component, and on information and data derived and acquired by other CyberSANE components, especially the LiveNet and DarkNet components. In this vein, HybridNet analyses a large amount of data to further evaluate and correlate attack-related patterns associated with specific malicious or anomalous activities in the underlined CII. HybridNet provides risk assessment services, decision making and a simulation environment that allows Security Professionals to experiment on several cyber-attack scenarios and analyze the attack behavior.
- **The Intelligence and Information Sharing and Dissemination (ShareNet)**. It undertakes the proper identification of new attack patterns from the open web. ShareNet provides the necessary threat intelligence and information and shares useful incident-related information within the CIIs and with other relevant third parties (e.g., industry cooperation groups, Computer Security Incident Response Teams - CSIRTs) respecting the data sharing agreements required to be properly enforced. It provides operations, such as, Attack Pattern Collection, Protected Data Storage, Data Sharing Agreements, Knowledge Sharing, etc.
- **The Privacy & Data Protection (PrivacyNet) Orchestrator**. It is responsible for managing and orchestrating the application, regarding the required privacy mechanisms, maximizing achievable levels of confidentiality and data protection. It sets up the security and data privacy policies, allowing Security Professionals and Experts to specify all the protection rules and terms that must be performed, and the required conditions to execute them. This component is in very close interoperation with ShareNet, covering a wide range of techniques and mechanisms, including homomorphic cryptography, attribute-based and searchable encryption, anonymization, location privacy, multi-party, and verifiable computation, to meet highly demanding regulatory compliance obligations.

The CyberSANE components aforementioned comprise the **CyberSANE ecosystem**, depicted in Figure 4. The CyberSANE ecosystem hosts all project partners' tools that are utilized to support the significant set of services and features provided by those CyberSANE components.

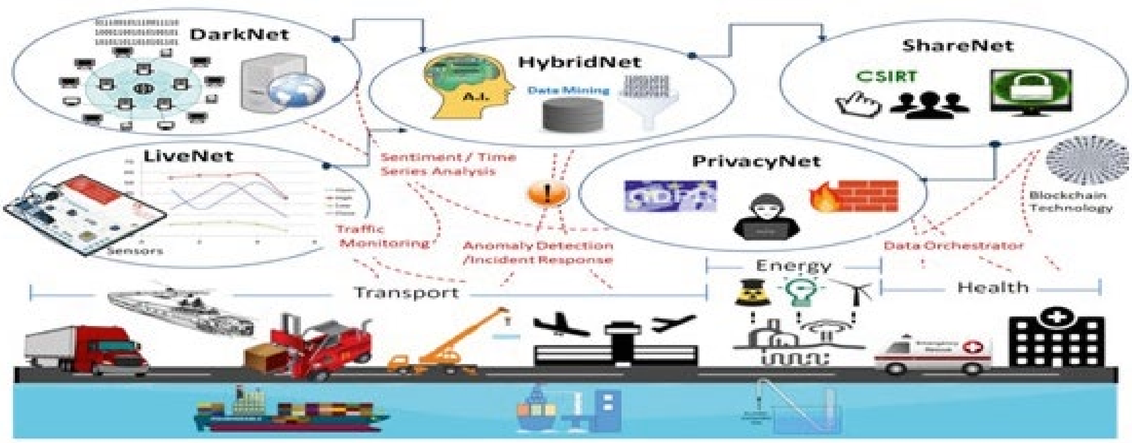


Figure 4 - CyberSANE Incident Handling Warning and Response System for the European Critical Infrastructures ecosystem.

The CyberSANE central Component is the heart of the CyberSANE system. It interoperates with the CyberSANE Ecosystem. It is the layer upon which the main CyberSANE services are built. Moreover, the **CyberSANE applications** refers to the CyberSANE system entity that hosts the main web. It facilitates the deployment of distinct experiences for all CyberSANE user types, devices, or specialized use cases that may require support during the project. In addition, **3rd party applications** refers to the CyberSANE system entity which integrates all 3rd party applications and tools, excluding those that provide the core services for the CyberSANE main components. The overview of the CyberSANE system architecture is shown in Figure 5.

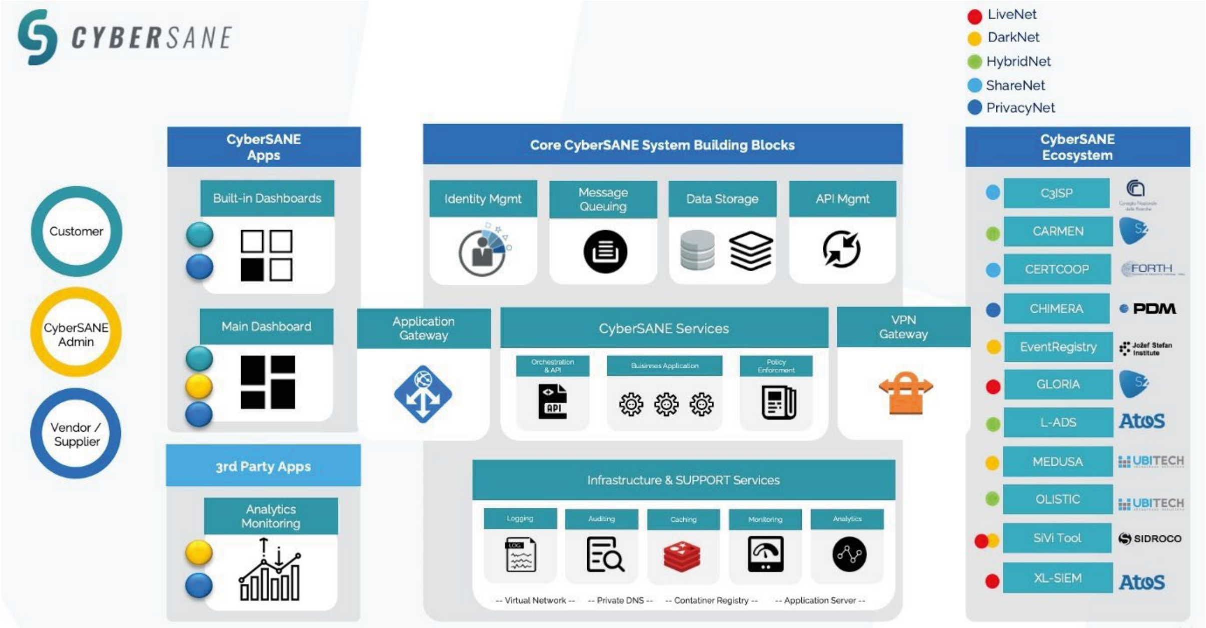


Figure 5 - The CyberSANE system architecture overview.

All CyberSANE structural elements provide a set of services and functionalities grouped in four different phases following the NIST Computer Security Incident Handling Guide which assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. Specifically, the CyberSANE system reflects the following incident handling phases:

- The **Preparation phase emphasizes** all actions required to be undertaken from an organization to be ready to respond to incidents but also to prepare from incidents by ensuring that systems, networks, and applications are sufficiently secure.
- The **Detection and Analysis phase** during which is determined whether the incident is really occurring and analyze its nature.
- The **Containment, Eradication and Recovery phase**, in which the incident response team tries to contain the incident and, if necessary, recover from it (restore any affected resources, data and/or processes).
- The **Post Incident Activity phase** during which Security Professionals and Experts attempt to determine specifically what happened, why it happened, and what the organization can do to keep it from happening again.

In the scope of testing and verifying the CyberSANE system functionalities under real conditions three pilots are considered from different Industries to gather as much feedback as possible from CII operators and stakeholders. These pilots are: the "**Container Cargo Transportation Pilot**" related to Port Transport and Logistics, the "**Solar Energy Production, Storage and Distribution Pilot**" concerning Energy Provider's procedures and the "**Cyber-threat Identification and Communication in Healthcare Pilot**" which addresses Hospital procedures. Each pilot implements the average of three different real-life scenarios, selected to test different corresponding features of the CyberSANE system. The first two pilots are already realized successfully, and fruitful feedback was received by pilot end-users. Moreover, the CyberSANE Port Transport and Logistics pilot was conducted on 2nd February 2022, whereas the CyberSANE Energy pilot took place on 5th April 2022. The demonstration event of the pilot related to healthcare is planned to run approximately between late June and at the beginning of July 2022.

More info about the project is available at https://www.cybersane-project.eu/ .

You may follow us on social media to reach project's live updates and blog posts on our latest events and achievements: CyberSANE Twitter, CyberSANE LinkedIn , CyberSANE YouTube

5.3 Cyber Securing Energy Data Services

CyberSEAS (https://cyberseas.eu/): Cyber Securing Energy Data Services by Paolo Roccetti, Head of Cysec research unit, Engineering (ENG)

The Electrical Power and Energy System (EPES) are rapidly evolving under the double boost created by digital transformation processes on one side, and by climate crisis on the other. This evolution aims at increasing the EPES efficiency and business continuity through the integration of new components, including HW and SW Commercial off-the-shelf (COTS) products, with legacy ones. Also, digital services are a key enabler of this process, building on an increased level of collaboration between all stakeholders connected to the power supply chain that relies on near real-time availability and exchange of data and knowledge. This causes a major increase in cyber exposure which can lead to major consequences, as witnessed by recent ransomware attacks to the Colonial Pipeline [Kerner 2022] and to Ukrainian energy companies over recent years [Polityuk 2017], [ESET 2022].

In this emerging context, effective solutions for protecting EPES from such high-impact cyber-attacks are of paramount importance. CyberSEAS focuses exactly on these attacks, which not only have the highest potential of disrupting the business continuity of critical elements in the energy distribution, but also – and most importantly – result in major safety incidents, with loss of lives and substantial damage to infrastructure (including cascading effects) and critical privacy breaches. CyberSEAS considers the challenges and the constraints resulting from the increasing use of decentralized renewable energy sources and the large proportion of legacy systems that will continue to co-exist in extended energy supply chains involving a variety of diverse operators and consumers. CyberSEAS also covers attacks targeting the confidentiality of citizens' data, as well as on the privacy and the integrity of the Energy data space in general.

CyberSEAS aims at addressing the aforementioned challenge by means of three strategic objectives (SO):

- **SO1 - Countering the cyber risks related to the highest impact attacks against EPES**, which are those resulting in attacks that (i) have the highest impacts, (ii) are predicted to grow exponentially in the next years, and (iii) encompass mechanisms that are only very recently being understood or still to be discovered.

- **SO2 – Protecting consumers against personal data breaches and cyber-attacks**, which is characterized by two main aspects: (i) protects consumer's personal data against attacks and (ii) protects the supply chain as a whole from attacks that exploit consumers as channels of attack, especially in their role as active party (prosumers) in the energy chain.

- **SO3 - Increasing security of the Energy Common Data Space**, by (i) enhancing the governance related to exchanging operational data across interconnected EPES, (ii) integrating those specific needs related to end-to-end resilience and (iii) achieving the right balance between data managed in relation to its sensitivity level and the need for real-time detection of cyber threats.

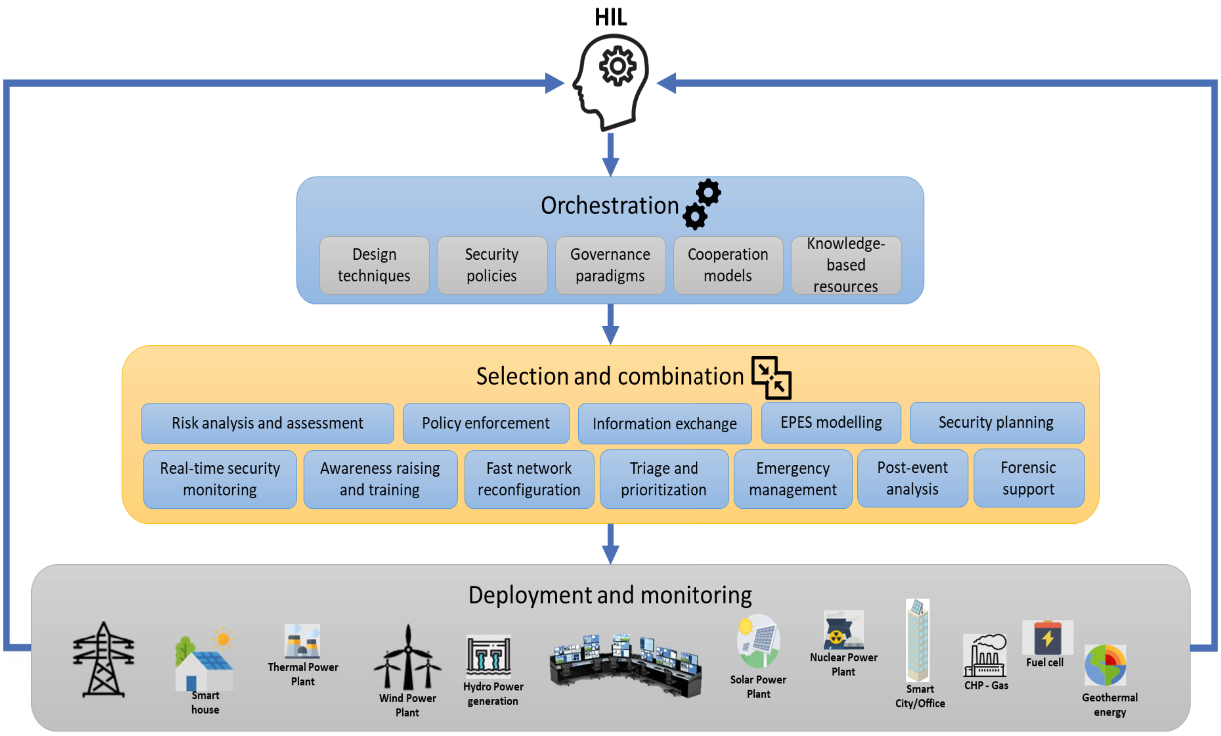


Figure 6 - CyberSEAS ecosystem

To support the three SOs introduced above, CyberSEAS foresee the provisioning of **Methodological Measures (MMs)** and **Technological Measures (TMs)** for EPES operators. Methodological Measures includes the design techniques, security policies, governance paradigms, cooperation models, and knowledge-based resources in general that can be exploited to increase the security level of EPES via increased situation awareness. In turn, Technological Measures include tools and services providing security-enhancing features specifically tailored to the needs of EPES, and in particular: risk analysis and assessment, real-time security monitoring, awareness raising and training, policy enforcement, information exchange, EPES modelling, security planning, triage and prioritization, fast network reconfiguration, emergency management, forensic support, and post-event analysis.

These MMs and TMs will be part of an ecosystem that can be customized and combined based on the specific characteristics of individual setups to improve the resilience of EPES infrastructures against cyber-attacks. These measures and solutions are dynamically orchestrated according to a Human-In-the Loop (HIL) approach – as shown in the picture below – where the orchestration process exploits CyberSEAS MMs to effectively combine CyberSEAS TMs and iteratively apply them to the infrastructure to be protected. This results in a dramatic innovation of the business and organizational models of the enterprise, which enables a continuous improvement process of the resilience of the EPES.

To sustain its proposition the CyberSEAS ecosystem can count on a collection of 30 tools, already available in partners' portfolios as solutions or prototypes, which the project will make interoperable in an integrated flow that can be taken up as a whole, or through combinations of customized subsets of tools that can interface to pre-existing environments of individual operators. Different subsets are made available and tested during the project through 100+ scenarios in 5 different infrastructures. The set of processes to ease the uptake and deployment of tools, the internal collaboration between operators as well as the external collaboration with CERT's form part of the CyberSEAS 's governance.

During its initial phase, CyberSEAS performed a thorough and interdisciplinary analysis of vulnerabilities and failures related to cyber and privacy attacks and data breaches, including cascading effects across the energy end users. The work took an integrated approach that considered both technical and technological aspects related to EPES devices, as well as organizational and human factors related to the various stakeholders.

The work started with the identification of the structure and operation of EPES components and services, including the definition and modelling of interactions among them and with external infrastructures. The resulting asset model is an extension of the SGAM model framework [CEN-CENELEC-ETSI 2012] which includes the human layer where employees of EPES operators are considered. After the asset identification, various assessments have been conducted to link assets to vulnerabilities and to estimate impacts in a collaborative manner, i.e., involving all partners from the energy supply chain. Finally, the information from the analysis is being used to create meaningful and realistic use cases which will drive the definition of the methodological and technical measures, as well as the adaptation of the tools which are part of the CyberSEAS ecosystem, in the second phase of the project.

During the third phase, CyberSEAS will validate its results through a progressive piloting approach that will start with a laboratory deployment and continue with on-site deployments. Laboratory deployment will be especially useful (i) in the first phases of the experimental campaigns, when on-site deployments may not be available yet and (ii) in all phases of the experimental campaigns when potentially destructive tests are to be performed. In turn, on-site deployments are protected environments provided by operators in Croatia, Estonia, Finland, Italy, Romania and Slovenia consisting of the same infrastructure (or an equivalent one) that would be used in operation. These will be used (i) in all phases of the experimental campaign, for experiments which do not have destructive effects and (ii) in the “ex-ante” and “ex-post” penetration testing experiments that will be done to evaluate the resilience improvement achieved.

More info about the project is available at https://cyberseas.eu/.

5.4 Privacy-preserving AI in Systems Medicine with Federated Learning

FeatureCloud (featurecloud.eu): Privacy-preserving AI in Systems Medicine with Federated Learning by Julian Matschinske, University of Hamburg

FeatureCloud is a platform for federated machine learning, focused on Biomedicine. It enables collaborative machine learning across multiple facilities. Specifically, it facilitates the development of federated algorithms, by providing an open API, as well as deployment, distribution, and execution of algorithms through configurable workflows. It comes with several privacy-preserving techniques, such as differential privacy (DP) and secure multiparty computation (SMPC) to increase privacy-awareness of the platform to further increase privacy-awareness of the system. During development, FeatureCloud helps with an execution simulator, mimicking a federated workflow to test and debug the implementation.

Partners from across Europe (Germany, Austria, Denmark, the Netherlands, and Romania) collaborated to combine their respective expertise ranging from supervised to unsupervised, theoretical to practical, and legal to technical knowledge on machine learning and conducting of medical studies. After two years of development, a functioning version is up and running and open to 3rd-party developers to contribute their apps. As of mid-2022, about 30 apps are in the AI store for various ML tasks, such as model training, dimensionality reduction, normalization, cross-validation and visualization. Figure 7 shows the interplay between the overall system and the users.

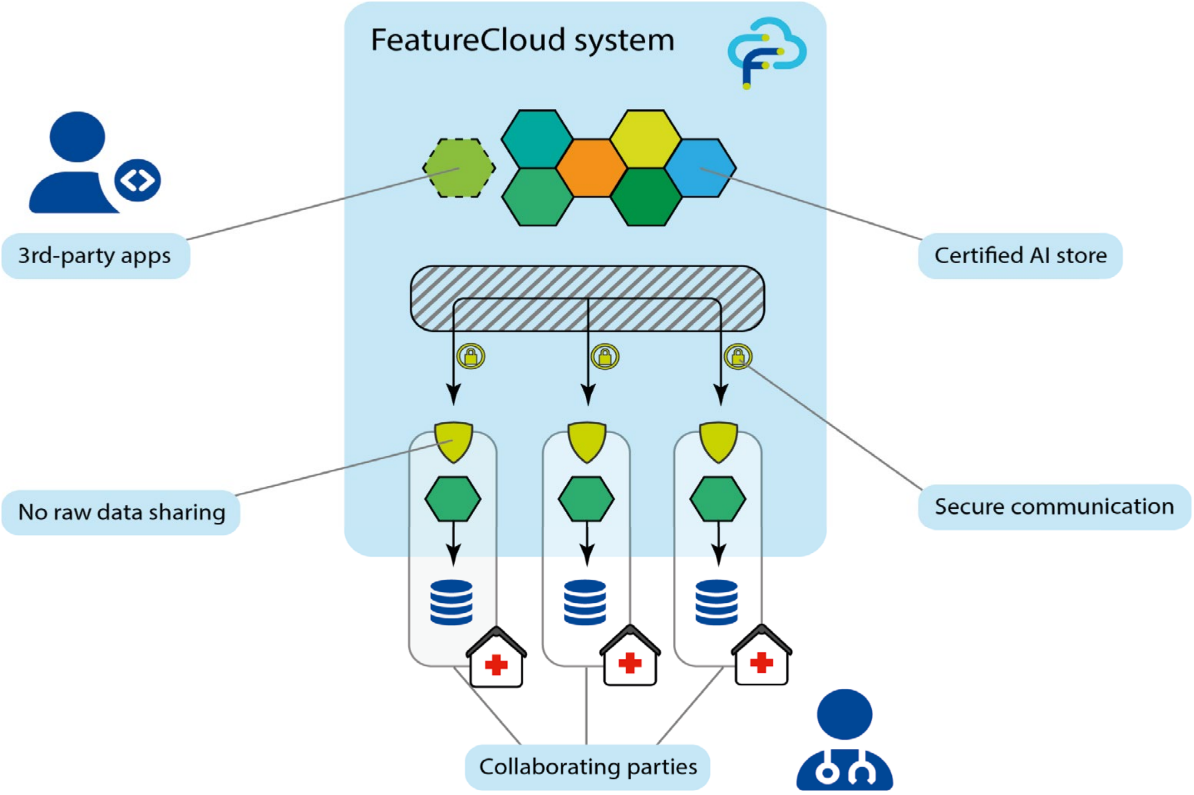


Figure 7 - The overall FeatureCloud system provides access to 3rd-party developers, isolates app execution on the hospital infrastructure and enables non-developers to use existing apps with their own data.

Architecture and implementation. FeatureCloud is a multi-component system consisting of parts running on local infrastructure (controller) and on global servers (relay server and backend). It mostly uses web technologies, i.e., the HTTP protocol and JSON as serialization technique. For workflow communication between apps, an own TCP/IP-based protocol has been implemented to minimize overhead. For isolation of apps, we use Docker containers that are orchestrated by the local controller component. To aid developers, there is a PIP package command-line interface (CLI) that can be used to start and stop the controller, create new app projects, test and debug the federated app implementation.

Results and evaluation. Several standalone tools [Nasirigerdeh 2020, Zolotareva 2021] have been implemented before or in parallel to FeatureCloud, serving as a proof of concept. These tools then have been turned into FeatureCloud apps, making use of the consolidated platform. Evaluations on various datasets have been conducted, demonstrating that federated learning yields satisfactory results in most cases, with non-identically distributed data still posing a challenge [Hauschild 2022].

Challenges. Several challenges have had to be overcome, particularly strict conditions regarding hospital IT infrastructure. FeatureCloud requires minimal changes, if any, to run on hospital IT as it does not require anything more than an outgoing internet connection and provides isolation of running apps. Still, varying architectures, operating systems and levels of technical knowledge make it challenging to offer a version that works out of the box for everyone. During the first international FeatureCloud hackathon in June 2022 with participants from all over the world, we learned that most technical barriers could be overcome, and participants found it straightforward to implement apps for the AI store.

Next steps. As next steps, FeatureCloud plans to include a federated database connection to allow for automatic collaboration based on registered datasets to facilitate large-scale AI studies further and remove manual steps. Also, trained models will be available in a model store, so that medical doctors and researchers can apply pre-trained models on their data.

5.5 Shielding the power grid from cyberattacks

EnergyShield (energy-shield.eu): Shielding the power grid from cyberattacks by Otilia Bularca, SIMAVI

EnergyShield project is an Innovation Action aiming at "capturing the needs of EPES operators and combining the latest technologies for vulnerability assessment, supervision and protection to draft a defensive toolkit". The project started in July 2019 and has a duration is 36 months. 18 partners from 10 different EU Member States and Associated Countries have embarked on this project to create a toolkit that has the capabilities of defending the smart grids.

The objectives of EnergyShield project are to:

- Adapt and improve available tools to support the needs of EPES
- Integrate them into a holistic solution
- Validate the practical value of the EnergyShield toolkit in demonstrations involving EPES stakeholders
- Develop best practices, guidelines and methodologies to support the deployment of projects results

Starting from 5 existing tools, we have extended functionalities, adapted them to the needs of EPES and combined them all in a defensive toolkit as shown in Figure 8.

The proposed toolkit comprises of five existing tools that technology providers are improving and adapting to the needs of EPES sector:

- The assessment tools (Vulnerability Assessment, Security Behaviour Analysis) - provide information on most critical attack vectors and probable paths.
- The monitoring tools (Anomaly Detection, Distributed Denial of Service Mitigation) provide early warning on incoming attacks and malware
- Learning and sharing tools (Security Information and Event Management) provide feedback on the proposed attack vectors by enabling real-time incident logging and analysis for immediate sharing throughout the industry (i.e., decision-support tools to coordinate cyber defender response across the EPES value chain).

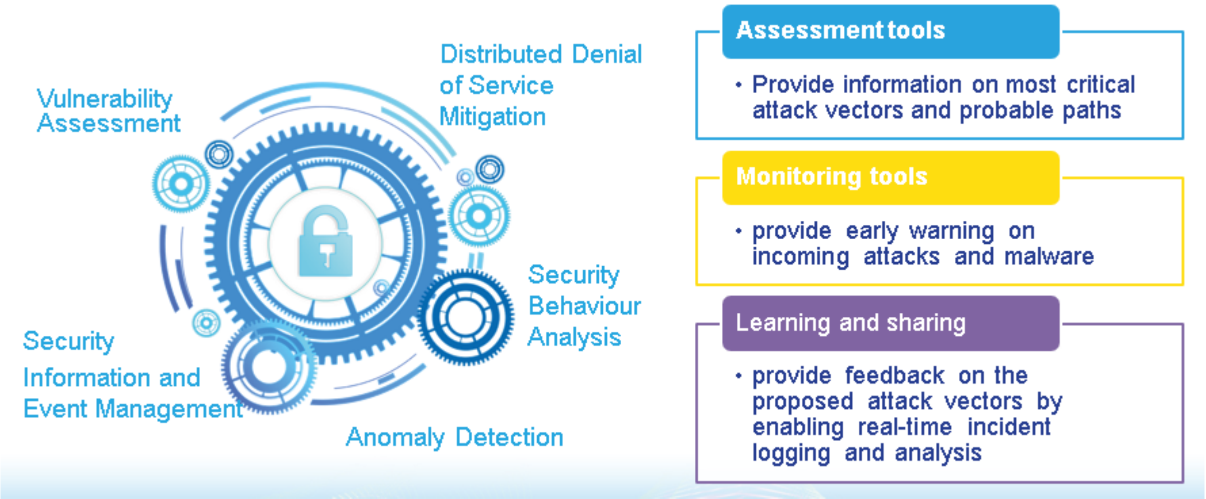

Vulnerability Assessment
Distributed Denial of Service Mitigation
Security Behaviour Analysis
Security Information and Event Management
Anomaly Detection
Assessment tools
• Provide information on most critical attack vectors and probable paths
Monitoring tools
• provide early warning on incoming attacks and malware
Learning and sharing
• provide feedback on the proposed attack vectors by enabling real-time incident logging and analysis

Figure 8 - EnergyShield tools presentation

The above tools and toolkit are demonstrated in a large-scale pilot studying the cascading effects of cyberattacks throughout the EPES value chain in Bulgaria and in Italy in a small-scale pilot, where the Consortium is performing a feasibility study on a dedicated, simulation area of the networks control systems. Mitigation of cyber-attacks and data breaches and identification of threats and vulnerabilities are among the expected results of the project.

Considering the technical activities, the project is approaching closure and partners are collecting & consolidating the results. The dashboards with the planned activities look as follows:

- The analysis and architecture design activities are now complete
- Technology providers continue the development of tools (final release in December) and have started the integration of tools and deploying the equipment on site.
- A first version of the EnergyShield toolkit was also release
- The practitioners have been actively involved in the validation of the tool's functionalities
- The evaluation and testing frameworks were drafted
- Currently focusing on field trials activities

EnergyShield policy contributions. The relevance of a toolkit for Critical Infrastructures (CI) / EPES - like the one proposed by EnergyShield - was evaluated during project implementation. The supply chain for CI has gotten recently and software supply chain risks become additionally very visible (e.g., Solar Winds incident). To this end, the need for complex systems that are fully flexible and ensure different deployment possibilities and easy adoption of new technologies is highly relevant. Moreover, the current market shows the existence of many cross-sector tools and a limited offer for the energy sector. The latest incidents however provide good arguments for the exploitation of a toolkit like EnergyShield.

Risk assessment is a policy topic also approached as part of the EnergyShield project and it covers the following steps: (1) identification of critical assets as part of VA tool & identification of specific cyber-threats on the achieved socio-cultural behaviour; (2) Assessment - using specific methodologies: Risk matrix, MITRE ATT&CK and (3) Modelling with CVSS scoring of vulnerabilities and MERIT**.** The vulnerability assessment tool assesses the cyber security resilience through threat modelling and attack simulations (drafts critical paths and determines the time to compromise a critical asset. (The tool also collects the attacker's most likely path and plots the probability of the attacker reaching the asset), while the security behavior analysis tool evaluates the current security readiness of an organization's workforce.

Assessment, monitoring protection and learning tools are accommodated in a toolkit that provides continuous monitoring, exposes REST APIs that enable tools interoperability and integration with other tools, offers asynchronous message exchange, allowing external systems to subscribe to the topics.

EnergyShield toolkit (Figure 9) includes container engine (Docker), Authentication and Authorization (Keycloack), Communication system (Kafka), REST, and Process management (Kubernetes). The whole architecture is federated. There is a central federation Coordinator where federation members are locally deployed; the central component is responsible for maintaining the rules and standards, for common processing, while the federation members are responsible for local data collection and processing.

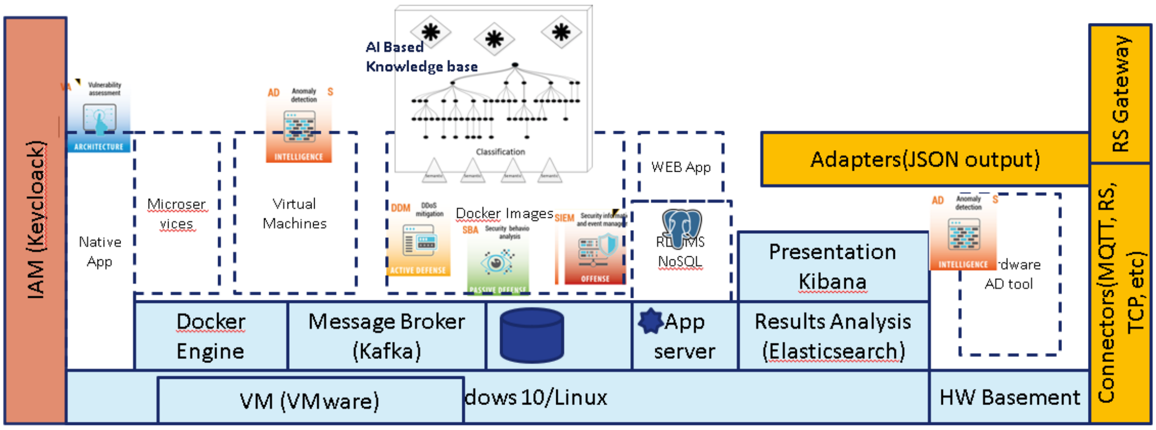


Figure 9 - EnergyShield toolkit

Energy Shield Consortium has also worked on a number of concept tools approaching: (1) cybersecurity supply chain risk analysis (chain of software and hardware components that are part of tools such as control systems that are used to operate critical energy infrastructures.), (2) automated forensic tool (enrich events identified by the embedded vulnerability detector module with information deriving from different security databases, such as CWE, CAPEC, OVAL, WASC, OWASP) and (3) searchable Encryption and Homomorphic Encryption (anonymize and search data in the encrypted domain using the state-of-the-art homomorphic encryption techniques)

Lessons learned. An important outcome of the EnergyShield project refers to what Consortium partners have learned during implementation.

Building online identity is essential. EnergyShield has a consolidated presence online: Twitter and LinkedIn are preferred as social media tools. A constantly updated website is also available and includes project reports, scientific articles (26 until now) and short communication articles. A collaboration was established with 15 H2020 projects, while also being foundation members in ESCI and CyberEPES clusters.

Another important lesson is that **flexibility is key**. Starting from a plethora of technologies and use case functionalities the EnergyShield system needs to provide full flexibility. In adapting and integrating technologies the technology providers have improved and adapted the tools making them ready for integration through the overall EnergyShield system and interacted with Practitioners to collect feedback (testing and evaluation of tools. Also, a flexible integration concept was designed and is being implemented to ease the accommodation of tools and a Portal to securely access the toolkit.

Technology providers have collaborated towards preparing and accommodating tools using different technologies in a common environment (EnergyShield toolkit) and using a data fusion mechanism combined with machine learning to create a global view.

A series of **challenges** were also faced during implementation: (1) OT and IT integration and testing; (2) integration itself due to a wide area of technologies used; (3) working with different business aspects (from behaviour analysis to anomaly detection and monitoring.

More info about the project: www.energy-shield.eu, @EnergyShield_,

5.6 Securing the e-commerce ecosystem from cyber, physical and cyber-physical threats

ENSURESEC (www.ensuresec.eu): Securing the e-commerce ecosystem from cyber, physical and cyber-physical threats by Luís Júdice Sousa, INOV

E-commerce is the primary pillar of the European Digital Single Market and as such it is a critical ecosystem for the future and autonomy of the European Union (EU). The relevance of e-commerce for EU economy was already patent before the emergence of the COVID-19 pandemic, with the total volume of e-commerce transactions reaching €621 billion during 2019 [Ecom 2019], but this pandemic significantly accelerated the growth of digital commerce [Ecom 2021]. This context makes e-commerce an attractive area for cyber-crimes. For instance, in 2016, the EU suffered €1.32 billion of fraud losses through e-commerce payments [ECB 2018], while 73% of global e-commerce declared fraud incidents occurred in the EU. Due to its size, financial impact, often poor IT practices and highly complex services, the sector is often suffering from cybersecurity threats resulting in a substantial financial and physical loss. Moreover, the e-commerce ecosystem involves actors with different social and technical characteristics, from citizens, technical vendors, numerous levels of cyber and physical services and their underlying soft and hard infrastructures, i.e., delivery services and physical security services. This makes the security handling of e-commerce services exceptionally complex, having to address a large attack surface with limited visibility of the entities involved in their value chains.

In this context, ENSURESEC's overarching objective is to equip e-commerce infrastructures and ecosystems with through-life protection against cyber, physical, and cyber-physical threats, including cascading effects, thus contributing towards the vision of a reliable and trusted European Digital Single Market. ENSURESEC is a sociotechnical solution for safeguarding e-commerce operations against both cyber and physical threats. It combines an automatic, rigorous, and distributed toolkit for protecting e-commerce, with monitoring of the impact of threats in physical space and a campaign for training e-commerce customers aimed at creating awareness and trust. The project addresses the whole gamut of modern e-commerce, from standard physical products purchased online and delivered via post, to entirely virtual products or services delivered online. It addresses threats ranging from maliciously modifying web e-commerce applications or rendering them unavailable to legitimate customers, to delivery issues or fraud committed by insiders or customers. It achieves this by focusing on the common software and physical sensor interfaces that sit along the e-commerce, payment, and delivery ecosystem. At technical level, it integrates proven state-of-the-art inductive (machine learning) with deductive (formal methods) reasoning tools and techniques so that e-commerce operations are protected by design, as well as through continuous monitoring, response, recovery, and mitigation measures at run-time. Although ENSURESEC innovations are applicable to any critical infrastructure that relies on and is monitored by networked software systems, its design and integration philosophy make it uniquely prepared to protect distributed and evolving e-commerce infrastructures with its various forms of payment and delivery (virtual, online, and physical).

ENSURESEC also enhances citizens' resilience to threats and their trust in e-commerce companies, especially SMEs, thus contributing towards the vision of a reliable and trusted digital single market.

The project has started in June 2020, and it has been successfully concluded in May 2022. In sum, the main objectives of the ENSURESEC project were the following:

- Identify critical cyber and physical interfaces of the e-commerce ecosystem and their associated security threats with cascading effects and cyber, cyber-physical and physical impact
- Identify ENSURESEC's technical, user, legal and ethical requirements for a diverse range of use cases involving e-commerce critical infrastructure against combined cyber, cyber-physical and physical threats with their cascading effects
- Integration of the design-time, threat detection and security enforcement, incident response and impact mitigation, as well as impact assessment and situational awareness components into a unified toolkit
- Evaluate the ENSURESEC platform in relevant environments
- Conduct a security awareness and training campaign for citizen users of e-commerce SMEs

The technical part of the ENSURESEC solution was a cyber-physical security toolkit, which operates as a platform of security tools to protect an e-commerce operator (Figure 10), by integrating with the existing complex infrastructure of the companies which are part of the e-commerce ecosystem. Figure 10 presents the conceptual architecture of the ENSURESEC toolkit.

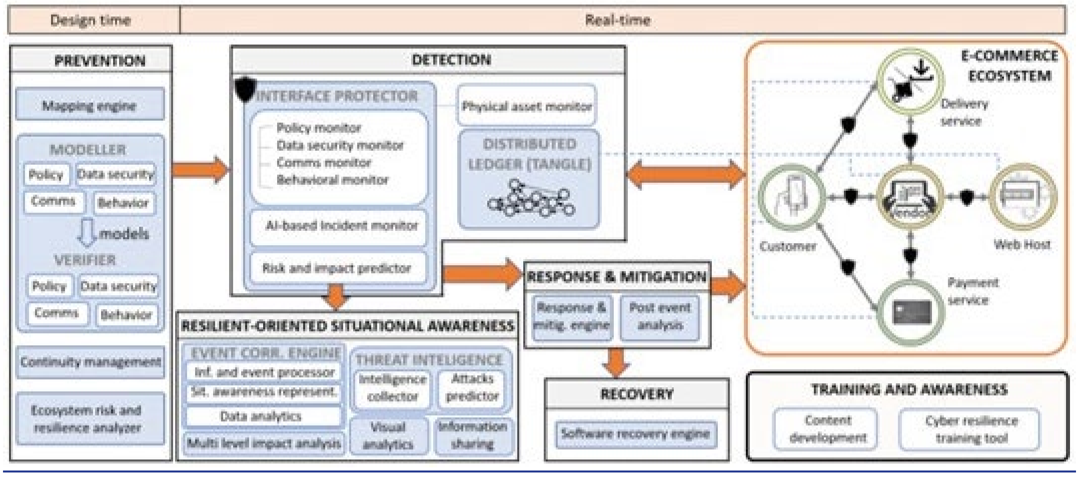


Figure 10 - ENSURESEC conceptual architecture

The ENSURESEC concept is based on a low-cost security toolkit deployed to protect the interfaces of the e-commerce ecosystem, through the integration of 4 main modules:

- **Prevention (by design)** – Assesses and certifies that the design of the system interfaces is secure against certain classes of critical attacks and vulnerabilities. This module is composed of 4 components: (i) the Mapping Engine that maps cyber, cyber-physical and physical components of the ecosystem and determines the qualitative and quantitative risk of certain threats and attacks to the infrastructure based on that mapping; (ii) the Modelling and Verification tool, which models and verifies the implementation of cyber and physical interfaces and their associated threats (e.g. application behaviour, cryptographic libraries, etc.); (iii) the Business Continuity Management maturity assessment tool, which allows assessing the maturity of the business continuity processes and policies of an organisation based on industry standards; and (iv) the Risk and Resilience Management maturity assessment tool, which assesses the implementation of risk management processes within an organisation to identify shortfalls.

- **Detection and security enforcement** – this module enforces the security of the ecosystem in real-time by monitoring run-time interface operations at the application level and network level for resilience against both known and unknown threats. It is composed of 6 different monitors: (i) the Behavioural Monitor; (ii) the Data Security Monitor; (iii) the Communications Monitor; (iv) the Physical Assets Monitor; (v) the Policy Monitor; and (vi) the AI-based Incident Monitor.
- **Response, mitigation and recovery** – this module is responsible for responding to the incident and communicating it to business and services partners and their citizen clients on one hand, and initiating a corresponding mitigation strategy to eliminate or reduce the impact of the incident on the other hand. The module includes a response and mitigation engine, an audit trail based on distributed ledger technologies to extract all logs of the operations of the compromised interface in an immutable way, a software recovery engine to assure continuous availability of the e-commerce critical infrastructure even in it is under cyber-attack, and a post-event analysis tool that produces a knowledge base of post-events and security incidents for future analysis.
- Situational awareness – this module goes beyond classical security situational analysis tools and employs advanced machine learning and data analysis techniques to continuously perform situational analysis of suspected and current incidents and to determine their impact.

In total, the ENSURESEC toolkit is composed of 19 tools, 9 of them working as backend tools, and the remaining being user-facing, i.e., to be part of a Security Operations Centre. The ENSURESEC user-facing tools are available to the user through a common dashboard, that provides a continuous situational picture of the e-commerce critical infrastructure and allows the user to seamlessly navigate through each of the tools (Figure 11).

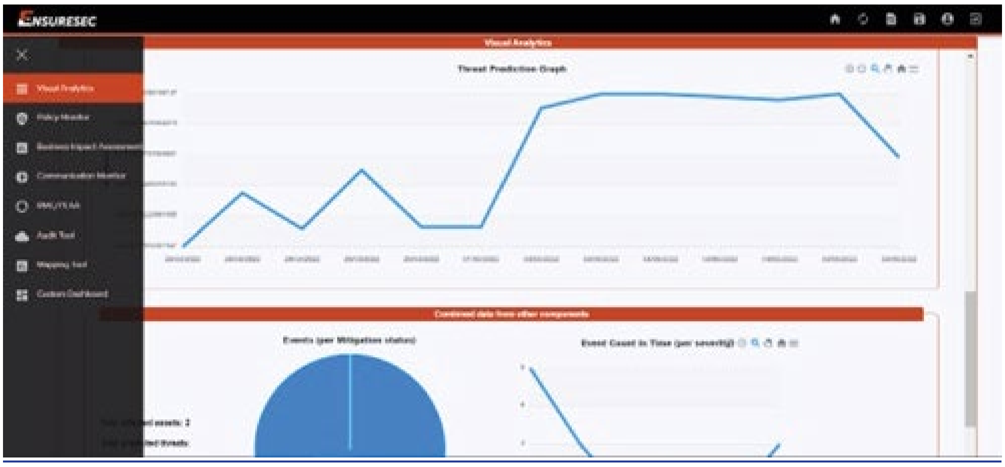


Figure 11 - View of the ENSURESEC Global Dashboard

The ENSURESEC toolkit was demonstrated and validated by end-users in 3 complementary pilots, composed of different scenarios. The first pilot was focused on **Cyber-attacks to an e-commerce platform**, in which the main end-user was a multinational retail company (Sonae MC), and where the main goal was the protection of customers' data. The second pilot comprised **Physical attacks on pharmacy e-commerce operators**, in which the whole e-commerce supply-chain was represented by the participation of specific end-users: online pharmacy operator (TOFAR), logistics and transportation company (Milsped), and physical security and VIP transportation company (G4S). Finally, the third pilot focused on **Cyber-physical attacks to a Bank providing online payment services**, where the end-user was one of the biggest banks in Spain (CaixaBank). In order to address the specificities of each pilot, different configurations of the ENSURESEC toolkit were deployed, also demonstrating the versatility and adaptability of the solution. Moreover, each pilot was also deployed in a different type of environment: the first pilot was executed in a simulated environment that realistically represented Sonae MC's data handling infrastructure; the second pilot was carried out in real operational conditions, comprising the transport of pharmacy products from Greece to Serbia; the third pilot was executed in a sandbox environment provided by CaixaBank that is used by this end-user to test new security technologies. All three pilots have been successfully executed, and very positive feedback was received from the project end-users, as well as external stakeholders such as the members of the ENSURESEC Advisory Board.

In addition to the technical solution, the ENSURESEC concept also encompasses a social dimension, which has been implemented in the form of an e-commerce-tailored cybersecurity training and awareness campaign, aimed at customers of digital commerce. In order to set-up the campaign, the consortium carried out consumer behaviour studies and investigated malicious marketing techniques, as well as tools, techniques and procedures currently used for both legitimate purposes in digital marketing, and for malicious purposes to commit online frauds and other cybercrimes. This allowed to identify common e-commerce and social media human interaction vulnerabilities that can be exploited by malicious users, in order to shape the campaign accordingly.

The ENSURESEC cybersecurity training and awareness campaign is composed of content and tools, including illustrations, videos and descriptions of the most common threats for e-commerce customers, as well as attack simulations, in order to educate online consumers on how to identify malicious practices in e-commerce and how to avoid them. This campaign, available in 6 European languages (English, German, Italian, Spanish, Greek and Romanian) was launched in the form of a website – accessible at https://becyberaware.eu/ – in which citizens can find videos explaining a number of different threats (e.g. phishing, smishing, QRishing, fake reviews), and carry out self-assessment tests to evaluate their current awareness towards each of these kinds of threats. The website also provides the possibility to register for free for a training campaign, which is delivered through sample phishing emails, fake malicious landing pages, among others. A dedicated Youtube channel [Aware] was also created to disseminate the awareness videos. With this contribution, the ENSURESEC project aims at raising e-commerce customers' awareness towards the risks and threats of online shopping, and in this way increase the resilience of the whole ecosystem. During the project execution, the campaign was highly successful, reaching more than 20,000 people across Europe and abroad. The BeCyberAware website and YouTube channel will continue online even after the end of the project, in order to keep raising awareness towards e-commerce threats.

More information about ENSURESEC: https://www.ensuresec.eu/; ENSURESEC LinkedIn; ENSURESEC Twitter

5.7 Empowering a Pan-European Network to Counter Hybrid Threats

EU-HYBNET (euhybnet.eu): Empowering a Pan-European Network to Counter Hybrid Threats by Päivi Mattila, Isto Mattila (Laurea), Rolf Blom (RISE), Maria Kampa (KEMEA), Monica Cardarilli (JRC).

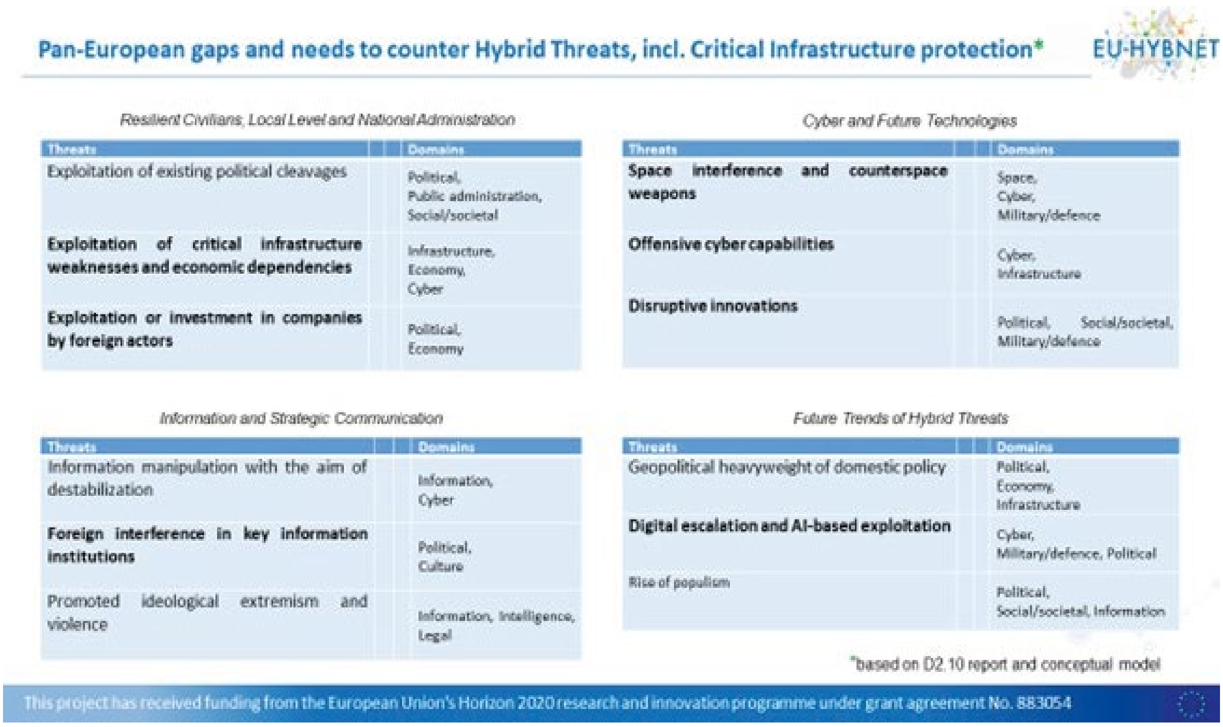
Abstract on the EU-HYBNET Projects' Main Objectives

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties [EU 2016]. The EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats) project brings together pan-European practitioners and stakeholders to identify the challenges in countering hybrid threats. Thorough research activities are conducted for the identification of innovations to counter hybrid threats, and training events are organised to test innovations and proceed with recommendations for their uptake, industrialization and standardization. The project results are shared with EU practitioners & policymakers, which has a positive influence on the public procurement process. In EU-HYBNET the definition of hybrid threats is based the EC document "Landscape of Hybrid Threats. The Conceptual Model" written by the JRC and the European Centre of Excellence for Countering Hybrid Threats (Dec 2020). EU-HYBNET is funded by the European Commission Horizon 2020 program for years 2020-2025, Grant Agreement No. 883054. https://euhybnet.eu/

This paper focuses on the main results of EU-HYBNET Work Package (WP) 2 "Gaps and Needs of European Actors against Hybrid Threats"/ Task (T) 2.2 "Research to Support Increase of Knowledge and Performance" (JRC) and WP4 "Recommendations for Innovations Uptake and Standardization"/ T4.2 "Strategy for Innovation uptake and industrialization" (RISE). The paper introduces T2.2 latest findings on pan-European security practitioners and other relevant actors (industry, SMEs, academia, NGOs) gaps and needs, vulnerabilities to counter hybrid threats focusing on topics relevant to the CI domain. All T2.2 identified gaps and needs are presented according to the EU-HYBNET project four core themes: future trends of hybrid threats; cyber and future technologies; resilient civilians, local level and administration; and information and strategic communications. For each of the gaps and needs under a project core theme, key domains where the hybrid threats may occur are highlighted. In this paper also an innovative solution identified in EU-HYBNET T4.4 to support Critical Infrastructure (CI) operators to counter hybrid threats is shortly described. The innovation is about information sharing between public-private CI operators on a voluntary basis to enhance CI operators' measures to detect and counter hybrid threats. Lastly, the paper highlights topics for future research to increase knowledge of measures to counter hybrid threats in the CI domain.

Present EU-HYBNET Focus on Hybrid Threats in Critical Infrastructure Domain

According to the latest EU-HYBNET T2.2 research on pan-European security practitioners' and other relevant actors' (industry, SMEs, academia, NGOs) gaps and needs to counter hybrid threats are described in Figure 12 as "threats". The gaps and needs, threats focusing on CI domain are highlighted in the table in **bold**.



Pan-European gaps and needs to counter Hybrid Threats, incl. Critical Infrastructure protection*

Resilient Civilians, Local Level and National Administration

Threats	Domains
Exploitation of existing political cleavages	Political, Public administration, Social/societal
Exploitation of critical infrastructure weaknesses and economic dependencies	Infrastructure, Economy, Cyber
Exploitation or investment in companies by foreign actors	Political, Economy

Cyber and Future Technologies

Threats	Domains
Space interference and counterspace weapons	Space, Cyber, Military/defence
Offensive cyber capabilities	Cyber, Infrastructure
Disruptive innovations	Political, Social/societal, Military/defence

Information and Strategic Communication

Threats	Domains
Information manipulation with the aim of destabilization	Information, Cyber
Foreign interference in key information institutions	Political, Culture
Promoted ideological extremism and violence	Information, Intelligence, Legal

Future Trends of Hybrid Threats

Threats	Domains
Geopolitical heavyweight of domestic policy	Political, Economy, Infrastructure
Digital escalation and AI-based exploitation	Cyber, Military/defence, Political
Rise of populism	Political, Social/societal, Information

*based on D2.10 report and conceptual model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

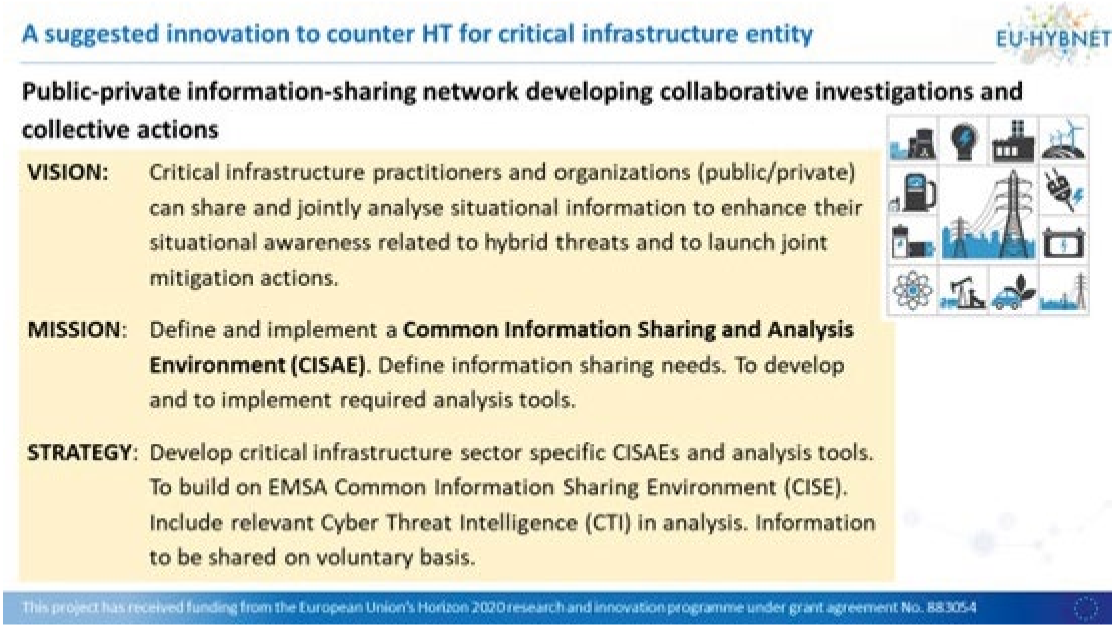
Figure 12 - EU-HYBNET T2.2 latest research results on pan-European security practitioners and other relevant actors' gaps and needs, "threats" to counter hybrid threats.

As Figure 12 describes in the economic domain hybrid threats are identified to take place especially in the form of "Exploitation of CI weaknesses and economic dependencies" and "Exploitation or investment in companies by foreign actors". From a technology perspective "Offensive cyber capability" remain a key challenge to CI operators and "Disruptive innovations" and "Digital escalation and AI-bases exploitation" are seen to increase possibilities for a new type of and severe hybrid attacks and threats. "Space interference and counter space weapons" are identified as a CI area requesting enhanced measures to counter hybrid attacks. It is also important to keep in mind that hybrid attacks may take place in other than the CI domain, e.g., in the information or political or administration domain, but still aim to harm CI operators. From this perspective "Foreign interference in key information institutions" may cause serious hybrid threats in the CI domain as a result of cascading effects.

At present, the EU-HYBNET project is discovering innovations that may deliver solutions to the above-mentioned, identified threats. However, from the earlier EU-HYBNET gaps and needs analysis and promising innovations mapping to the gaps and needs, an innovation was discovered to support CI entities to enhance their measures to counter hybrid threats. The Innovations is focusing on a public-private information-sharing network developing collaborative investigations and collective actions.

An Innovation to Enhance CI operators Measures to Hybrid Threats

The "public-private information-sharing network developing collaborative investigations and collective actions" innovation was discovered to answer CI entities needs to learn and to know more about the hybrid threats - how they can take place, in what kind of form etc. The goal is to increase awareness on similar hybrid attacks to own CI entity from the other CI entities, in addition the importance is also to learn how the hybrid threats may take place and to evolve. The information sharing supports not only preparedness but also response to hybrid attacks. The main element in the innovation is described in Figure 13.



A suggested innovation to counter HT for critical infrastructure entity

Public-private information-sharing network developing collaborative investigations and collective actions

VISION: Critical infrastructure practitioners and organizations (public/private) can share and jointly analyse situational information to enhance their situational awareness related to hybrid threats and to launch joint mitigation actions.

MISSION: Define and implement a **Common Information Sharing and Analysis Environment (CISAE)**. Define information sharing needs. To develop and to implement required analysis tools.

STRATEGY: Develop critical infrastructure sector specific CISAEs and analysis tools. To build on EMSA Common Information Sharing Environment (CISE). Include relevant Cyber Threat Intelligence (CTI) in analysis. Information to be shared on voluntary basis.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Figure 13 - Ideas & Innovations proposed to counter Hybrid Threats, EU-HYBNET Deliverable 4.4 [RISE 2021]

A key element in information sharing is that CI entities will decide on their own which type of information they wish to share with other CI entities – the sharing would take place on a voluntary basis. Increased knowledge of features of hybrid attacks would support CI entities' preparedness and resilience for future similar attacks due to recognizing some patterns in hybrid attacks. On the whole, the innovation would support CI entities also in the implementation of the new CER Directive (Directive for the resilience of critical entities) which repeals the existing framework for the protection of European Critical Infrastructures (2008 ECI Directive) and introduces wider obligations across sectors. In short, Entities in this sector, once identified by the Member States as critical, will be required to conduct risk assessments; take technical and organisational resilience enhancing measures; and notify disruptive incidents without undue delay to the relevant national authorities. Because the hybrid threats and attacks may be created during a wide time span and in many domains so as to cause the wanted harmful effect in the CI domain or entities, information sharing is much requested to ease the recognition of a hybrid attack taking place or possibly under preparations.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054. This article reflects only the authors' views and the Research Executive Agency, and the European Commission are not responsible for any use that may be made of the information it contains.

5.8 Securing critical financial infrastructure

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

FINSEC is a project related to the Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures. The project is a Horizon 2020 with almost 8 million euros of funding. Duration 36 months, ended in April 2021.

The team is composed of 23 partners with security experts, research centers, technology providers, academia and financial organizations that represent the end-users.

The objectives
FINSEC is the first example of integration between Physical + Cyber security fully dedicated to the critical infrastructures in the financial sector. The main results of the FINSEC project are:

- Standard based reference architecture
- Predictive security
- Collaborative security
- Security toolbox and certification services

And why FINSEC?

- Because of its integration between physical and cyber security
- Because of the increased efficiency due to predictive and collaborative security
- Because of the easy-to-deploy integrated strategies and architecture that lead to cost-saving

The Tools
The following tools, provided by technological partners, have been integrated and enhanced in the FINSEC solution:

- Security Information and Event Management (SIEM)
- Risk Assessment Engine (RAE)
- Collaborative Risk Assessment
- ATM Network Security Platform
- Pentesting service and TLS assistant
- Anomaly Detection
- CCTV Analytics

Most of the integrated tools reached TRL 6 or 7 at the end of the project.

The problem to solve
What is the problem that drove the consortium to present the project to the commission? There was an increase of security incidents in the financial sector. Some examples:

- In the 2016 a SWIFT attack against the Bangladesh Bank for about 1 billion US dollars
- In the 2017 the Wanna Cry ransomware created big issues to Russian and Ukrainian banks
- In the 2017 Equifax with a data breach of 140 million consumers
- In the 2019 Metro Bank with an attack through the telephone network
- Still in the 2019 a big data breach with more than 100 million consumers happened at Capital One

This represents a big need for financial institutions to have a structured and integrated security platform for the protection and the reason why we decided to propose this kind of project.

FINSEC, as already reported, is a solution that integrates physical and cyber security. All information coming from the fields are sent to a central FINSEC system that processes them and automatically reacts, predicts threats and attacks, and interacts with the security control center using the FINSEC dashboard.

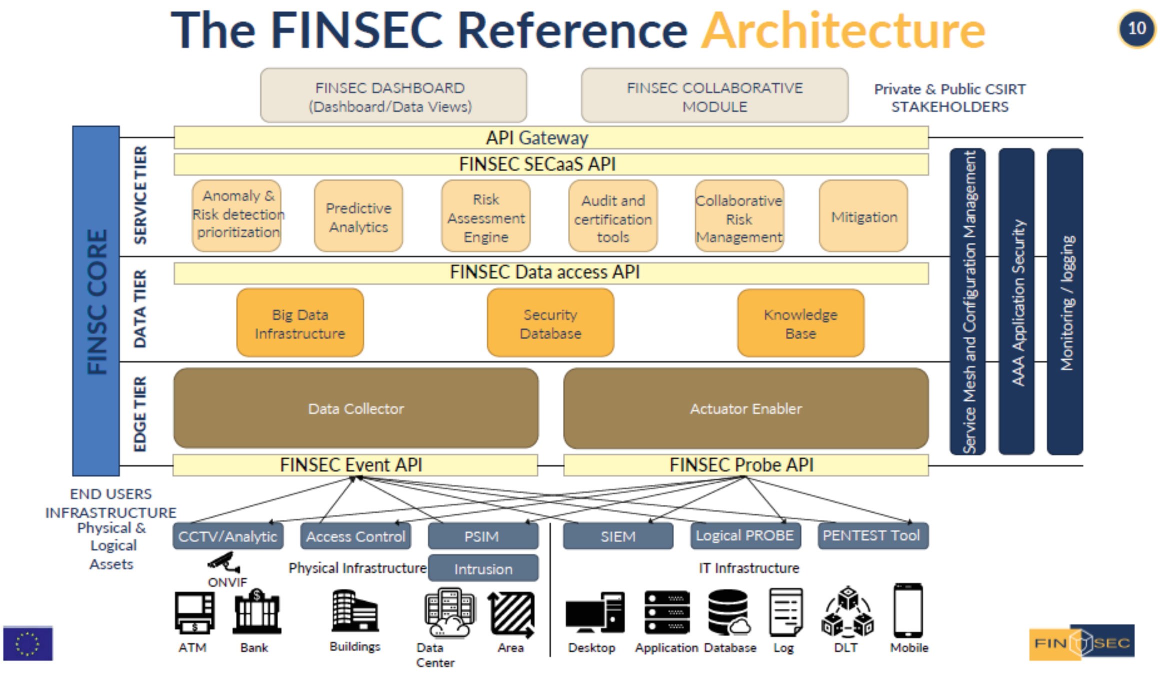


Figure 14 - FINSEC Reference Architecture

One very important pillar of the FINSEC solution is the collaboration, where it is possible to share information on threats and attacks between different organizations, preventing possible issues. The sharing of the information is made through a security network that has been developed on Hyperledger Fabric blockchain technology.

FINSEC platform, being developed as a multi-tenant solution, can be used as Security as a service, available on the cloud but can also be easily deployed on the customer premises.

As we can see from Figure 14, the reference architecture is composed of various layers: from the bottom:

- Field layer with probes sending data to the data layer and receiving messages from the services
- Edge tier layer with the data collector and the actuator enabler
- Data tier layer
- Service tier layer composed of Anomaly and risk detection, Predictive analytics, Risk Assessment Engine, Audit and Certification tools, Collaborative Risk Management, Mitigation
- Platform control layer with dashboard and collaborative module

The Reference Architecture Highlights are the following:

- State-of-the-art intelligent platform based on the edge paradigm, where local metadata and video images are input for “deep learning” algorithms
- Powerful fusion and artificial intelligence engines supporting the decision-making process
- Advanced functions and versatile integration, compatible with new FINSTIX proposed architecture and data-model

The Pilots

The project includes 5 different pilots related to financial institutions, each of one composed of various use cases and implementing the integration between physical and cyber security, anomaly detection and predictive analytics:

- **Pilot 1** - Attacking the SWIFT Network - Use cases have been developed for monitoring SWIFT messages outside the online period, failed login attempts, non-admin user login attempt outside working hours, enforcing four-eye principle for HSM administration, Integration of PIN Pad, Audit and Certification
- **Pilot 2** - Correlating Physical and Cyber Attacks in Buildings – Use cases have been implemented for data center protection and ATM protection. About Data Centers: Access Control, Server Rack opening procedure checked through CCTV, Server's login attack detection. About ATM: Physical attack on the customer, Physical attack on the ATM, Loitering, Cyberattack - such as malware - on the ATM PC or the network, Jackpotting.
- **Pilot 3** - Predictive Protection of Peer-to-Peer Payments Infrastructure – Use cases have been developed for predicting attacks on the payment solution like transactions made from different locations and transactions made with suspicious amounts. Then predicting attacks on the blockchain through transactions and sender addresses monitoring. Also, use cases have been set up for collaborative security and audit and certification.
- **Pilot 4** - Protecting the infrastructures of small financial institutes through Security-as-a-Service – Use cases have been implemented for detecting bank workstations attacks, attacks to bank through VPN, internet banking attacks during login, illegal access to user bank account and illegal transfers, dynamic risks assessment on PCI-DSS
- **Pilot 5** - Insurance & Risk Management in Public Infrastructures – Use cases have been developed for improving security during mobile app login through face recognition and monitoring insurance mobile app usage through anomaly detection and predictive analytics

5.9 Intelligent Management of Processes, Ethics and Technology for Urban Safety

IMPETUS (www.impetus-project.eu): Intelligent Management of Processes, Ethics and Technology for Urban Safety by Joe Gorman, SINTEF Digital

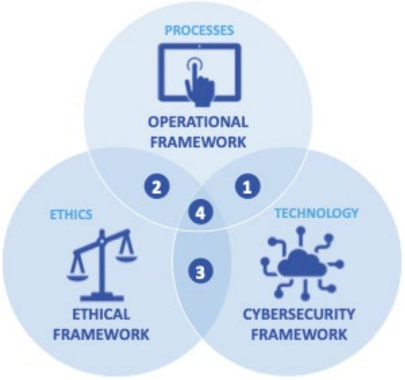
The main goal of IMPETUS is to provide city authorities with new means to address security issues in public spaces, and so help protect citizens. Using data gathered from multiple sources, it will facilitate detection of threats and help human operators dealing with threats to make better-informed decisions. By innovating existing tools, integrating them into a single platform, as well as testing them during live exercises in pilot cities IMPETUS aims to answer the following questions:

- Can advanced technologies improve the detection and management of security events?
- How will this affect processes used in day-to-day operations?
- How can ethical and legal issues be safeguarded and handled?
- Do they create new cyber security risks and reliance on infrastructure?

IMPETUS provides different types of results, as follows:

- Public safety tools providing specific capabilities around: Detection, Simulation & analysis, Intervention
- Platform: Integrates tools; common interface/dashboard
- Practitioners Guides to support deployment: Managing operational change, Accounting for ethical and legal concerns, Managing cybersecurity

The basic architecture of the IMPETUS solution is shown and briefly explained in Figure 15.



1. AI-based threat detection, analysis and intervention
2. Privacy-preserving technical and legal guidelines
3. Ethical & explainable AI including security awareness
4. Decision-making support tools combining AI + human-in-the-loop

Figure 15 - IMPETUS basic Architecture

One of the key results is the Integrating Platform, which acts as central information hub supporting security and emergency operations. It supports the integration, analysis and visualisation of data from multiple technologies and sources, including smart city systems and data, and tools developed in IMPETUS. The IMPETUS tools are presented in Table 1 through different phases of the security cycle.

Table 1 - Brief description of tools developed in IMPETUS

BE PREPARED	
Breach and Attack Simulation	A tool that automatically uncovers the attack paths in a safe and secure manner (i.e., no interruption of services).
DETECTION	
Social Media Detection	Tool that collects and analyses massive amounts of online public data to help Law Enforcement and Investigative Professionals detect specific written content, to prevent terror, crime and threats affecting cities.
Weapon Detection	An AI (Artificial Intelligence)-based tool that detects small magazine fed handguns and assault rifles using security cameras in indoor or outdoor environments.
Biological Risk Detection	A device that collects and analyses the level of microbiological contamination in the air. The purpose of this device is to monitor the microbiological status of the air quality and to create an alert if there are indications of deliberate pathogen dispersion.

SITUATIONAL AWARENESS	
Cyber Threat Intelligence	The tool provides unique and advance warnings about new cyberthreats. It is contextual and fully automated (machine-to-machine). IOCs are delivered in real-time and are actionable.
Physical Threat Intelligence	Anomaly detection from multivariate sensor data. The system will generate an alert when data observed by the sensors show an anomalous /unexpected trend. The user will be able to understand the reasons for the alert and see which measurements in which locations showed an anomalous /unexpected trend.
RESPONSE OPTIMISATION	
Human-Computer Interaction	The tool sends real-time Assessment and Alert Data on the operator/team workload state. It is dependent on the operator's neuro-physiological signals. The data are anonymized and the assessment model will be deployed on a secured USB drive to the individual person.
Physical Threat Response Optimization	The tool for Oslo pilot city will create simulations of crowds of humans to identify possible hazards or reasons for different challenges such as congestion points. The tool for Padova pilot city will propose possible ways to manage critical or dangerous situations in public spaces.
LEARNING	
Cyber Threat Mapping	The Prelude-ELK tool provides collection and post-processing of events created by other cyber security components (e.g., antivirus reports, network firewall logs and intrusion detection system alerts).

The project will also produce a set of Practitioners Guides:

- Ethics and Data Privacy in security operations - a set of guidelines and practices while storing and processing sensitive data and implementing and or using smart tools in the context of smart cities.
- Security Operations in smart cities - guidelines which provide practical recommendations for real-time monitoring of all kinds of data, detection of security events, and continuous threat intelligence updates of the infrastructure.

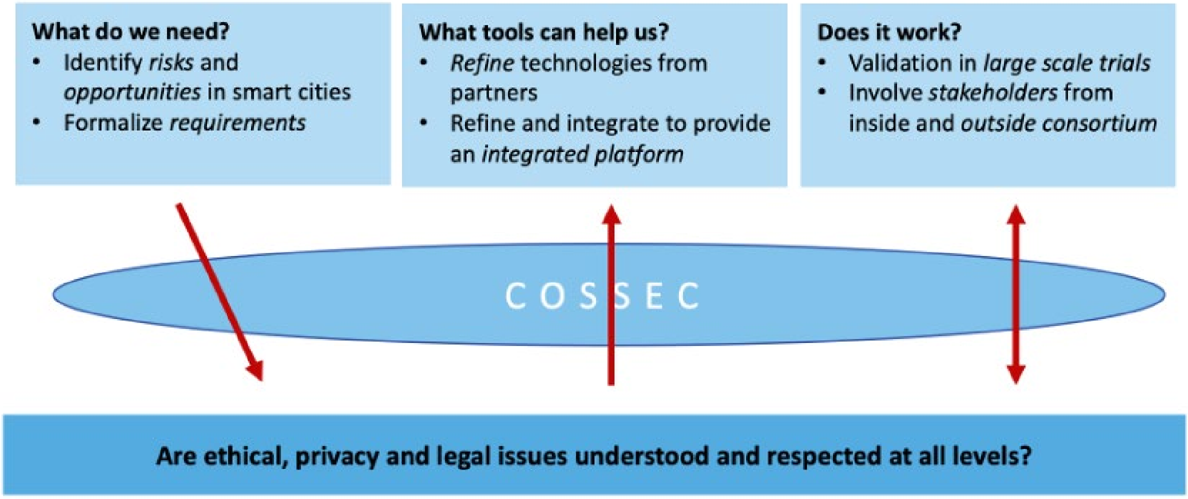
- Cybersecurity in smart cities - The cyber-security practitioners' guidelines provide practical recommendations for implementing and maintaining new smart technology solutions.

Finally, IMPETUS will make all lessons learned throughout the project available to stakeholders who are looking for the type of support offered by IMPETUS so that they can benefit from what we learned when devising their own plans and making decisions about the adoption of tools and methods.

Besides the development of a solution, IMPETUS pays a lot of attention to external collaboration. The central networking group for IMPETUS is COSSEC, which stands for "Community of Safe and Secure Cities". It is a group of individuals representing organisations or projects that have an interest in or might be affected by the work being done by the IMPETUS project. The idea of COSSEC is to extend involvement in the project to stakeholders beyond the project consortium. COSSEC members will influence IMPETUS activities so that solutions emerging from the project will meet local needs in other cities and/or meet other concerns or requirements they might have. Some COSSEC members will be early adopters of project results. COSSEC members will be consulted to collect information related to local contexts of cities, test the project tools and methodologies, involvement of experts from various public authorities, and exchanges experience and best practices. The objectives of the interplay between COSSEC and the IMPETUS Consortium are the following:

- To influence project direction, ensure results fit needs;
- To move policies in the right direction;
- To provide external feedback that helps development;
- To channel for long-term smart city R&D promotion.

Figure 16 shows how IMPETUS will achieve its vision with COSSEC.



What do we need?
- Identify *risks* and *opportunities* in smart cities
- Formalize *requirements*

What tools can help us?
- *Refine* technologies from partners
- Refine and integrate to provide an *integrated platform*

Does it work?
- Validation in *large scale trials*
- Involve *stakeholders* from inside and *outside consortium*

Are ethical, privacy and legal issues understood and respected at all levels?

Figure 16 - The role of COSSEC in IMPETUS project

The IMPETUS solution is validated in three phases in pilot cities Oslo and Padova:

- **Phase 1**: Technical and acceptance testing on non-live systems
- **Phase 2**: Data collection from live systems, for analysis but no intervention
- **Phase 3**: Live test with simulated physical and cyber attack

The first two phases are done, and we are in the process of the preparation of live exercises which will take place in the forthcoming months.

The IMPETUS consortium believes that the Integrating Platform, tools, guidelines and lessons learned will attract the attention of other smart cities and stakeholders and will be implemented in future. To this end a long-term plan is to:

- promote uptake of results in smart cities throughout Europe and elsewhere,
- influence policy-making to facilitate uptake consistent with ethical and legal principles,
- establish COSSEC as a permanent community of users.

5.10 Improving resilience of sensitive industrial plants and infrastructures

InfraStress (www.infrastress.eu): Improving resilience of sensitive industrial plants & infrastructures - Gabriele Giunta, Engineering.

Security threats, whether physical or cyber-related, are an increasing concern for sensitive industrial plants and infrastructure. Current solutions are fragmented and cannot address tailored and integrated activities from both kinds of threats. In the last decades, high levels of industrial safety have been achieved due to industry and legislative actions (the current EU Directive 2012/18/EU aka 'Seveso III'). However, since security breaches in SIPS may result in safety incidents (the so-called "security-induced safety cases" phenomenon), there is a need to advance traditional approaches to enable an accurate analysis of the interdependencies between security vulnerabilities – both in the cyber and in the physical world – and safety properties of the infrastructure being protected. Up to now cyber and physical security have often been addressed as separate/unrelated areas but especially the move into the 'digital everywhere' era must consider them in a holistic manner.

InfraStress addresses cyber-physical (C/P) security of Sensitive Industrial Plants and Sites (SIPS) Critical Infrastructures (CI) and improves the 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 a reasonable cost.

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*: InfraStress has provided adaptive, flexible, and customizable set of innovative and configurable security measures and tools.
- *Guarantee continuity of operations, while minimizing cascading effects in the infrastructure itself, the environment, other Critical Infrastructures, and the citizens in the vicinity, at a reasonable cost*: InfraStress has enabled effective collaboration among SIPS operators.
- *InfraStress deals with the security of both sensitive industrial production plants and sensitive storage sites, along with ICT infrastructures supporting them*: InfraStress has delivered an open Framework that allows future evolution to easily integrate (1) detection technologies, (2) data feeds, (3) analysis and decision support services, and (4) existing solutions already deployed at the SIPS CI side.
- *InfraStress supports a culture of EU SIPS Critical Infrastructure Protection*: InfraStress has enabled full exploitation of the technological innovation potential by implementing a human-centric approach that effectively combines decision support and human expertise.

InfraStress started with TRL4+ results from relevant past and current projects or products in current partners' portfolios, towards TRL7 level and developing its own new approach, by evolving and integrating them, in particular adapting them to SIPS needs. The **InfraStress methodology** is based on a set of composite indicators of SIPS security and resilience, which will be embedded into the new risk and resilience ISO and CEN standards, and into education and training programs. The methodology and indicators seek to yield innovation and the benefits/savings to be achieved by the project were assessed by users (i.e., Pilots) and advisory groups. Addressing the current fragmentation of available

security solutions and technology, InfraStress has provided an **integrated framework** including cyber and physical threat detection, integrated C/P Situational Awareness, Threat Intelligence, and an innovative methodology for resilience assessment – all tailored to each site. InfraStress has adopted a user-driven approach carried out through a) delivery of usable and user-friendly Services and Applications for C/P protection and resilience; b) technical activities driven by and receiving active input from end users, i.e., SIPS and relevant stakeholders; c) a comprehensive set of 5 real-world Pilots and Evaluation activities carried out by User partners.
InfraStress has involved 27 partners of excellence from 11 countries with very cross-cutting and complementary competences and excellent track records, including 5 SIPS operators.

The InfraStress results successfully capture the diversity and complementarity of the requirements which must be satisfied by a platform enabling true convergence of cyber and physical security. They collectively cover a variety of high-impact threat scenarios to SIPS CIs, ranging from natural disasters to direct cyber-physical attacks to critical assets. They provide concrete examples of the threats and attacks for which InfraStress delivers efficient support. From the architectural point of view, the InfraStress modules are illustrated in Figure 17.

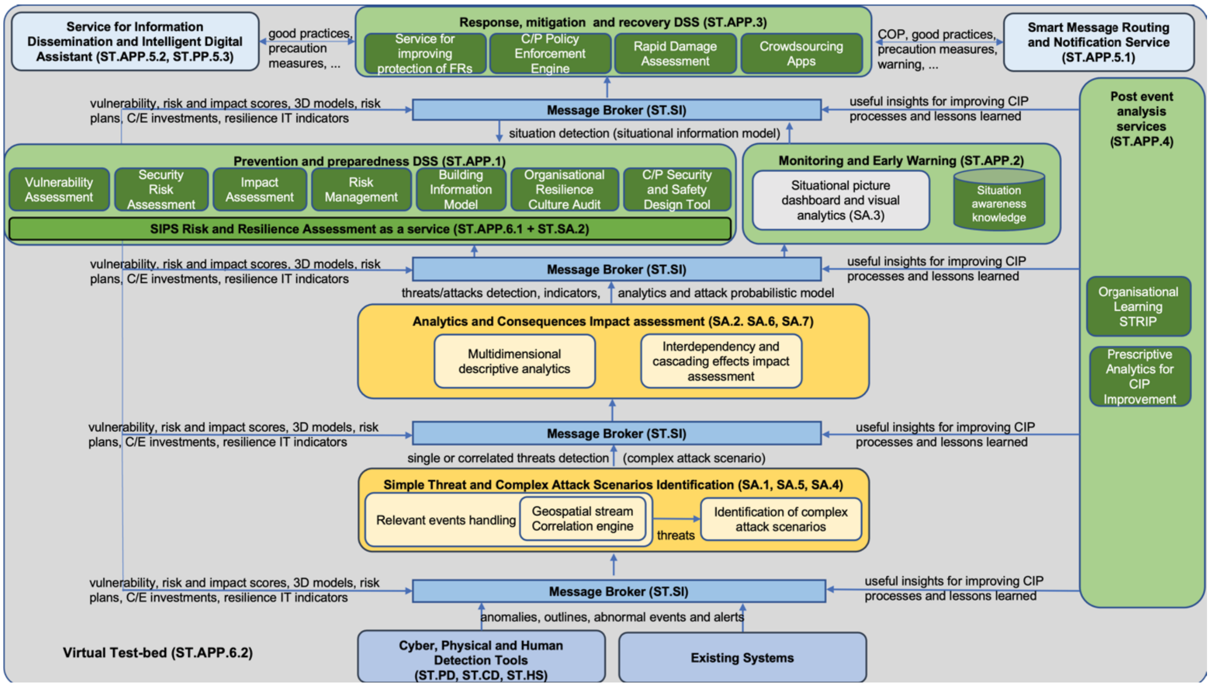

Service for Information Dissemination and Intelligent Digital Assistant (ST.APP.5.2, ST.PP.5.3)
good practices, precaution measures, ...
Response, mitigation and recovery DSS (ST.APP.3)
Service for improving protection of FRs
C/P Policy Enforcement Engine
Rapid Damage Assessment
Crowdsourcing Apps
COP, good practices, precaution measures, warning, ...
Smart Message Routing and Notification Service (ST.APP.5.1)
vulnerability, risk and impact scores, 3D models, risk plans, C/E investments, resilience IT indicators
Message Broker (ST.SI)
useful insights for improving CIP processes and lessons learned
situation detection (situational information model)
Post event analysis services (ST.APP.4)
Prevention and preparedness DSS (ST.APP.1)
Vulnerability Assessment
Security Risk Assessment
Impact Assessment
Risk Management
Building Information Model
Organisational Resilience Culture Audit
C/P Security and Safety Design Tool
SIPS Risk and Resilience Assessment as a service (ST.APP.6.1 + ST.SA.2)
Monitoring and Early Warning (ST.APP.2)
Situational picture dashboard and visual analytics (SA.3)
Situation awareness knowledge
vulnerability, risk and impact scores, 3D models, risk plans, C/E investments, resilience IT indicators
Message Broker (ST.SI)
useful insights for improving CIP processes and lessons learned
threats/attacks detection, indicators,
analytics and attack probabilistic model
Organisational Learning STRIP
Prescriptive Analytics for CIP Improvement
Analytics and Consequences Impact assessment (SA.2. SA.6, SA.7)
Multidimensional descriptive analytics
Interdependency and cascading effects impact assessment
vulnerability, risk and impact scores, 3D models, risk plans, C/E investments, resilience IT indicators
Message Broker (ST.SI)
useful insights for improving CIP processes and lessons learned
single or correlated threats detection
(complex attack scenario)
Simple Threat and Complex Attack Scenarios Identification (SA.1, SA.5, SA.4)
Relevant events handling
Geospatial stream Correlation engine
threats
Identification of complex attack scenarios
vulnerability, risk and impact scores, 3D models, risk plans, C/E investments, resilience IT indicators
Message Broker (ST.SI)
useful insights for improving CIP processes and lessons learned
anomalies, outlines, abnormal events and alerts
Virtual Test-bed (ST.APP.6.2)
Cyber, Physical and Human Detection Tools (ST.PD, ST.CD, ST.HS)
Existing Systems

Figure 17 - InfraStress Integrated Framework: main modules

InfraStress followed the holistic Innovation Management methodology [Sofou 2017] which includes a combined strategy for IP management, Data management, Dissemination and Exploitation of Project Results throughout the lifecycle. More specifically, it foresees specific actions as well as the order of their implementation, in order to manage the innovations generated during the project and to ensure the appropriate access to, protection and usage of IP rights before and after the project.

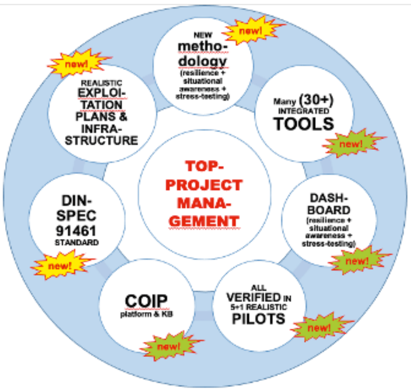
The possible products and services that were designed to embody InfraStress Results were selected based on i) a holistic view of the market and an understanding of the current market segmentation in relation to what InfraStress has developed, in terms of product and services, and ii) an effort to capture the trends of the market over the coming years, challenging -to the extent possible- the current view of the market.
Suggested InfraSreess solutions with short descriptions and contact details can be found in the project website https://www.infrastress.eu/infrastresssolutions.

The InfraStress main achievements:

- All components successfully integrated
    - 40+ components developed by the project +
    - 25+ selected COTS technologies
    - The InfraStress solutions have been tested and demonstrated in 5 pilot sites, with a participative approach involving the owners, operators and stakeholders. Validation done in five substantial pilots:
        - Refinery: Motor Oil – Petrolchemicals (Greece).
        - Medical manufacturing Ireland (orthopaedics): DePuy Synthes (franchise of Johnson & Johnson).
        - Chemical storage site: Carmagnani (Italy).
        - Municipality including chemical plant, with involvement of public authority/civil society: Fisipe + Barreiro (PT)
        - Port including a storage site: Petrol chemical storage + Luka Koper (Slovenia)

InfraStress has matched key impacts not only in response to the Work Programme Call but also at Strategic, Socio-economic and Market levels. In fact, InfraStress was conceived since the beginning with a strong business vision in mind and will carry out effective exploitation actions ensuring a successful go-to-market. Tailored activities are also planned to rise a culture of participatory security to involve all stakeholders including companies, workers, public authorities, citizens and civil society. The main impacts beyond the project:

- NEW methodology (resilience + situational awareness + stress-testing)
- INTEGRATED tools
- DASHBOARD
- ALL VERIFIED IN 5+1 REALISTIC PILOTS
- COIP platform
- DIN SPEC 91461 STANDARD
- REALISTIC EXPLOITATION PLANS & INFRASTRUCTURE


NEW methodology (resilience + situational awareness + stress-testing)
new!
Many (30+) INTEGRATED TOOLS
new!
DASH-BOARD (resilience + situational awareness + stress-testing)
new!
ALL VERIFIED IN 5+1 REALISTIC PILOTS
new!
COIP platform & KB
new!
DIN-SPEC 91461 STANDARD
new!
REALISTIC EXPLOI-TATION PLANS & INFRA-STRUCTURE
new!
TOP-PROJECT MANA-GEMENT

Specifically, the **InfraStress dissemination** was **bidirectional**, meaning that the results of the project were not only “sent to others”, but also because the feedback of the addressees was actively searched for and implemented into the R&D work; and **dynamic** (COIP). The **COIP system** was developed as a live system constantly allowing the users from “both sides” (project internal and external) to see the current state and results of the interaction/dialogue. Apart from the usual “list of exploitable deliverables”, the project has proposed to have the whole system usable for “***Assessment-as-a-Service***””- i.e., the people can access the system, register and use it for Assessment done by themselves and verified by the external experts together or alone. This was implemented through the **ERRA-concept** and infrastructure resulting from the project (ERRA – European Risk & Resilience Assessment for “Assessment-as-a-Service” – with approx. 50 members registered). Many projects use to produce the standardization drafts, usually the limited duration (3 years) documents such as EN-CWAs and usually not brought to the published stage during the project. InfraStress has produced and brought to the final (published) stage one national standardization document, the **DIN SPEC 91461** “*Stress testing resilience of SIPS and other critical infrastructures*”. The document was produced with the participation of all project partners and with the participation of the Italian and French NSBs (UNI and AFNOR). The basic concept of InfraStress was anchored in ISO 31050 “Enhancing management of emerging risks for enhanced resilience”; the ISO standard is now at the CD (Committee Draft) stage and has been developed by the Joint Working group of TWO ISO committees: The “risk” one (TC262) and the “resilience” one (TC 292). The new EU P4P – “Projects-to-policies” is a mechanism ensuring that the EU project results are embedded into current and the new EU policies – e.g., the Directives. The results and experiences from InfraStress have been continuously considered in the discussions about **NIS2** and **CER Directives** (cyber & critical infrastructures directives, respectively) and this was done through forwarding the reports to the Directive developers, discussion on the dedicated events (e.g., CERIS) and informal contacts and discussions related to single issues: e.g., the issue of standardization in CER-Directive – treated differently than in the NIS2 Directive.

5.11 Improving the cyber security of the European electrical power energy systems

PHOENIX (phoenix-h2020.eu): Improving the cyber security of the European electrical power energy systems by Ganesh Sauba, DNV.

The PHOENIX project focuses on the protection of the European end-to-end Electrical Power and Energy Systems (EPES), from energy production to prosumption via prevention, early detection and fast mitigation of cyber-attacks against EPES assets and networks (such as primary and secondary substations, transformers, SCADA, PLC, maintenance tools) and from (intentional and unintentional, internal and external) human activities, while protecting the utilities and end-users' privacy from data breaches by design.

PHOENIX consists of a prestigious consortium of 24 partners) covering all required expertise including energy (RES) generation/VPP, TSO, DSOs, aggregators, retailers, prosumers, end-users, technology providers, SMEs. Some partners have multiple roles in the project.

There are three strategic goals for PHOENIX, they are:

1. Strengthen EPES cybersecurity preparedness by employing security by design and innovation and validating them in five real-live large-scale pilots.
2. Coordinate European EPES cyber incident discovery, response and recovery, contributing to the implementation of the NIS Directive by developing and validating at national Member States and pan-European level.
3. Accelerate research and innovation in EPES cybersecurity by a novel deploy, monitor, detect and mitigate DevSecOps (Development of Secured Operations) mechanism, a secure gateway, privacy preserving federated Machine Learning algorithms and establishment of certification methodologies and procedures through a Netherlands-based Cybersecurity Certification Centre.

PHOENIX will achieve these strategic objectives by encapsulating the key challenges of incidents forecast, risk identification and analysis, mitigation and recovery in 3 project pillars as shown in Figure 18.

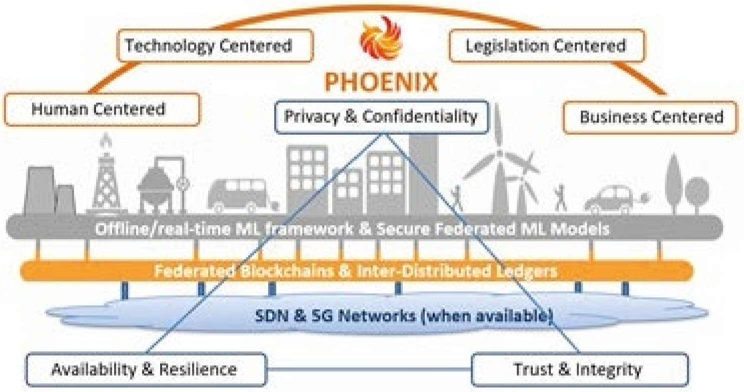

Technology Centered
Legislation Centered
PHOENIX
Human Centered
Privacy & Confidentiality
Business Centered
Offline/real-time ML framework & Secure Federated ML Models
Federated Blockchains & Inter-Distributed Ledgers
SDN & 5G Networks (when available)
Availability & Resilience
Trust & Integrity

Figure 18 - PHOENIX Key Challenges, Pillars and Technologies

1. **Technology centred security & privacy**: cyber-human security threats & attacks on data privacy may be so complex and inter-dependable that PHOENIX would need to be treated as an adaptive, self-learning ecosystem, where security & privacy by design will be combined with technology innovations to protect new and existing EPES sites and data from known and yet unknown/zero-day threats. Diverse technologies such as (heterogeneous) blockchains and distributed inter-ledger persistent communications should be combined with Big Data analytics and secure cloud technologies, to securely store critical and sensitive information such as logs and firmware upgrade schedules or customer consumption records; SDN and 5G communications (as they become wide available) will ensure security, while Artificial Intelligence would play a crucial role in malware identification and situation awareness.

2. Human centred security & privacy: technological centred solution is not efficient, without considering the full range of humans involved i.e., employees, LEA, CERT and citizens. PHOENIX has adopted the Human-In-the-Loop (HITL) concept to create a Community of Security & Privacy, where trusted information can be exchanged between involved humans, while ensuring GDPR compliance and privacy protection from data breaches. PHOENIX is also contributing to the implementation of the NIS Directive and collaboration between ENISA supported CERTs and utilities CSIRT by actively supporting the pan-European Incidents' Information Sharing Platform (I2SP) and the CEI Security Stakeholders Group (CEIS-SG).

3. *Business centred security & privacy:* Security has cost implications. Each EPES plant, site or segment needs specialized attack prevention and incident mitigation actions to operate securely and to return to normal operation following an attack. PHOENIX extends the Security as a Service business model, to Security & Privacy as a Service (SPaaS) considering the cost of offered services (such as authentication, anti-virus, anti-malware, intrusion detection, penetration testing, privacy protection), the incident probability, the cascading severity and restoration requirements, normalized by the total cost of ownership, to introduce novel service delivery models for EPES infrastructure security management and data (both infrastructure or human related) privacy protection.

The PHOENIX architecture is made up of three layers as show in Figure 19.

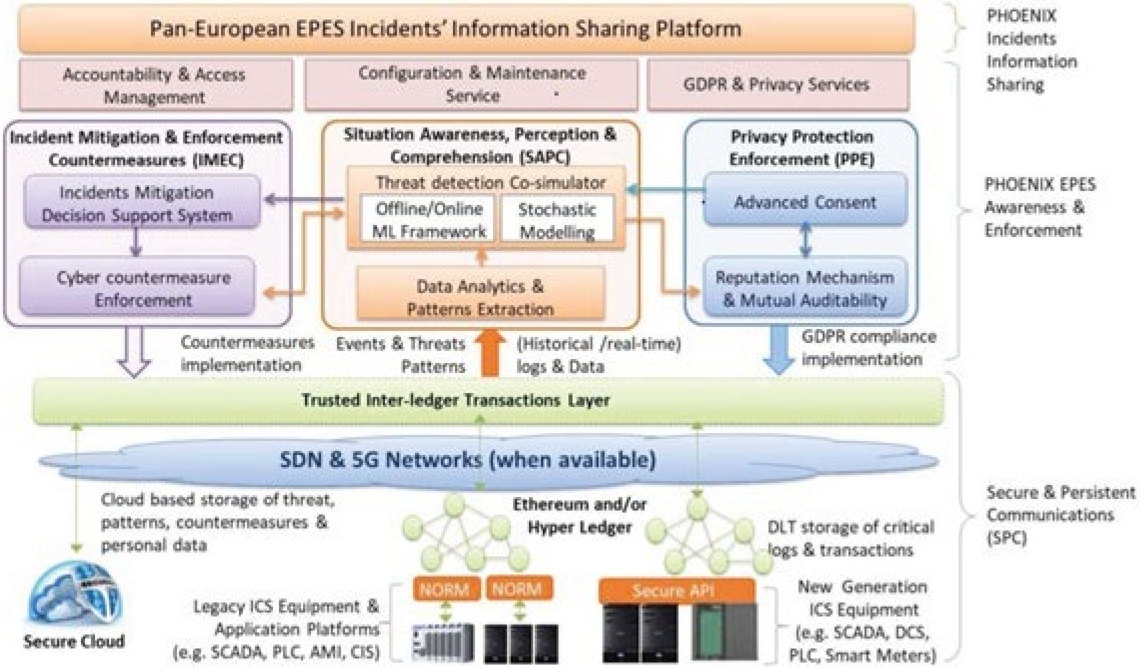

Pan-European EPES Incidents' Information Sharing Platform
Accountability & Access Management
Configuration & Maintenance Service
GDPR & Privacy Services
PHOENIX Incidents Information Sharing
Incident Mitigation & Enforcement Countermeasures (IMEC)
Incidents Mitigation Decision Support System
Cyber countermeasure Enforcement
Situation Awareness, Perception & Comprehension (SAPC)
Threat detection Co-simulator
Offline/Online ML Framework
Stochastic Modelling
Data Analytics & Patterns Extraction
Privacy Protection Enforcement (PPE)
Advanced Consent
Reputation Mechanism & Mutual Auditability
PHOENIX EPES Awareness & Enforcement
Countermeasures implementation
Events & Threats Patterns
(Historical /real-time) logs & Data
GDPR compliance implementation
Trusted Inter-ledger Transactions Layer
SDN & 5G Networks (when available)
Cloud based storage of threat, patterns, countermeasures & personal data
Ethereum and/or Hyper Ledger
DLT storage of critical logs & transactions
Secure & Persistent Communications (SPC)
Secure Cloud
Legacy ICS Equipment & Application Platforms (e.g. SCADA, PLC, AMI, CIS)
NORM
NORM
Secure API
New Generation ICS Equipment (e.g. SCADA, DCS, PLC, Smart Meters)

Figure 19 - PHOENIX Platform Architecture

Layer 1 is the Secure and Persistent Communications Layer (SPC), which is responsible for information gathering, including EPES ICT systems and SCADA, (cyber) sensors, networked devices, events and alarms. Though engineering solutions, such as encrypted VPNs offering sufficient security, many legacy EPES assets are not designed to support them. As a workable solution, PHOENIX will develop a Universal Secure Gateway (USG), as a secured network edge device, directly connected with existing/legacy EPES assets (i.e., RTUs, PLC, SCADA). It is also responsible for the secure, transparent and distributed exchange and storing of data objects, ensuring their integrity, availability and confidentiality via (i) an innovative inter-ledger transactions layer, which enables trusted information exchange between secure cloud technology and various ledger fabric and (ii) 5G networking features when and where available.

Layer 2 is the PHOENIX EPES Awareness & Enforcement core modules, responsible for multi-criteria Situation Awareness, Perception & Comprehension (SAPC) of the information and data, Incidents Mitigation & enforcement of Countermeasures (IMEC) along with Privacy Protection Enforcement (PPE). The SAPC which proactively detects any threats that might be carried out with criminal intent, human error or data breach. Initially, a Data Analytics and patterns extraction module will enable continuous monitoring of the IT infrastructure for suspicious activities. The IMEC Module will implement Business analytics and offer incidents mitigation and countermeasures considering specific security and privacy SLAs (as smart contracts), priorities in order to minimize downtime and cascading effects, along with the associated cost. Countermeasure strategies already identified include enhanced resilience, incident localization & network restoration and information provision to the EPES personnel and citizens. PPE implements an advanced legal framework for suitably managing data, ensuring adequate levels of GDPR compliance, well beyond legacy Data Management

Platforms. It features a Reputation mechanism & Mutual Auditability component to offer role-based access for transaction verification and validation in a Proof-of-Stake manner, using distributed consensus algorithms, considering zero knowledge validations of associated data transactions via providing novel blockchain-based verification loops.

Finally, **Layer 3** combines individual EPES stakeholders and CERTS under a Pan-European EPS cybersecurity Incidents' Information Exchange Centre (I2SP) partially implemented under the H2020 SUCCESS project and further developed within PHOENIX with more up-to-date systems. It is a fully distributed information-sharing system, operating as a crowdsourced cyber threat analysis platform, thus facilitating communication between utilities' CSIRTs and CERTs.

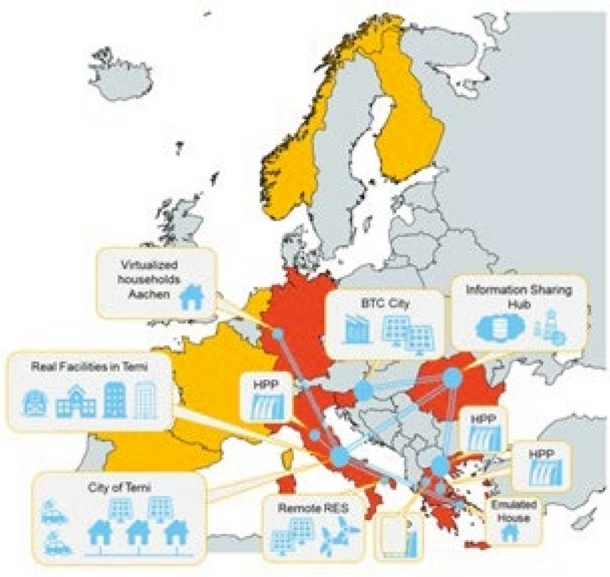


Figure 20 - PHOENIX Large Scale Pilot Locations

The PHOENIX project is underpinned by five large-scale pilots (LSPs) as shown in Figure 20 and are as follows:

- **LSP1:** deals with Multi-utility/Multi-owner RES cyberthreats and data breach detection based in Italy.
- **LSP2**: offers National-wide cooperative remotely controlled HPP security located in Greece.
- **LSP3:** presents Collaborative Microgrid-enabled cyber risks mitigation based in Slovenia.
- **LSP4**: tackles Collaborative / DSO flexibility vs cybersecurity and privacy distributed in Italy, Germany, and Greece.
- **LSP5**: Considers the National vs Pan-European cooperative cyber threat information sharing and is located in Romania.

All 5 LSPs are being subjected to penetration testing work to show their resilience to cyber-attacks. In addition, the project is also contributing to Certification and Standardisation activities.

For more up-to-date information, please visit our website: https://phoenix-h2020.eu.

5.12 Protection of Critical Infrastructures from advanced combined cyber and physical threats

PRAETORIAN (praetorian-h2020.eu): Protection of Critical Infrastructures from advanced combined cyber and physical threats by Eva María Muñoz Navarro, ETRA I+D

PRAETORIAN is an Innovation Action funded under the SU-INFRA01-2018-2019-2020 topic in 2020, and officially started in June 2021. PRAETORIAN's strategic goal is to increase the security and resilience of European Critical Infrastructures (CIs), particularly facilitating the **coordinated protection of interrelated CIs against combined physical and cyber threats**. To that end, the project provides a multidimensional (economical, technological, policy, societal) yet infrastructure-specific toolset comprising: (i) a Physical Situation Awareness system, PSA (ii) a Cyber Situation Awareness system, CSA (iii) a Hybrid Situation Awareness system, HSA, all of which use digital twins of the infrastructure under protection, as well as (iv) a Coordinated Response system. The PRAETORIAN toolset supports the security managers of CIs in their decision enabling them to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

The project specifically aims to tackle (i.e., prevent, detect, respond and, in case of a declared attack, mitigate) human-made cyber and physical attacks or natural disasters affecting CIs. It also addresses how an attack or incident in a specific CI can jeopardise the normal operation of other neighbouring/interrelated CIs, and how to make all of them more resilient, by predicting cascading effects and proposing a unified response among CI operators and assisting First Responder (FR) teams.

PRAETORIAN strategic goal can be mapped into six objectives which are grouped into technological objectives and impact and user-oriented objectives. The technological objectives are the following:

- O1-Evaluate the hazards and minimize their level of risk by assessing the vulnerabilities of targeted sectors and designing adequate security measures
- O2-Improve the understanding of any physical or cyber threats and their consequences in the interdependent network of critical infrastructures
- O3-Improve and enhance the resilience of the CIs and neighbouring population and enable coordinated response to an attack with effective decision support making
- O4-Share with the public pertinent information on the risks associated with an event and the emergency response actions planned to overcome the incident

On the other hand, the user-oriented objectives are listed as follows:

- O5-Validate the project results in real contexts of interdependent CIs to improve its efficiency, cost-effectiveness, and societal benefit
- O6-Ensure compliance of the solutions with the legal, ethical, privacy, and societal principles, including recommendations to policy planners, as well as disseminate results on the researched threat information sharing models to the relevant communities of users, to promote the adoption of the proposed cost-effective solutions beyond the project participants.

These solutions will be packaged in the form of 4 products (P), as shown in Figure 21.

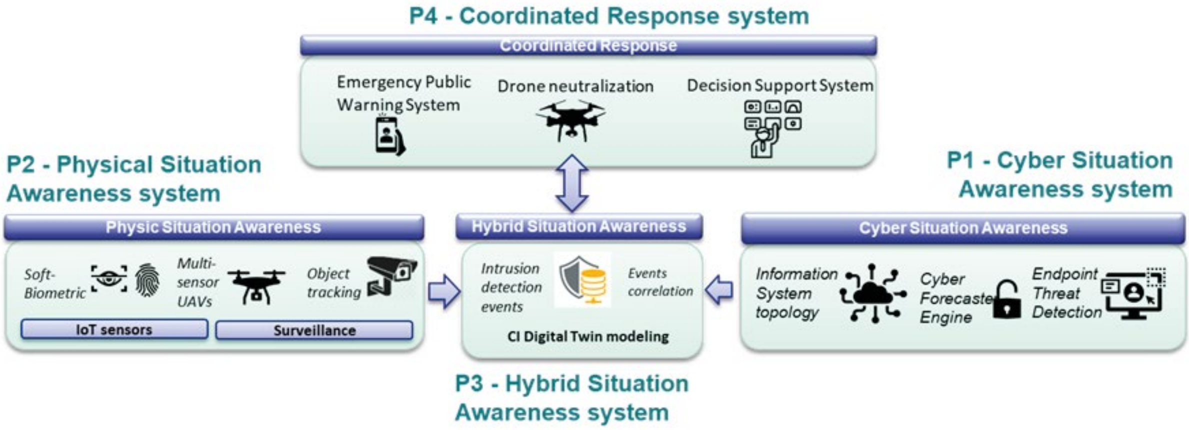

P4 - Coordinated Response system
Coordinated Response
Emergency Public Warning System
Drone neutralization
Decision Support System
P2 - Physical Situation Awareness system
Physic Situation Awareness
Soft-Biometric
Multi-sensor UAVs
Object tracking
IoT sensors
Surveillance
Hybrid Situation Awareness
Intrusion detection events
Events correlation
CI Digital Twin modeling
P3 - Hybrid Situation Awareness system
P1 - Cyber Situation Awareness system
Cyber Situation Awareness
Information System topology
Cyber Forecaster Engine
Endpoint Threat Detection

Figure 21 - PRAETORIAN solution

The threats detected by a wide set of sensors both in the cyber (P1) and physical (P2) domains will generate corresponding alarms, which will be correlated in the hybrid system (P3), which include digital twins of the infrastructure under protection, to estimate possible cascading effects. This information will then be processed in P4 to provide assistance to the CI operators to better respond to the threats and allow them to liaise with the affected CIs and the FRs.

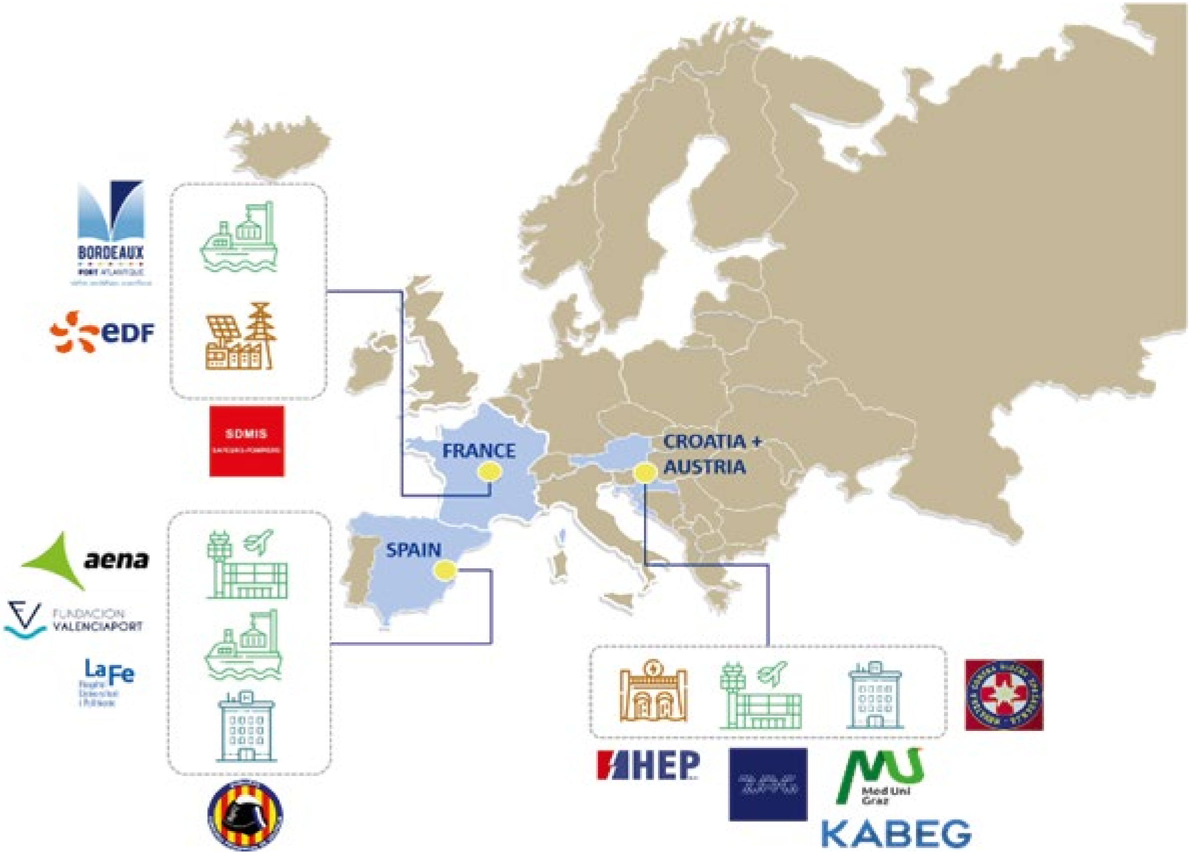


Figure 22 - PRAETORIAN pilot sites

PRAETORIAN project is a CI-led, user-driven project that will test and demonstrate its results in three complementary and cross-site demonstrators organized by three international pilots (Figure 22), one of them involving cross-border use cases: the Port of Bordeaux and a simulator of power plant critical system are the CIs in the French scenario; the Port of Valencia, focusing on the cruise terminal, the airport of Valencia and a hospital are part of the Spanish scenario; finally, the CIs involved in the Croatian scenario are a pump hydro power plant and the airport of Zagreb, as well as two hospitals in Austria, one of them with a biosafety level 3 (BSL-3) laboratory, thus creating the cross-border use case. The pilot sites will interact with each other, providing feedback and lessons learnt from one demo-site into the others.

PRAETORIAN is currently reaching its first year of life. The technical developments are nearing completion and the main activity now is the integration of all modules and systems into a unified and interoperable PRAETORIAN platform. In September 2022, the preparation of the activities in the demonstrators will begin, in which the platform will be deployed in real scenarios for its evaluation, with a clear focus on meeting the needs of the end users of the project.

5.13 Cascading cyber-physical threats and effects

PRECINCT (www.precinct.info): Cascading cyber-physical threats and effects by Antonis Mygiakis & Aristea Zafeiropoulou, Konnecta Systems

Critical Infrastructures (CIs) are increasingly at risk from a variety of intentional cyber-physical attacks (malware, terrorist-driven exploits, etc.), as well as risks from natural hazards and hybrid threats including fake news. Recent research and emerging solutions focus on the protection of individual critical infrastructures such as ports, energy distribution, hospitals, etc. However, managing the impact of cascading effects arising from the interdependencies between different types of critical infrastructures (e.g., related to energy, water, transport, and communications) and their resilience towards enabling 'rapid recovery' is becoming more and more pertinent and is highly challenging, especially in the context of delimited geographical areas The pervasive connectivity in smart cities also implies a threat canvas with growing exposure to new threats that can affect a city's or region's economy, operational data, infrastructures, connected devices, as well as citizen safety.

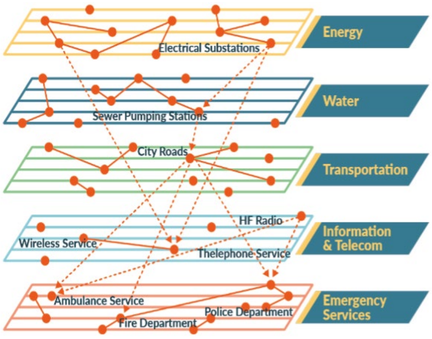


Figure 23 - Interdependencies between Critical Infrastructures

The inter-dependencies between Critical Infrastructures (see above), including their links to emergency services and smart city systems, need to be addressed in a more holistic way to increase the safety and security of citizens. CI threats associated with transport and energy create cascading risks that ripple through interconnected CI systems and pose life-threatening conditions in affected areas. It is therefore evident that a comprehensive approach is needed to secure existing and interdependent CIs, which is accurate, efficient and cost-effective and (where possible) automated, that minimizes these cascading effects.

The goal of PRECINCT is to supervise and control complex interdependent networks and Cyber-Physical Systems of Systems (CPSoS). PRECINCT exploits the **Digital Twin concept**, historically used in industrial settings and more recently in Smart Cities, to model the current and future behaviour of territory-based interdependent CIs in a variety of conditions and configurations, to anticipate threats, to detect anomalies, and to incentivise optimised command structure and coordinated responses between CIs and first responders, thereby enhancing the resilience. In PRECINCT, vulnerabilities to previously unanticipated combinations of threats or cascading effects are identified through a **novel Serious Games approach**. The ingenuity of people (Gamers) will be exploited by data mining and ML (reinforcement learning) of Serious Games' gameplay records to pre-empt the potential for successful attacks and inform defence strategies. Along with the Digital Twin concept, the Serious Games in PRECINCT provides a means of testing and validating new detection and mitigation approaches in present-day real-life contexts.

The overall project's technical objective is to establish an Ecosystem Platform for connecting stakeholders of interdependent CIs and Emergency Services to collaboratively and efficiently manage security and resilience by sharing Data, Critical Infrastructure Protection models and new resilience services. The main outputs of PRECINCT are:

5.13.1 PRECINCT Framework Specification for systematic CI security and resilience management

PRECINCT specifies a Framework for systematic CIs security and resilience management, fulfilling industry requirements elicited with stakeholders within the LLs and integrating new insights from reference EU projects. The framework comprises of: (i) Needs analysis and CI Cascading effects Threat Scenarios, (ii) CI Interdependencies and Cascading Effects Knowledge Graphs, (iii) Resilience Methodological framework for resilience quantification (Resilience Index) and (iv) Short-term and long-term resilience enhancement measures

5.13.2 Cross-Facility collaborative cyber-physical Security and Resilience management Platform

The PRECINCT Ecosystem Platform implements the Framework Specification to be deployed and configured by different European CI Communities. It features a Directory of Smart CIP Blueprints to be exploited in LL driven developments. Its' innovation focuses on the benefits that combined integration of Digital Twins and Serious Games bring in CIPs as well as on enabling CIP providers to interact with CI stakeholders to establish new short-term and long-term measures that enhance resilience.

5.13.3 Vulnerability Assessment Tool - Serious Games

This tool supports the Resilience Methodological Framework and is integrated with the Digital Twins and the PRECINCT Ecosystem Platform and Services Directory. The Serious Games component spatially represents a series of modelled disaster scenarios enabling virtual experiments in the context of various capacity development strategies. Data Mining of gameplay Recordings help identify vulnerabilities to Cascading Cyber-Physical Threats. The integration with the Digital Twins generates probabilistic response functions and helps validate, refines and/or discover new CIP models. Finally, Serious Gaming is used for training through Learning and Competencies Scenarios applied across all Living Labs.

5.13.4 CI Digital Twins

PRECINCT's Digital Twins allow for smart and dynamic cyber-physical security and resilience supervision and control of cascading effects in territory-based CI Networks. PRECINCT is also developing tools to support the easy development of PRECINCT DTs focusing on interfacing with AI platforms/Neural nets, Serious Games and Cyber Range laboratories.

5.13.5 PRECINCT Living Labs (LLs)

PRECINCT has established four LLs providing both an experimentation environment and innovation testbed for the PRECINCT Infrastructure and Services to evaluate and improve the enablement and empowerment of CI communities to achieve tangible benefits from the connected CIs resilience approach. In addition, the transferability of the findings and the benefits of the PRECINCT approach, are demonstrated through 3 transferability demonstrators in: Luxemburg (Energy Tele-Communications focus), Dublin (Transport, Energy focus) and Uruguay (water, electricity and telecom focus).

Living Lab 1
Ljubljana (Slovenia)
Thematic Focus: Multi-CI Coordination Center for major city Transport Hub
June 2022
PRECINCT
Living Lab 2
Antwerp (Belgium)
Thematic Focus: Early warning system to prevent the impact of flooding Emergency Services coordinated CIs through city level DigitalTwin
June 2022
PRECINCT
Living Lab 3
Athens (Greece)
Thematic focus: Increased resilience against cyber-physical incidents affecting urban transport
September 2022
PRECINCT
Living Lab 4
Bologna (Italy)
Thematic focus: Region level Digital Twin linking multiple CIs with city ICT and IoT systems
September 2022
PRECINCT

Figure 24 - PRECINCT Living Labs

5.13.6 Resilience Improvement Workflows

PRECINCT has defined two workflows for CI Resilience Improvement and CI Operational Response Improvement utilizing all PRECINCT tools.

The first workflow, namely "PRECINCT Workflow for CI Resilience Improvement" comprises 3 phases: Design, Simulation & Resilience Index Calculation and Vulnerability Assessment through Serious Games.

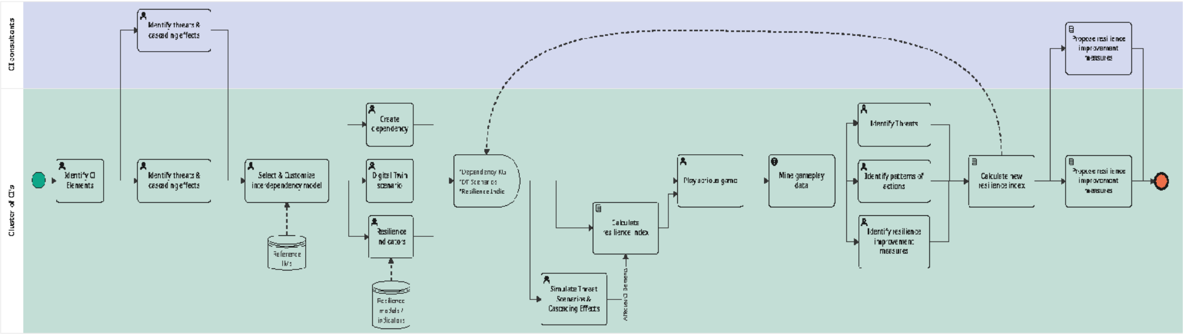

CI consultants
Cluster of CI's
Identify threats & cascading effects
Identify CI Elements
Identify threats & cascading effects
Select & Customize interdependency model
Reference IM's
Create dependency
Digital Twin scenario
Resilience indicators
Resilience models / indicators
*Dependency KG
*DT Scenarios
*Resilience Indic
Simulate Threat Scenarios & Cascading Effects
Affected CI Elements
Calculate resilience index
Play serious game
Mine gameplay data
Identify Threats
Identify patterns of actions
Identify resilience improvement measures
Calculate new resilience index
Propose resilience improvement measures
Propose resilience improvement measures

Figure 25 - PRECINCT Workflow for CI Resilience Improvement

The workflow starts with identifying the CI elements that are of interest. Each CI and the cluster of interdependent CIs collaboratively identify the CI elements that can be monitored and play a significant role in the resilience of the CIs. Next step is to identify threats for these elements and any cascading effects that are known or can be predicted. Based on these findings, the CI Operators can select and customize one of the Interdependency Models that PRECINCT framework provides or create a new one that fits the particular CI cluster configuration. Then this interdependency model is transferred to the PRECINCT Knowledge Graph module to produce the servitized version of the model, the Dependency Knowledge Graph (KG). The Digital Twin (DT) is used to produce threat Scenarios and with the help of the PRECINCT Framework, relevant Resilience Indicators are identified. The outcomes of this phase encapsulate the vulnerabilities, threats and cascading effects that were identified. These outcomes are: (a) the Dependency KG, (b) DT Threat Scenarios, (c) Resilience Indicators.

The next step is to utilize the outcomes of the Design phase to Simulate the Threat scenarios and Cascading effects in order to identify the affected CI elements. This information is then added to the results of the previous phase and the current Resilience Index is calculated.

Finally, the Serious Games come into play. Utilizing all the results from the previous phases, Serious Games are set up in order to perform Vulnerability Assessments both at the individual CI level and at the coordination level in clusters of CIs. CI Operators, First Responders, etc. play the games and react to threat scenarios and cascading effects. The gameplay data is then mined in order to identify: (a) Threats and Vulnerabilities, (b) Patterns of Actions, and (c) short- and long-term Resilience Improvement Measures.

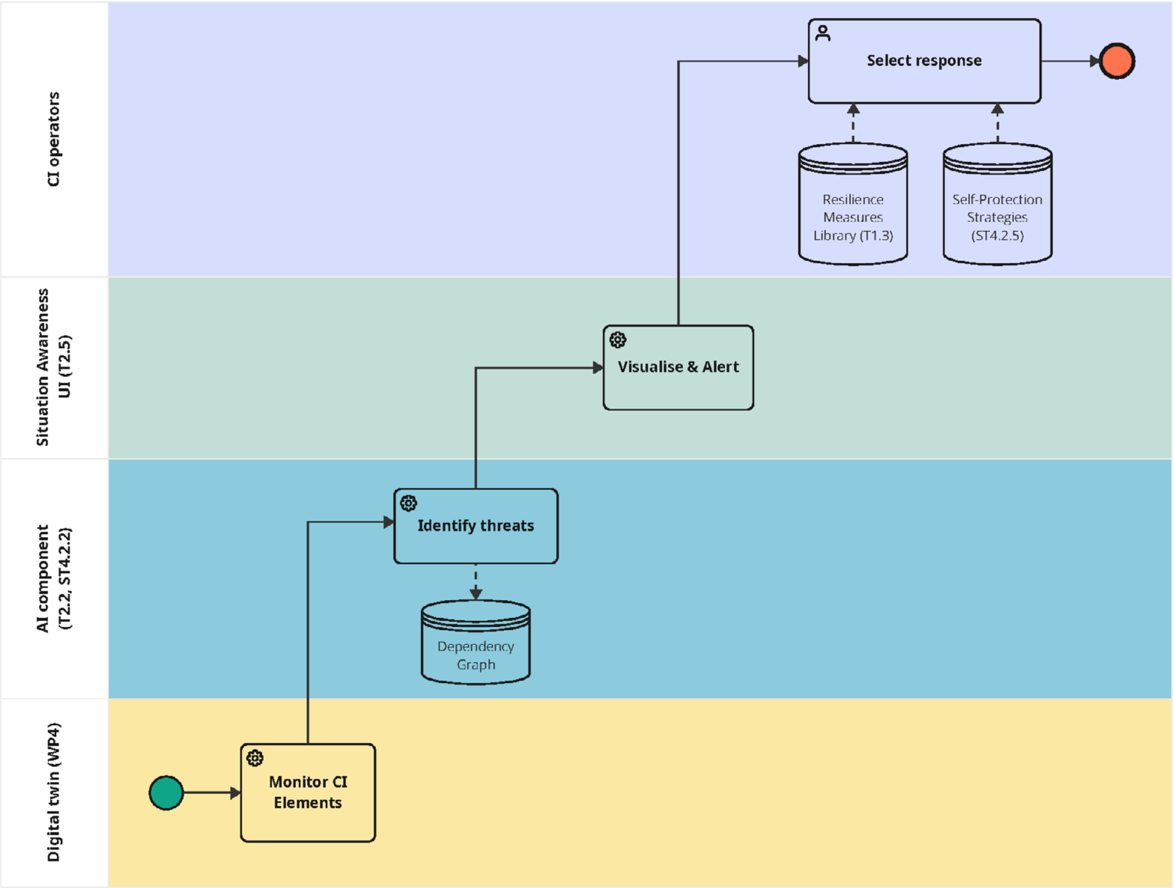

CI operators
Situation Awareness UI (T2.5)
AI component (T2.2, ST4.2.2)
Digital twin (WP4)
Select response
Resilience Measures Library (T1.3)
Self-Protection Strategies (ST4.2.5)
Visualise & Alert
Identify threats
Dependency Graph
Monitor CI Elements

Figure 26 - PRECINCT Workflow for Operational Response Improvement

The "Workflow for Operational Response Improvement, aims at enhancing situational awareness and alerting CI operators of upcoming threats through feedback loops and automated forensics enabled by the PRECINCT Platform. Here the Digital Twin is modelled to the specific scenarios of each LL. Associated data sources are connected to the PRECINCT infrastructure and enable the monitoring of the CI elements. AI algorithms, utilizing the Dependency Knowledge Graph, predict threats and cascading effects. The Situation Awareness UI provides monitoring capabilities to the CI operators but also alerts them of predicted threats and recommends suggested responses from the Resilience Measures Library and Self-Protection Strategies of the PRECINCT Framework.

For more information, please visit our project website: https://www.precinct.info/

5.14 Resilience enhancement and risk control for communication infrastructures

RESISTO (www.resistoproject.eu): Resilience enhancement and risk control for communication infrastructures - Bruno Saccomanno, Leonardo – Società per azioni

Communications play a fundamental role in the economic and social well-being of the citizens and in the operations of most of the Critical Infrastructures (CIs). Thus, they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also, extreme weather events and natural disasters represent a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. **RESISTO** platform is an innovative solution for Communication CIs to increase situation awareness and enhance CIs resilience. An integrated Risk and Resilience analysis management and improvement process is in charge to identify threats and prevent impacts as well as RESISTO implements an innovative Decision Support System to protect communication infrastructures able to detect negative events, respond and recover from physical, cyber and combined cyber-physical threatening events. A suite of state of the art cyber/physical threat detectors (Machine Learning based, IoT security, Airborne threat detection, holistic audio-video analytics) complete the platform. Through RESISTO, Communications Operators, will be able to implement a set of recovery actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation. RESISTO adopts a unified approach to face physical as well as cyber threats as well as a double and integrated approach between off-line and run-time activities applicable to different kinds of CIs.

RESISTO architecture

The logical architecture of RESISTO integrates two control loops both running on top of the Communication Infrastructure and interlinked with each other (see Figure 27), 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”, namely: Identify, Protect, Detect, Respond and Recover.

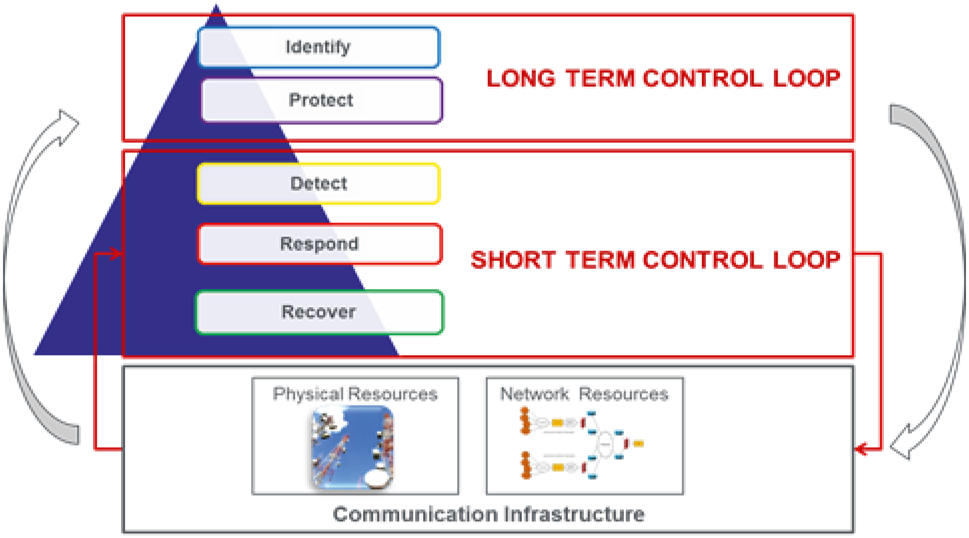


Figure 27 - RESISTO architecture

The Long-Term Control Loop (LTCL) is an off-line 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 assets configuration and interventions in order 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). A LTCL cycle is performed periodically 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, a 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.

Figure 28 reports the STCL functional control flow, and the main modules developed within RESISTO: Cyber/Physical Correlator, Risk Predictor, Workflow Manager, Orchestration Controller and Emergency Warning Communication function.

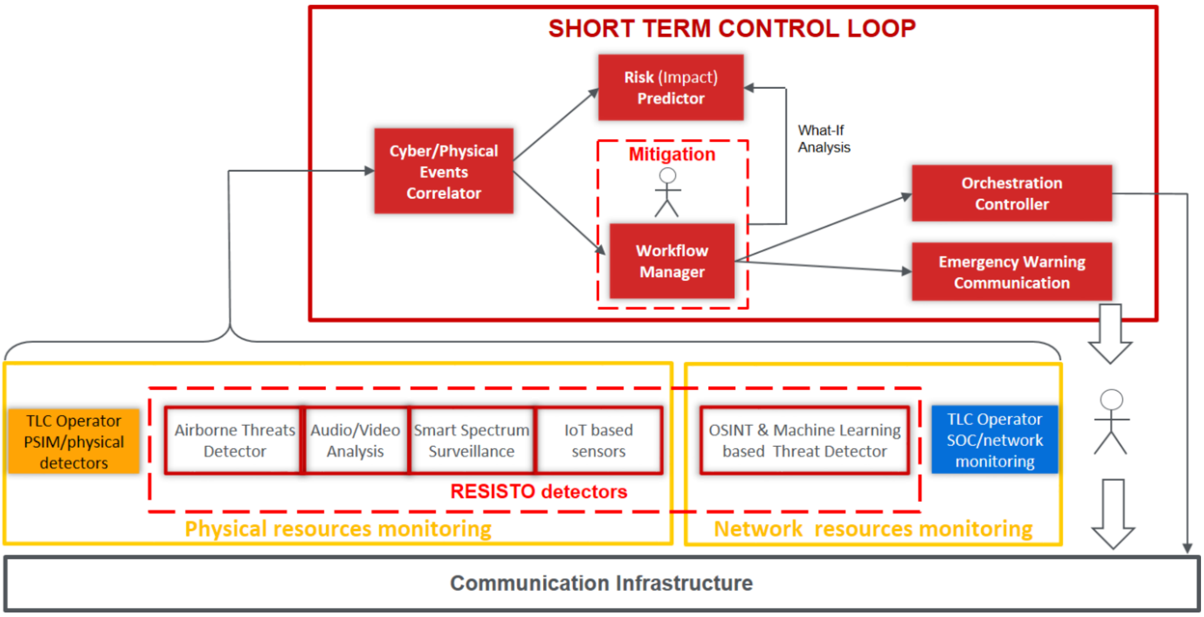

SHORT TERM CONTROL LOOP
Risk (Impact) Predictor
What-If Analysis
Cyber/Physical Events Correlator
Mitigation
Workflow Manager
Orchestration Controller
Emergency Warning Communication
TLC Operator PSIM/physical detectors
Airborne Threats Detector
Audio/Video Analysis
Smart Spectrum Surveillance
IoT based sensors
RESISTO detectors
Physical resources monitoring
OSINT & Machine Learning based Threat Detector
TLC Operator SOC/network monitoring
Network resources monitoring
Communication Infrastructure

Figure 28 - STCL functional control flow and the main modules developed

Input data to the STCL can be grouped into the following categories:

- physical events related to attacks (e.g., intrusions, damage) or to potentially dangerous events (e.g., unauthorized UAV flights)
- Cyber-attacks
- communication infrastructure physical layer/HW monitoring data (e.g., power and energy consumption and HW faults)
- communication network QoS monitoring data (e.g., offered traffic, throughput, latencies, error statistics, …)

The sources of such data and information could be:

- legacy Physical Security Information Management (PSIM) systems or other physical attack detectors made available by the telecommunication operator
- legacy Security Operating Centers (SOCs) or other cyber-attack detectors made available by the telecommunication operator,
- **RESISTO additional physical/cyber threat detectors** (e.g., airborne threats detection systems, smart spectrum surveillance, OSINT (Open-Source Intelligence)-based)

As part of the Horizon Results Platform (HRP) promoted by the European Commission, the following 11 Key Exploitable Results (KER) with a high potential value to be “exploited” have been defined:

1. Orchestrator
2. CISIApro 2.0 - Risk Predictor and Interdependecies Modeler
3. Cyber/Physical Events Correlator
4. Blockchain for Data Integrity
5. Audio and video analytics
6. Cyber-Physical Risk/Resilience Assessment of Communication Infrastructure
7. Machine Learning for Threat Intelligence
8. Emergency Warning Communication Function
9. Innovative secure deployment for IoT physical sensors

10. Responsible Disclosure Framework (RDF)
11. Software for Interdependency models

For more details regarding the RESISTO KERs please visit our website: http://www.resistoproject.eu/

Enhancing the concept of resilience in Telecom CIs

RESISTO defines a unique framework to assess the consequences of heterogeneous types of adverse events and suggest possible countermeasures. This concept is strictly dependent on improving resilience for large infrastructures, especially if they are interconnected with others, causing the so-called cascading effects. Interdependency analysis is at the base of real-time emergency response, as clearly stated by the RESISTO project. Having models of critical infrastructures and services delivered is at the base of decision-making during a crisis. RESISTO has improved such capability considering not only physical elements, but services that are supported by infrastructures and all different paths such services can have to the end-users. In this way, we can compute a real-time risk (the impact on the interconnected system) to be exploited in recovery actions.

In RESISTO, the key consistent elements of such a framework were developed and integrated into a single-pane-of-glass solution within the scope of improving situational awareness for the telecommunication end-users. The most policy-relevant findings are:

- Handling resilience indicators, measured/estimated quantitatively, considering both physical and cyber adverse events
- A unique framework to assess the effects of adverse events on large infrastructure, suggesting also possible mitigation actions and eventually automatically implement some of these actions
- The mitigation actions in telecommunication networks exploit network function virtualizations (NFV), software-defined networks (SDN), Internet of Things (IoT) solutions, and the future improvements leading to 5G networks

RESISTO use cases and recommendations

Considering the RESISTO use cases, we have to consider that some of them are based on novel 5G business models enabled by NaaS and the separation of service providers and (virtual) infrastructure providers, for which, to a large extent, regulation is still needed. In addition, apart from 5G, the possibility of sharing mobile access/edge network resources among competitor operators under certain circumstances (e.g., natural events such as forest fires affecting the availability of the mobile network in a certain zone) has been suggested for possible implementation as a way to avoid loss of communication, which is often a cause for aggravation of the effects of this kind of events.

A further drive to derive a series of best practices is recommended, in principle in the following areas:

- A consistent and scalable framework, composed of processes and software recommendations, is meant to help telecommunication operators to improve the assessment of specific vulnerabilities in their network assets
- Consistent and traceable methods for assessing the cascading effects of (at minimum) such threats as those described in the test scenarios of RESISTO
- A means of objective representation of resilience indicators that applies to most telecommunication operators
- A liability framework could be useful if not already exist. A system such as RESISTO does modelling, simulating cascading efforts and recommending mitigation actions should have clear policies that are reliable when the results cause damages and harm.
- Further research is needed for automating recommended mitigation actions such as using SDN to automate security, common message formats, etc.

5.15 Security of air transport infrastructure of Europe

SATIE (www.satie-h2020.eu): Security of air transport infrastructure of Europe by Tim Stelkens-Kobsch, German Aerospace Center (DLR)

The non-stop growth in air transport has increased pressure to boost cyber-physical security. The EU aviation security policy aims to ensure a proper balance between security and travel convenience, privacy and protection of personal data and operational factors. The EU-funded SATIE project created new “Security Operation Centre” philosophies for inclusion in a comprehensive airport security policy. This includes a holistic approach on threat prevention, detection, response and mitigation in airports, while ensuring the protection of critical systems, sensitive data and passengers. To do this, SATIE developed an interoperable toolkit that helps to improve cyber-physical correlations, forensic investigations and dynamic impact assessment at airports. Demonstrations were conducted at international airports in Croatia, Greece and Italy.

The recent high investments to secure Critical Infrastructures are a reaction to an increasing number of cyber, physical and combined cyber-physical attacks on Critical Infrastructures. As the latest developments show, even the number of hybrid attacks significantly increases, too. This endangers the integrity of single states and the entire EU. Current defence strategies are staggered and not combined to achieve efficient decision-making. The SATIE project was inaugurated in May 2019 and finished in October 2021. The developed product addresses exactly this EU need. The SATIE Solution takes cyber-attacks, physical-attacks, and combinations of them into account and has the potential to also detect hybrid attacks.

Potential solutions to increase the resilience of CI are operationally applicable Security Management Systems, which provide a security situation awareness for the operators in Security Operation Centres (SOCs). They should be able to communicate this with operators in airport operating centres (AOC) which then can get in contact with e.g., first responders. Following this, the SATIE Solution is set up as a modular system, which allows to interconnect security sensors and correlate their indications. These indications are finally presented as a holistic overview of the current security situation to the operators. Important to say is, that the monitoring is not limited to either cyber or physical sensors. SATIE successfully combines all kinds of sensors by weighing and rating them depending on correlation rules. These rules can be set up manually, while SATIE also provides AI-based proposals for new rules to the operators.

The SATIE Solution is comprised of a set of 14 innovation elements (IE) as shown in Table 2.

Table 2 - SATIE Innovation Elements

Ref	Name
IE1	Risk Integrated Service (RIS)
IE2	Vulnerability Management System (VuMS)
IE3	Secured Communication on the BHS
IE4	Unified Access Control (UAC)
IE5	Anomaly Detection on Passenger Records (ADPR)
IE6	Secured ATM Services
IE7	Traffic Management Intrusion and Compliance System (TraMICS)
IE8	Cyber Threat Detection Systems
IE9	Correlation Engine
IE10	Investigation Tool (SMS-I)
IE11	Impact Propagation Tools
IE12	Incident Management Portal (IMP)
IE13	Crisis Alerting System (CAS)
IE14	Cyber Range

These innovative solutions have been integrated into a simulation platform to improve the state of the art by solving pre-identified conceptual, technical, economical or societal limitations. The toolkit enables security practitioners and airport managers to collaborate more efficiently against individual physical or cyber threats, but most importantly, against complex scenarios combining both categories of threats.

Together, these innovation elements form a holistic toolkit covering all aspects from threat detection directly at airport systems and Air Traffic Control (ATC) systems to top-level management of incidents and impact mitigation, as well as from operational safety and security verified in the field to the security of the processes that govern the entire infrastructure.

As shown in Figure 29, the SATIE Toolkit is structured into Central Alerting Systems and their Supporting Systems, residing in the airport's Security Operation Centre and Airport Operation Centre, and Threat Prevention and Detection Systems implemented on the Airport & ATC Systems. Furthermore, it is embedded into a Validation Environment providing virtual simulation and on-site demonstration capabilities.

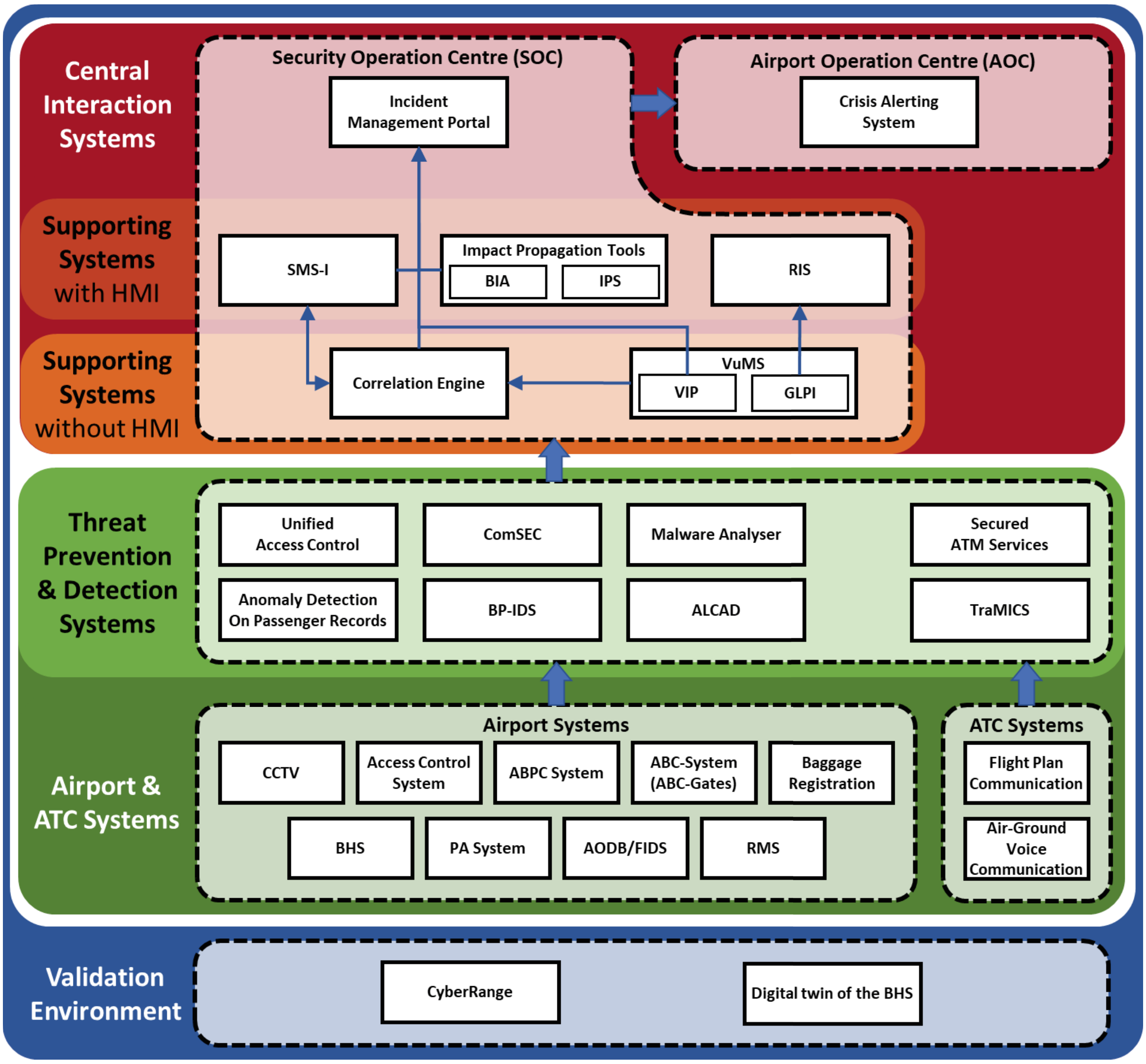


Figure 29 - Security management as proposed by SATIE

The two Central Alerting Systems represent the primary interfaces of the SATIE Toolkit designed for the operators in the Security Operation Centre and Airport Operation Centre.

The term “Security Operation Centre” describes part or the whole platform whose purpose is to provide detection and reaction services to security incidents. In the Security Operation Centre, information from a multitude of systems is collected to detect, identify, analyse, investigate, defend, and report physical and cyber incidents. To aggregate and correlate this data, a Security Information and Event Management (SIEM) system is employed, interconnecting with a variety of systems including intrusion prevention systems, endpoint detection and remediation, and threat intelligence platforms. SATIE’s Incident Management Portal (IMP) builds on this foundation, centralizing alerts from the entire toolkit, providing contextual information and access to the Supporting Systems, and enhancing communication with the Airport Operation Centre.

The AOC is in turn responsible for the management and optimization of all landside and airside processes as well as infrastructural, human, and equipment resources. It is essential that the operators here constantly have a clear and common overview of passenger flow, aircraft position on the apron, and the handling processes for departing, arriving and connecting baggage. Their main responsibility is information sharing and collaborative decision-making with the airport’s main stakeholders, such as airlines, air traffic control providers, ground handling agents, and first responders. The Crisis Alerting

System (CAS) presents the AOC operators with a unified interface that is deeply integrated with the SATIE Toolkit. Information from the SOC's Incident Management Portal and Supporting Systems are seamlessly and instantly shared with the CAS, improving the communication between the two centres. Furthermore, incident response times are shortened by unifying collaboration with airport stakeholders, first responders, passengers, and nearby citizens.

The work of the operators in the SOC and AOC is aided by five Supporting Systems situated in the Security Operation Centre. The first three of these are designed for direct user interaction and hence provide a Human Machine Interface (HMI) accessible from inside the IMP: The Investigation Tool (SMS-I) unifies the physical and cybersecurity investigation. It performs a deep analysis of activities and threats over a long-time frame to identify, in real-time, alerts stemming from the same attack. SMS-I also supports fast recovery in case of an incident by analysing past mitigation strategies using Machine Learning (ML) techniques. The two Impact Propagation Tools, Impact Propagation Simulation (IPS) and Business Impact Assessment (BIA), build interdependency models between airport assets, airport operations, and business processes to provide impact assessments and decision support. Finally, the Risk Integrated Service (RIS) enables pre-incident analysis of assets' risk levels and testing of 'what-if' scenarios to better determine the most efficient mitigation efforts.

In the background, the Correlation Engine as the core system of the SATIE Toolkit aggregates data from other Supporting Systems and the Threat Prevention and Detection Systems to correlate them based on a set of specified rules. Information on detected threats is forwarded to the Incident Management Portal. Additionally, the Vulnerability Management System (VuMS) enhances raised alerts with information on publicly known vulnerabilities. To this end, information on the airport's assets is collected by the Gestion Libre de Parc Informatique (GLPI), an open-source solution for IT (Information Technology) Service Management. The Vulnerability Intelligence Platform (VIP) then utilizes the asset database to build a list of know vulnerabilities associated with them.

The foundation of the SATIE Toolkit is constituted of eight Threat Prevention and Detection Systems located between airport and ATC systems and the Supporting Systems. They gather information from the airport systems and ATC systems, interpret the data, and determine whether there is relevant information to be conveyed to the Security Operation Centre. Improving physical security, the Unified Access Control monitors physical access points around the airport and the Anomaly Detection of Passengers Records detects persons of interest among passengers and ensures complete traceability of their baggage. Cyber threats such as malicious files and Denial-of-Service (DoS) or Man-In-The-Middle (MITM) attacks are detected by the Malware Analyser and the Application Layer Cyber Attack Detection (ALCAD). The Secured Communication on the BHS (ComSEC) and Business Process-based Intrusion Detection System (BP-IDS) additionally secure the Baggage Handling System (BHS) by monitoring network traffic to the BHS machines and business processes. Lastly, the Secured ATM Services and Traffic Management Intrusion and Compliance System (TraMICS) provide attack detection capabilities for the Air Traffic Control domain.

It should be noted that the toolkit has been implemented on the CyberRange, a virtual validation environment, and validated in a two-step approach: First, simulations were carried out with replicated airport systems. Then, the CyberRange was connected to the actual airport systems at the Athens International Airport "Eleftherios Venizelos", Milan-Malpensa, and Zagreb Airport "Franjo Tuđman" in order to demonstrate SATIE's benefits in real airport environments.

SATIE's best practices and recommendations for public partners were updated with knowledge received from standardisation bodies, policy makers, airport stakeholders and security practitioners and reported in a dedicated deliverable (D7.3 - Best practices for updating airport security standard and policies, available on project website). The document is an extensive report on existing regulations, standards, frameworks and guidelines in airport security (cyber and physical).

The D7.3 was reviewed by representatives of DG HOME, DG CNECT, European Aviation Safety Agency (EASA), European Defence Agency (EDA), EUROCONTROL (specifically the Civil-Military Coordination-DECMA/CMC Division), German Air Navigation Service Provider (DFS) and the Centro Italiano Ricerche Aerospaziali (CIRA, specifically the Department of Reliability Availability Maintainability Safety & Security).

The recommendations for improvement, which were confirmed by the reviewers are the following:

- Improve security by utilizing SATIE's proposed innovative risk assessment methodology (advance cyber/physical security by utilizing a set of techniques).
- Improve security and current guidelines for Industrial Control Systems (ICS). → Explore ICS system characteristics, e.g., SCADA, and use SATIE Innovation Elements (IE) to reinforce ICS common best practices.
- Take the recommendations and best practices for improving the cyber/physical security tasks of an (A)OC.
- Introduce SATIE's best practices for improving anomaly detection on cyber/physical threats, including passenger data (i.e., SATIE check-in step/ border crossing step).
- Apply recommendations for airports employees' biometric access control deployment (i.e., accuracy of solution, GDPR compliance, security implementation).
- Adopt best practices related to airport crisis management and decision support operation and apply relevant existing security regulation framework (i.e., identify security gaps/propose holistic crisis management process).

SATIE also provided some initial input to improve and enhance existing standards by providing a policy brief on aviation security including lessons learned and several proposed recommendations. This document was handed over to DG Home in early 2022 (after the closing of the project). Looking at the contribution SATIE has delivered to standards it needs to be said, that it is a real challenge to set up a standard with a two-years-project.

However, SATIE managed to not only work on standards and policies but also produced a policy brief, which contains another set of recommendations on how to improve security in CI.

Finally, there is the "real" target group of the project, the operators in Security Operation Centres and Airport Operation Centres. Those operators who had the possibility to experience hands-on practice with the SATIE toolset were entirely excited and gave feedback like the following:

- Operators could react swiftly; the simulation of impact propagation assists operators in impact mitigation.
- Operators felt they were able to react quicker to physical and cyber threats compared to the current system.
- The IMP was rated as a great improvement compared to the operators' current situation.
- The operators were able to easily find the sought information, which was well understood as well as that the tools at hand allowed for low-effort decision-making.
- The unified SATIE Solution is preferred over the current system. Even the unconnected SATIE Tools without the information being correlated by the Correlation Engine were deemed as an additional value.

When specifically looking at the information exchange approach, the feedback was:

- CAS: Very much appreciated by operators as it provides novel functionalities to quickly raise awareness and organise mitigation measures.

Looking at the feedback above, the final words can just be that SATIE added a relevant piece of cake to the resilience of critical entities.

For more info: www.satie-h2020.eu

5.16 Scalable, trusted, and interoperable platform for secured smart GRID

SealedGRID (www.sgrid.eu): Scalable, trusted, and interoperable platform for secured smart GRID by Christos Xenakis, University of Piraeus

Grant Agreement Number: 777996
Project Acronym: SealedGRID
Topic: "MSCA-RISE-2017 Research and Innovation Staff Exchange"

SHORT ABSTRACT

The consortium consists of 3 Universities and 3 SMEs,

- University of Piraeus from Greece
- University of Malaga from Spain
- National Inter-University Consortium for Telecommunications from Italy
- BEIA Consult International SRL, from Romania
- Neurosoft S.A.,
- Fogus from Greece

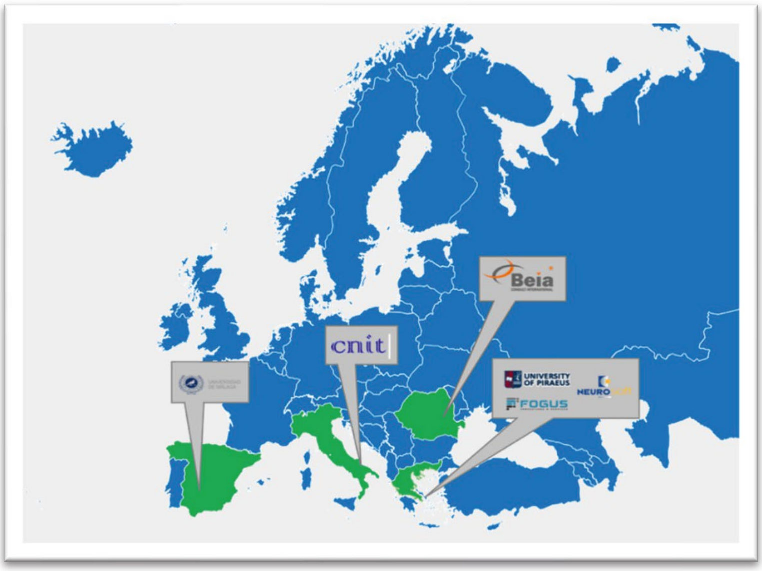


Figure 30 - SealedGRID consortium

The project consists of 7 Work Packages.

- Project Management and Coordination (WP1)
- Requirements, Business Cases and Architecture (WP2)
- Key Management and Authentication (WP3)
- Trusted Computing and Privacy Protection (WP4)

- Authorization and Security Interoperability (WP5)
- Platform Integration and Assessment Experiments (WP6)
- Dissemination, Standardisation, and Exploitation (WP7)

Most of WPs are complete and the consortium is now working on the final one, the Integration and Assessment of the platform.

Aim-Objectives

The rapid evolution of ICT has revealed the potential for centrally monitoring, controlling, and optimising the power grid. In this context, a more intelligent, responsive, and efficient, system has been devised, known as the Smart Grid (SG). As explained in the EU Third Energy Package the SG will support a dynamic two-way information exchange between utility companies and their customers, contributing towards a smart and sustainable energy management in Europe and the establishment of a wiser energy consumption mentality. However, besides the benefits of such an endeavour, the power grid will be exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities, related to the specific characteristics of the SG infrastructure, will emerge. The problem is assessed as crucial, if we consider that a potential attack on the SG may lead to cascading failures, ranging from the destruction of other interconnected critical infrastructures to the loss of human lives. Thus, the development of a security platform tailored to the SG is required, that i) can efficiently manage the plethora of SG nodes, ii) deal with potential malicious hardware or software modifications due to the physical access of the customers to the SG nodes, and iii) operate over heterogeneous systems. Considering all the above, SealedGRID aims to bring together experts from industry and academia from cross-sectorial research areas having a complementary background with the long-term goal to design, analyse, and implement a scalable, highly trusted and interoperable SG security platform. The platform will combine, for the very first time, technologies like Blockchain, Distributed Hash Tables, Trusted Execution Environments, and OpenID Connect, while for its realization the SealedGRID consortium is committed to a fully integrated and multi-disciplinary secondment programme combined with a set of networking, dissemination, and exploitation activities.

Architectural design and main components

The SealedGRID architecture presents the components of the system and protocols used to communicate between them, while also considering the business case and system requirements. The reference architecture is the basis for the design and the implementation of the technical solutions for SealedGRID and utilizes three main different components:

1. Smart Meters, collect electricity consumption reading
2. The Aggregators are intermediate nodes between the collectors and the smart meters.
3. Utility calculates the final billing and produces the energy.

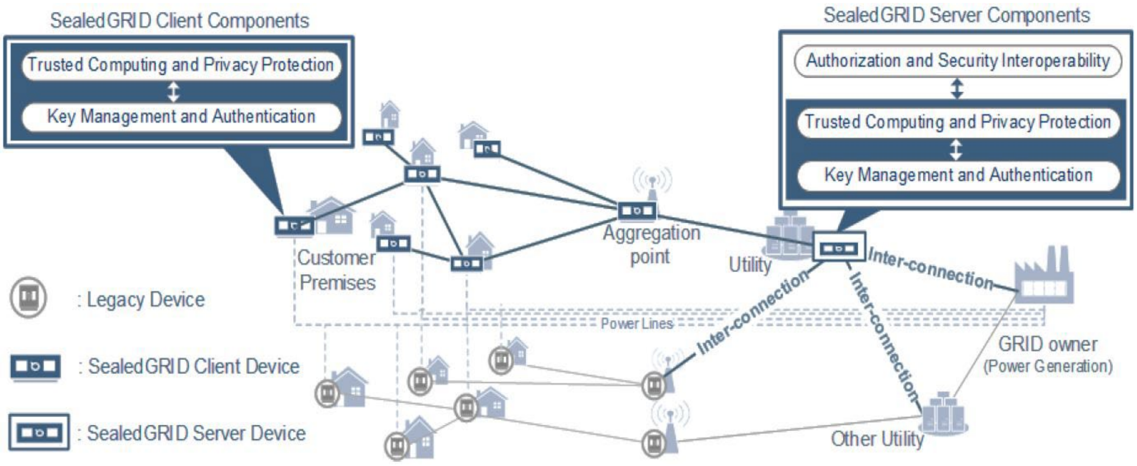

SealedGRID Client Components
Trusted Computing and Privacy Protection
Key Management and Authentication
SealedGRID Server Components
Authorization and Security Interoperability
Trusted Computing and Privacy Protection
Key Management and Authentication
Customer Premises
Aggregation point
Utility
Inter-connection
Inter-connection
Inter-connection
GRID owner
(Power Generation)
Power Lines
Other Utility
: Legacy Device
: SealedGRID Client Device
: SealedGRID Server Device

Figure 31 - SealedGRID architecture

In the architecture, a mix of SealedGRID-equipped and legacy devices that implement different or even obsolete security mechanisms are considered.

Platform main components

The SealedGRID platform consists of six main components. Those are in brief:

1. Key Management (W3)
2. Authentication (WP3)
3. Trusted Computing (WP4)
4. Privacy Protection (WP4)
5. Authorization and (WP5)
6. Security Interoperability (WP5)

Main achievements/innovations/KERs

The power grid is exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities, related to the specific characteristics of the SG infrastructure, will emerge. The platform is tailored to the SG, and can

I. efficiently manage the plethora of SG nodes,
II. deal with potential malicious hardware or software modifications due to the physical access of the customers to the SG nodes, and
III. operate over heterogeneous systems.
IV. combine, for the very first time, technologies like Blockchain, Distributed Hash Tables, Trusted Execution Environments, and OpenID Connect.

SealedGRID consortium innovations include:

MENSA: In the process of designing the Key Management component for the project, developed MENSA which is the First distributed hybrid key management and authentication system for microgrids.

I. is a Peer- to-Peer solution for authentication services. Each agent can place its own trust policy while keeping the autonomous characteristics of the nodes intact
II. It Allows frequent actions of node Join and Leave without network efficiency impact
III. Due to its decentralized nature, it is not a single point of failure.

The component evaluation included a series of performance tests with the first one being the Node Join Time Delay and the Second the Chain length. The results show Minimal increases in nodes saved at finger tables and no significant changes in MENSA as the size of the grid increases. Following the probability that two random nodes will be able to establish a trust relationship between them in relation to the chord ring size was tested and finally the average time needed for trust relationships. The results are more than adequate for the platform's needs

MASKER: In the process of designing the Privacy component for the project, developed MASKER which is a privacy protection mechanism for exchanging energy consumption readings for electricity grids that deals with

I. Masking and Unmasking Consumption Values,
II. Key sharing, And
III. Achieving a Trusted Execution Environment collaboration

The consortium is presently working on the performance testing phase.

Future work

Following the implementation of the components of the platform, specifically in the field of Secret Key Sharing research highlighted the need for the evolution of the platform in that field which will include the introduction of threshold cryptography. Research work is already underway and primary results are expected in the next months.

MAIN IDEA

The power grid is exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities, related to the specific characteristics of the SG infrastructure, will emerge. The project is developing a security platform tailored to the SG, that

I. can efficiently manage the plethora of SG nodes,
II. deal with potential malicious hardware or software modifications due to the physical access of the customers to the SG nodes, and
III. operate over heterogeneous systems.

The platform has combined, for the very first time, technologies like Blockchain, Distributed Hash Tables, Trusted Execution Environments, and OpenID Connect.

Technical details - Implementation

In the process of creating and evaluating the platform, SealedGRID Consortium established a virtual experimentation environment. The six main platform components (Key Management, Authentication etc.) developed for the needs of the platform have been set-up and evaluated in a standalone basis initially. The environment is established in a server of virtual machines where the components were initially developed one at a time. The next step was the consolidation of all the components in a stack creating the homogenous platform. The system architecture components (Smart Meter, Aggregator, Utility) were simulated in ARM devices with multiple virtual machines following the parameters set in the beginning of the project. Now in the final stage of the project, the Use Cases that were defined at the beginning of the project will be implemented and the results will be utilized in the evaluation of the platform.

Experimental Protocols

The experimental processes followed, and performance, security and other indicators vary, depending on the component that was tested. Different measurements were taken when executing simulations from each platform component. The common denominator is the fact that all simulations were carried out multiple times, to verify the soundness and repetitiveness of the results under the same environment.

Main Outcomes – Conclusions

The main outcomes at this stage indicate that SealedGRID platform developed components on a standalone basis perform above expectations and results are promising (i.e., Network Load and Response times). During this period the consortium is working on setting up the platform as a complete uniform system and conducting the evaluation testing based on the selected Use Cases. Based on the progress so far, the results are estimated to be above expectations.

5.17 An integrated, yet installation specific, solution for the resilience of gas infrastructure against cyber and physical threats

SecureGas (www.securegas-project.eu): An integrated, yet installation specific, solution for the resilience of gas infrastructure against cyber and physical threats by Celina Solari (Clemente Fuggini), RINA Consulting

Title: Securing the European Gas Network
Topic: "SU-INFRA01-2018 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe"
Grant Number: 833017

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 make them resilient to cyber-physical threats.

SecureGas overall objective is to increase the SECURITY & RESILIENCE of the EU Gas Critical Infrastructure, considering both physical and cyber threats, as well as their combination.

Securegas has the following ambitions regarding the EU Gas CI:

- Resist to hazards and absorb their impacts more efficiently and effectively.
- Be designed/restored to coordinate more efficiently across the various phases of a disaster risk management cycle.
- Accommodate and recover the effects of hazards more timely and safely, reducing the magnitude and/or duration of their consequences and allowing a fast recovery from disruption.

This project aims to propose a Resilience-based approach that links Resilience Capabilities (Plan/Prepare, Detect, Absorb, Recover, Adapt) to the Crisis Management Cycle (Prevention, Preparedness, Response, Recovery), embedding them into an Asset Management Process (ISO55001).

A multidisciplinary consortium (gas operators, technology providers, research institutions, and sector-related associations), has supported the project implementation across Construction, Demonstration and Validation phases, as well as a Stakeholder Platform that ensures inputs, advice, and wider diffusion of the project outcomes.

SecureGas has been conceived as a Business Case (BC) driven project. BC have been designed by the end-users in the consortium, fitting the needs of various type of first users (after the project ends) across the gas supply value chain (from upstream to midstream to downstream).

Technical and non-technical challenges have been faced to provide solutions which are operational or available. The challenges came from the needs and requirements of the different users and stakeholders, so from the market in the end and from the different requirements of the gas supplies and value chain, in particular from both the upstream and the downstream transmission and distribution.

To face it, SecureGas has developed a modular, adaptable and scalable architecture, **the SecureGas High-Level Reference Architecture**, which is a reference framework for the implementation, integration and interoperability of SecureGas components.

Another relevant challenge was to provide a viable business model to sustain impact and support take up: a Software as a Service (Saas) solution has been implemented acting as a single access point to SecureGas integrated solutions

All these issues were tackled by SecureGas through also a set of tools, methods and solutions, updated, incrementally improved, federated according to High-Level Reference Architecture (HLRA) built upon the SecureGas Conceptual Model (CM), a blueprint on how to design, build, operate and maintain the EU gas network to make it secure and resilient against cyberphysical threats. The components are contextualised, customised, deployed, demonstrated and validated in each BC, 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.

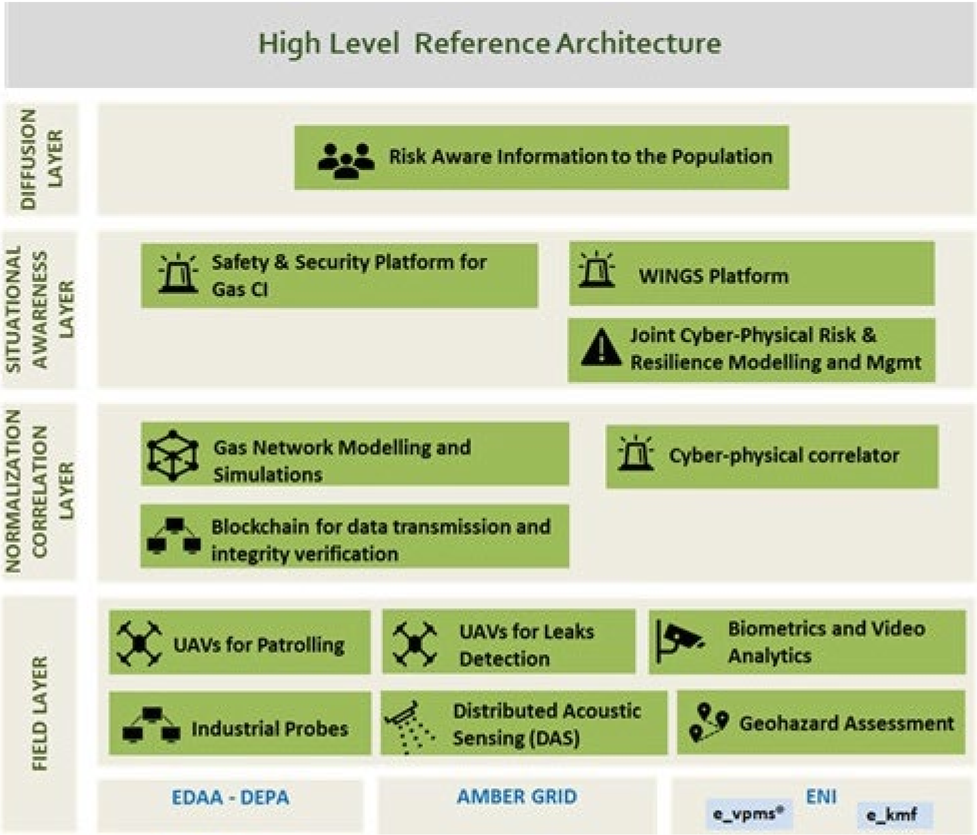
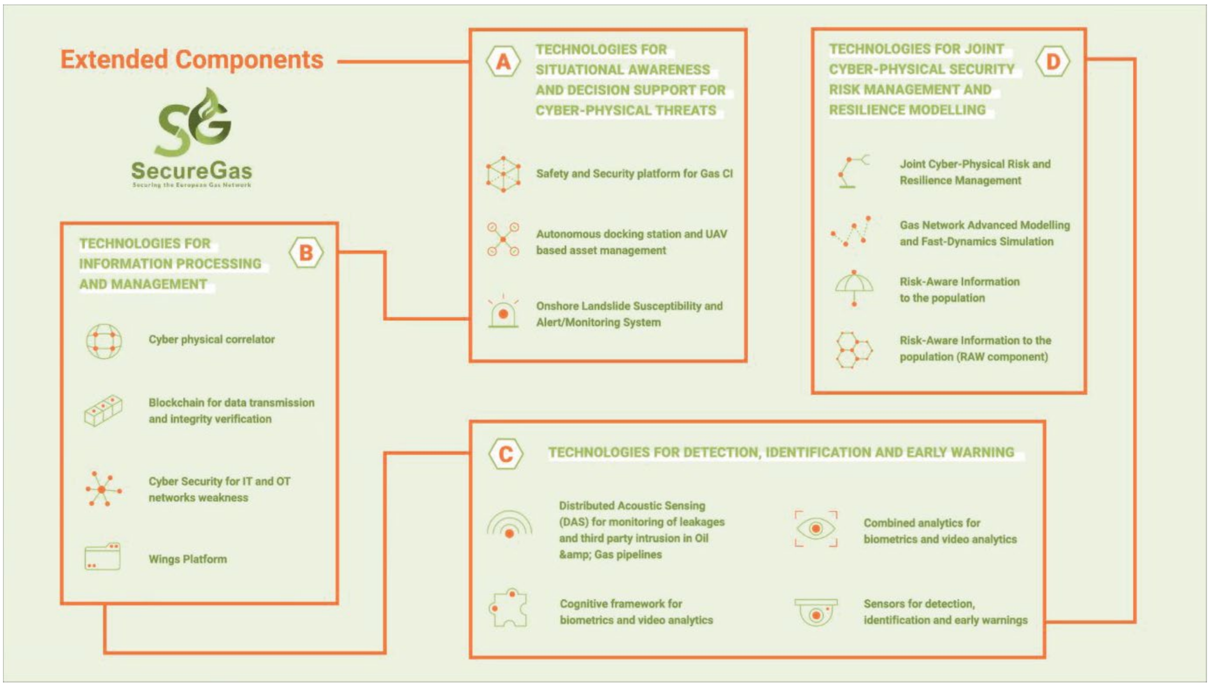

High Level Reference Architecture
DIFFUSION LAYER
Risk Aware Information to the Population
SITUATIONAL AWARENESS LAYER
Safety & Security Platform for Gas CI
WINGS Platform
Joint Cyber-Physical Risk & Resilience Modelling and Mgmt
NORMALIZATION CORRELATION LAYER
Gas Network Modelling and Simulations
Cyber-physical correlator
Blockchain for data transmission and integrity verification
FIELD LAYER
UAVs for Patrolling
UAVs for Leaks Detection
Biometrics and Video Analytics
Industrial Probes
Distributed Acoustic Sensing (DAS)
Geohazard Assessment
EDAA - DEPA
AMBER GRID
ENI
e_vpms®
e_kmf

Figure 32 - SecureGas High Level Reference Architecture

The SecureGas advanced components can be grouped into 4 categories:

- Technologies for situational Awareness and Decision Support for Cyber-Physical Threats;
- Technologies for information processing and management;
- Technologies for detection, identification, and early warning;
- Technologies for joint cyber-physical security risk management and resilience.

The service products developed within the SecureGas project are aimed at CI managers as they are innovative developments of market solutions.



Extended Components
SecureGas
Securing the European Gas Network
A
TECHNOLOGIES FOR SITUATIONAL AWARENESS AND DECISION SUPPORT FOR CYBER-PHYSICAL THREATS
Safety and Security platform for Gas CI
Autonomous docking station and UAV based asset management
Onshore Landslide Susceptibility and Alert/Monitoring System
D
TECHNOLOGIES FOR JOINT CYBER-PHYSICAL SECURITY RISK MANAGEMENT AND RESILIENCE MODELLING
Joint Cyber-Physical Risk and Resilience Management
Gas Network Advanced Modelling and Fast-Dynamics Simulation
Risk-Aware Information to the population
Risk-Aware Information to the population (RAW component)
B
TECHNOLOGIES FOR INFORMATION PROCESSING AND MANAGEMENT
Cyber physical correlator
Blockchain for data transmission and integrity verification
Cyber Security for IT and OT networks weakness
Wings Platform
C
TECHNOLOGIES FOR DETECTION, IDENTIFICATION AND EARLY WARNING
Distributed Acoustic Sensing (DAS) for monitoring of leakages and third party intrusion in Oil &amp; Gas pipelines
Combined analytics for biometrics and video analytics
Cognitive framework for biometrics and video analytics
Sensors for detection, identification and early warnings

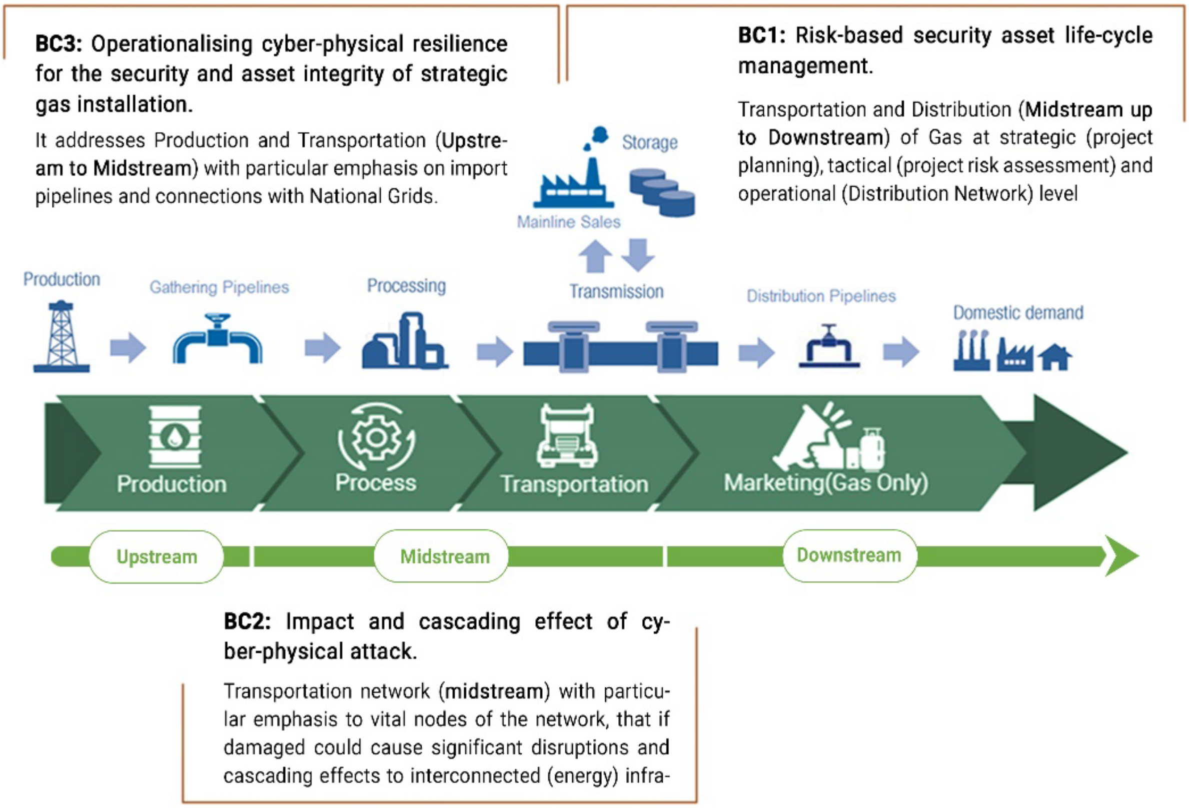
Figure 33 - SecureGas Advanced components

One of the main Securegas features is that it has included in 3 Business Cases addressing relevant issues for the Gas sector and beyond (e.g., oil) to ensure the delivery of solutions and services in line with clear needs and requirements. The modularity and scalability of the SecureGas architecture allows end-users to exploit selectively only the functions and services they need, as demonstrated by the 3 Business Cases.
All SecureGAs solutions have been identified demonstrated and validated in 3 specific areas:

a) Business Case 1 (BC1), located in Greece: here SecureGas addresses the transportation and distribution of gas at the strategic, tactical and operational levels.

b) Business Case 2 (BC2), located in Lithuania: here SecureGas targets the transportation network with particular emphasis on to impact and cascading effect of cyber-physical attack.

c) Business Case 3 (BC3), located in Italy: here SecureGas focuses on production and transportation with particular emphasis on operationalizing cyber-physical resilience for the security and asset integrity of the strategic gas installation.



BC3: Operationalising cyber-physical resilience for the security and asset integrity of strategic gas installation.

It addresses Production and Transportation (**Upstream to Midstream**) with particular emphasis on import pipelines and connections with National Grids.

BC1: Risk-based security asset life-cycle management.

Transportation and Distribution (**Midstream up to Downstream**) of Gas at strategic (project planning), tactical (project risk assessment) and operational (Distribution Network) level

BC2: Impact and cascading effect of cyber-physical attack.

Transportation network (**midstream**) with particular emphasis to vital nodes of the network, that if damaged could cause significant disruptions and cascading effects to interconnected (energy) infra-

Figure 34 - SecureGas Business Cases

Totally **24 KERs** have been identified within SecureGas, between them:

a) SG Conceptual Model: blueprint on how to design, build, operate and maintain the EU gas network to make it secure and resilient.

b) SG High-Level Reference Architecture: a reference framework for the implementation, integration and interoperability of SecureGas components.

c) A set of advanced components customized, deployed, demonstrated, and validated in the three project business cases, according to policy-relevant scenarios.

d) A Cost Benefit Analysis to asset the benefits and impact of SG in the three Business Cases.

e) SG White paper “Lessons learnt and recommendations for cyber-physical resilience of European Gas Critical Infrastructure”.

The SG project outputs listed above have contributed to the policy certification and standard landscape through liaison activities with key stakeholders and organizations in the domain at European and National levels and the Elaboration of proposals on improved or new certification mechanisms.

In the coming years the EU will be heavily dependent on non-EU critical supplies, and Gas clearly play a critical and strategic role in this, however, thanks to SecureGas MSs and Cis operators could have now knowledge, tools and solutions, to put in place forward-looking actions to anticipate potential new risks and failures.

For more details regarding SecureGas Project please visit our website: www.securegas-project.eu.

5.18 Cyber-security protection in healthcare IT ecosystem

SPHINX (sphinx-project.eu): Cyber-security protection in healthcare IT ecosystem by Evangelos Markakis, Electrical & Computer Engineering Department, Hellenic Mediterranean University-HMU, Crete, Greece

Data theft, denial-of-service (DoS), and ransomware are all major concerns within a healthcare infrastructure. Cybercriminals target hospitals and care centres by exploiting outdated and vulnerable services, and cybersecurity unaware personnel. The aforementioned issue underlines the need for a holistic cyber security vulnerability assessment toolkit for healthcare infrastructures, which is able to proactively assess and mitigate cyber-security incidents imposed by network-enabled entities and services within the infrastructure. SPHINX introduced a Universal Cyber Security Toolkit, enhancing the cyber protection of healthcare ecosystems and ensuring patient data privacy and integrity. Through the SPHINX toolkit, the IT department of a medical, clinical, or health infrastructure is able to choose from a variety of cyber security services provided by the SPHINX cybersecurity toolkit. These services are easily adapted and deployed on existing or new health infrastructures. Moreover, service providers are given a platform to specify, sell or advertise their services through a secure and easy to use user interface. SPHINX was validated through pan-European demonstrations in three different scenarios. The proposed cyber-security ecosystem and the overall solution were evaluated in three different nations against performance, effectiveness, and usability parameters (Romania, Portugal, and Greece). In the project's pilots, hospitals, care centres, and device manufacturers implemented and assessed the solution in both routine and emergencies across a variety of use case scenarios.

Figure 35 depicts the overall SPHINX architecture as well as the components it pertains.

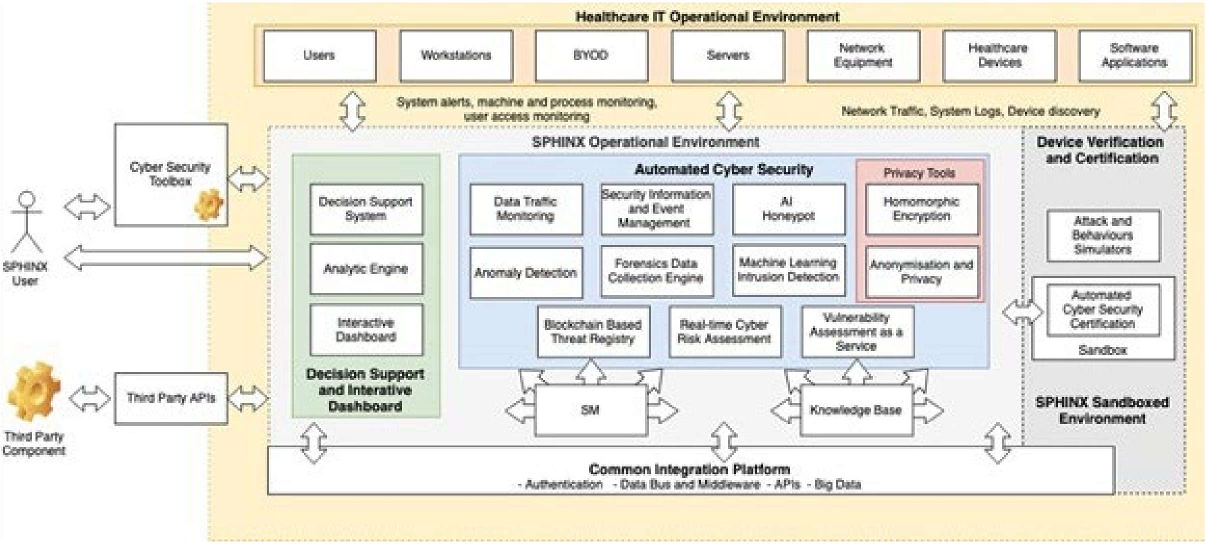

Healthcare IT Operational Environment
Users
Workstations
BYOD
Servers
Network Equipment
Healthcare Devices
Software Applications
System alerts, machine and process monitoring, user access monitoring
Network Traffic, System Logs, Device discovery
Cyber Security Toolbox
SPHINX User
Third Party APIs
Third Party Component
SPHINX Operational Environment
Decision Support System
Analytic Engine
Interactive Dashboard
Decision Support and Interative Dashboard
Automated Cyber Security
Data Traffic Monitoring
Security Information and Event Management
AI Honeypot
Anomaly Detection
Forensics Data Collection Engine
Machine Learning Intrusion Detection
Privacy Tools
Homomorphic Encryption
Anonymisation and Privacy
Blockchain Based Threat Registry
Real-time Cyber Risk Assessment
Vulnerability Assessment as a Service
SM
Knowledge Base
Device Verification and Certification
Attack and Behaviours Simulators
Automated Cyber Security Certification
Sandbox
SPHINX Sandboxed Environment
Common Integration Platform
- Authentication - Data Bus and Middleware - APIs - Big Data

Figure 35 - SPHINX Architecture

Out of the main components, the Vulnerability Assessment as a Service (VAaaS) component that was developed by HMU was tasked with the continuous monitoring of the underlying network for existing and newly introduced network-enabled entities; assessing entities against known vulnerabilities, producing detailed vulnerability assessment reports, mitigation actions (if any) and a vulnerability assessment score, based on the CVSS standard, propagate the reports to the message broker and expose a RESTful API for ad-hoc requests [Nikoloudakis 2019]. Furthermore, the Machine Learning-empowered Intrusion Detection (MLID) component enables the identification of potential attackers, classifying them into specific attack categories using data generated by the SPHINX Artificial Intelligence Honeypot [Markakis 2019].

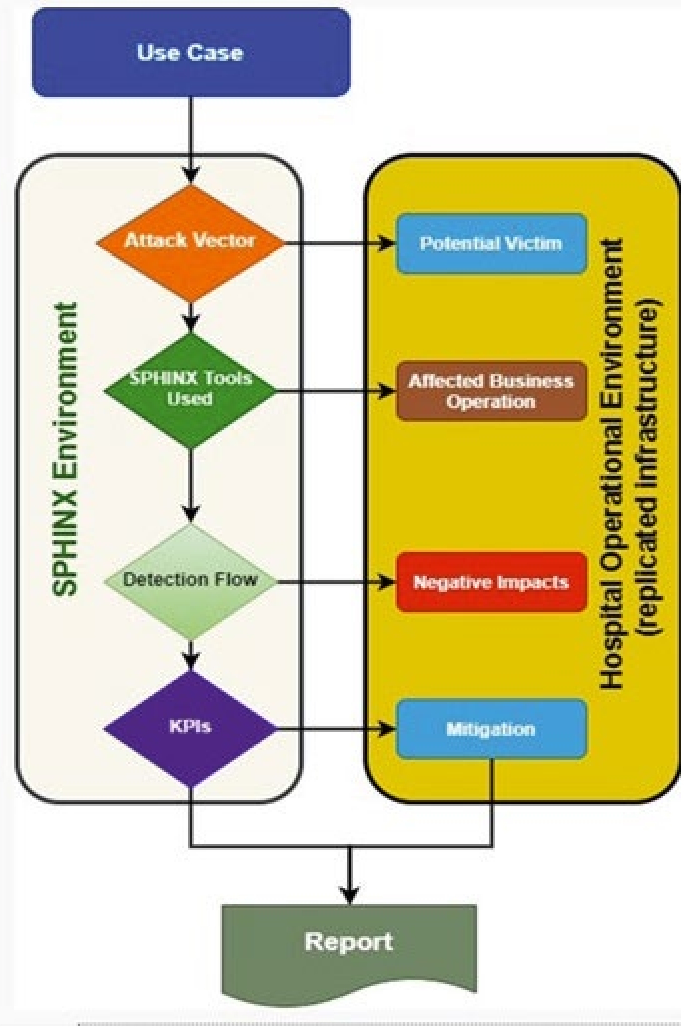


Figure 36 - Pilot execution Methodology

Regarding achievements, we executed unique real-life scenarios and test cases in all three [Nikoloudakis 2021] pilots following the methodology in Figure 36. Throughout the duration of the SPHINX project, a total of 16 scientific publications were released, stored in the Zenodo community, and 3 Workshops in our pilot sites.

To conclude, further work is needed to bring all of the components to market maturity, however, there is an imminent need for automation in the cybersecurity field, alleviating the IT personnel from the burden of tedious, repetitive, and time-consuming tasks such as updating the same services in the infrastructure. For that reason, our goal is to implement the Robotic Process Automation (RPA) [Adhikari 2020], within our ecosystem and chain of processes. The RPA framework will be able to record past actions that the admin took to patch vulnerabilities, and with the use of agents implemented in the infrastructures' network-enable entities, it will be able to reproduce these steps and patch the vulnerabilities in an automated way

5.19 Protection of critical water infrastructures

STOP-IT (stop-it-project.eu): Protection of critical water infrastructures by Rita Ugarelli, SINTEF AS

Water supply and sanitation infrastructures are essential for our welfare, but vulnerable to several attack types - facilitated by the ever-changing landscapes of the digital world.

Taking robust proactive steps to prevent, detect and mitigate cyber-physical attacks is mandatory for the sector and it has to be achieved through adaptive protocols since cyberattacks will continue to escalate in rate of recurrence and sophistication.

The COVID-19 pandemic has made even more manifest the vulnerabilities of the sector: water utilities had to open an operational environment for remote connections to employees and suppliers working from home to maintain the business running, but at the price of increased risk for cyber-attacks.

Although many utilities have invested resources in cybersecurity, more progress is necessary to secure water infrastructure at the strategic, tactical and operational decision levels.

The ultimate goal of the **STOP-IT** project has been 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.

During the four years of collaboration, the STOP-IT consortium has collaborated in different directions: raising awareness about cybersecurity in the water sector, by organizing dedicated thematic communities of practice; supporting water utilities to systematically protect their systems by addressing cyber-physical security as an integrated approach and by developing technological solutions; and improving the ability to cope with new risks, by building competence through training activities.

The STOP-IT outcomes (technological and non)

The STOP-IT project has delivered an integrated platform which is **Scalable** (scaling from small utilities to large ones), **Adaptable** (including various modules addressing different needs, with expandability for future modules, and **Flexible** (the water utility managers can decide how to use it and it will be usable by experts, novices, and even non-technical staff).

The STOP-IT platform has to be understood as a "lego-like" architecture, in which the different "bricks" can be applied as standalone, but also in combination, thanks to the established interoperability between the different components. Therefore, the platform provides users with the option to select technologies, which are more relevant for the specific challenges, while leaving open the possibility to build on the selection by adding additional "bricks" so to intensify, on need, the protection against combined cyber-physical threats and allowing the analysis of cascading effects of physical and cyber events.

The STOP-IT platform’s ultimate goal is to protect critical water infrastructures from physical and cyber threats. The threats that are addressed are the following:

- **Cyber**: Voluntary or not intent of individuals or groups to electronically corrupt or seize control of data or information essential to system operations.
- **Physical**: The threat is a physical occurrence on the water supply system. By the physical type of threats, assets or technical devices of the water supply system will be damaged or manipulated. The physical threat may also destroy or damage sensors, data transmission lines or the process control/SCADA system in a way that the normal function is no longer possible.

- **Cyber-Physical**: The threat as a combined cyber-physical nature. It can generate in different ways, as for instance:
    - **Combined cyber-physical threats**: coordinated and long-term attacks to the CI to reach and compromise the normal functioning.
    - **Cyber threat to any of the physical component of the water infrastructure**, e.g., monitoring devices (including e.g., IP cameras, networked sensors, AMR/AMI) that become more vulnerable to cyber-attacks due to their higher automation/networking level.
    - **Physical threats to the "cyber" environment of the water utilities**, e.g., Intrusion of attackers to the utilities control & operation centres (access to computers) or SCADA devices, etc.

The platform supports strategic/tactical planning, real-time operational decision making and post-action assessment for the key parts of the water infrastructure. This is possible, through the integration of the STOP-IT solutions at the strategic/tactical level and operational level, plus additional solutions developed to further support the water CI protection.

The STOP-IT platform integrates nine modular components (Figure 37) containing a total of 28 tools, methods, services and/or platforms brought by the STOP-IT partners.

The platform was validated in an operational environment and all solutions have been demonstrated in real environments, thus, all solutions have reached at least the TRL 7.

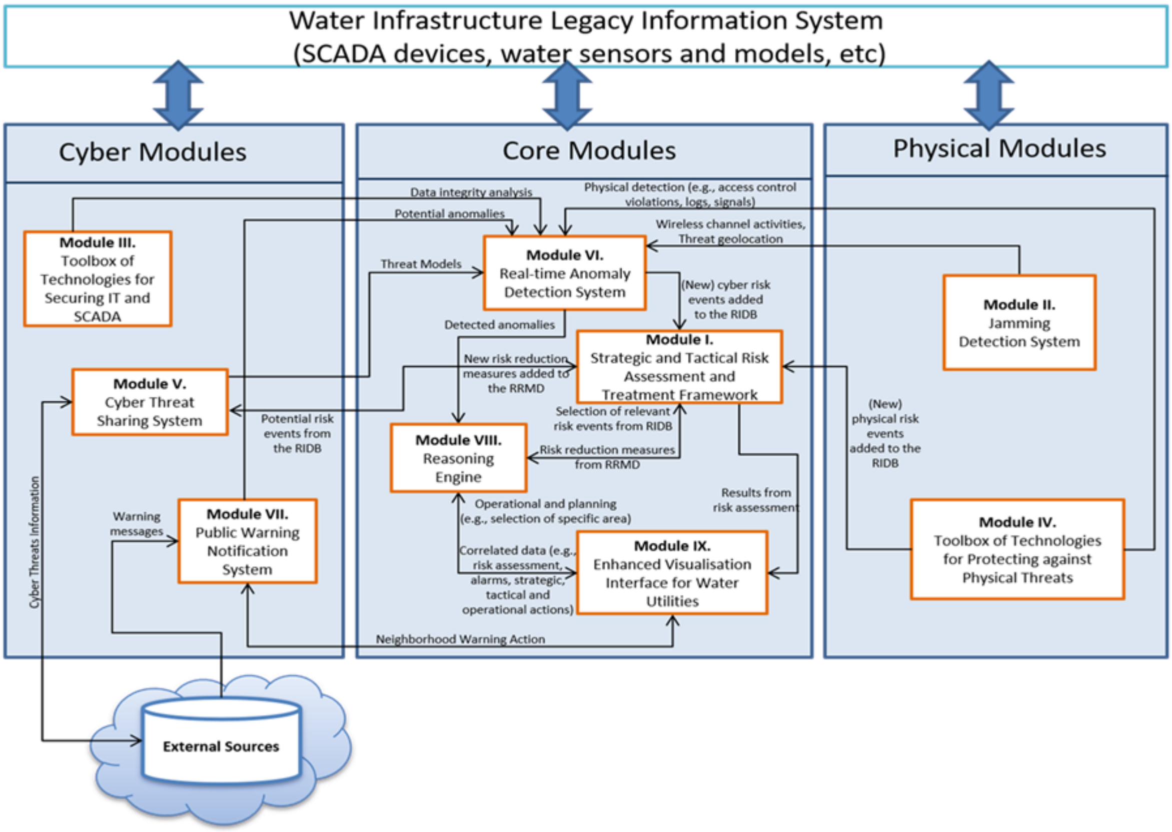

Water Infrastructure Legacy Information System
(SCADA devices, water sensors and models, etc)
Cyber Modules
Core Modules
Physical Modules
Data integrity analysis
Physical detection (e.g., access control violations, logs, signals)
Potential anomalies
Wireless channel activities, Threat geolocation
Module III. Toolbox of Technologies for Securing IT and SCADA
Threat Models
Module VI. Real-time Anomaly Detection System
(New) cyber risk events added to the RIDB
Module II. Jamming Detection System
Detected anomalies
Module I. Strategic and Tactical Risk Assessment and Treatment Framework
New risk reduction measures added to the RRMD
Module V. Cyber Threat Sharing System
Potential risk events from the RIDB
Selection of relevant risk events from RIDB
(New) physical risk events added to the RIDB
Module VIII. Reasoning Engine
Risk reduction measures from RRMD
Cyber Threats Information
Warning messages
Module VII. Public Warning Notification System
Operational and planning (e.g., selection of specific area)
Results from risk assessment
Correlated data (e.g., risk assessment, alarms, strategic, tactical and operational actions)
Module IX. Enhanced Visualisation Interface for Water Utilities
Module IV. Toolbox of Technologies for Protecting against Physical Threats
Neighborhood Warning Action
External Sources

Figure 37 - The STOP-IT platform architecture

At the strategic and tactical level the project has developed Module I (Figure 37), 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 digital 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 the strategic/tactical level.

At the operational level, the project has provided innovative solutions for risk treatment (prevention, detection, mitigation, and recovery) of water CIs. The range of the proposed protections schemes has been broad and comprehensive covering the full spectrum from communications to IT and SCADA systems, to physical protection. These solutions are (Figure 37): 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, the Network Traffic Sensors and Analysers and the Real-Time Sensor Data Protection; solutions for "physical protection of water infrastructure" comprising (Module IV): the Access Control System using Electronic Locks, the Computer Vision Tools, the Fine-grained Cyber Access Control, the Human Presence Detector using WiFi signals and the Water Quality Sensor Placement Tool; Module VI, providing the Real-time Anomaly Detection System and the Module V, Cyber Threat Sharing System.

Further, in addition to the creation of a fully operational and technically evaluated (and demonstrated) platform, additional solutions have been produced, such as Module VII, the Public Warning Notification System; Module VIII, the Reasoning Engine and Module IX, the Enhanced Visualisation Interface for Water Utilities (Figure 37).

STOP-IT has created Communities of Practice (CoPs) to contribute to the protection of critical water infrastructure against physical and cyber security threats by raising awareness on this topic in the water sector, encouraging and facilitating information sharing, and development and transferability of knowledge and tools between infrastructure operators, experts, communities and other stakeholders clustered in communities of practice. Three levels of CoP approaches are used:

- **Local CoP (L-CoP)**: one for each Front Runner (FR) water utility 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, the R&D experts and also Followers (FL), if appropriated);
- **Project CoP (P-CoP)**: designed to establish a network of different groups of stakeholders on the project and open to a broader audience (i.e., Follower (FL) water utilities, national water associations, first aid associations);
- **Trans-project CoP (T-CoP):** crossing boundaries between different CI sectors, involving international networks and non-project expert groups.

These three levels CoP approaches, T-CoP, P-CoP, and L-CoP have been successful in bringing together professionals and scientists in the domain of water cyber-physical security to share their knowledge and experience, to find a common understanding and to develop tools to protect critical infrastructure against cyber-physical threats. However, the L-CoPs and P-CoPs tended to focus on the specific characteristics of the STOP-IT cases. The tools developed in STOP-IT are highly technical and their development requires ensuring security and privacy. The complexity and confidentiality issues made the development process very complex, which in turn made it difficult to engage external stakeholders at a local and project level.

At the T-CoP level, STOP-IT has been successful at creating a lasting alliance, by successfully connecting the project to already existing initiatives that will outlive the project, most notably, STOP-IT's participation with the INFRA Scoping group resulting in contributing to workshops organized by DG home, the set-up of the ECSCI together with other EC funded projects on the topic of cyber-physical protection of CIs, and the participation in the ICT4Water cluster. It is through these initiatives and activities that STOP-IT has also contributed to influencing the European policy on cyber security.

As for the L-CoPs and the P-CoPs, the lessons learned from four years and 38 CoP meetings have led to the design of a step-by-step guidance for the design and implementation of CoPs that is currently applied in newly started H2020 projects (Ultimate, B-WaterSmart, WaterMining). This way, STOP-IT's influence on CoPs in the European context reaches beyond the project itself.

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)).

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 STOP-IT technology developers.

The FR operators have been actively involved in most of the project activities: they contributed to the exploration and categorization of risk events and risk management measures relevant to their water infrastructure, engaged in the CoPs, supported the adaptation and improvement of innovative solutions and have been responsible for the demonstration of the STOP-IT platform and selected modules at their demo-site. Furthermore, they have provided a "user experience" assessment including a list of barriers and suggestions per tool as valuable information for the technological providers in order to better position their product in the market.

In order to enhance practical knowledge on effective cyber-physical water infrastructure protection, training and knowledge transfer materials and products have been delivered and revised through interaction with the FL water utilities; to this purpose, training activities have been performed for the three different user profiles for which the material has been customized: the decision-makers, the risk assessment officers and the staff responsible for real-time operations.

The FL water utilities have undertaken the training and knowledge transfer exercises, with a focus on the experimentation, interactive learning and transferability and scalability of solutions provided by the project. The FLs have also contributed to the definition of user requirements along with the dedicated events of the project's CoPs and have been involved in the "road map" process to allow evaluating the market uptake and replication of STOP-IT outcomes.

Given the number of deliverables and the results produced during the project and in particular in the last two reporting periods, the STOP-IT dissemination activities performed by the project team are remarkable and have continued until the very end of the project (and beyond) at full speed.

A business plan and the exploitation strategy for each of the 28 KERs have been created following an approach consisting of three phases; Phase 1: stakeholders and market analysis, and exploitation potential assessment of the project results; Phase 2: exploitation strategy definition; and Phase 3: exploitation roadmap.

Interested readers can find fact sheets for each tool and technology along with training and dissemination materials on a dedicated https://stop-it-project.eu/results-and-downloads/.

5.20 A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats

7SHIELD: A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats by Gerasimos Antzoulatos, Centre for Research and Technology-Hellas – CERTH

7SHIELD project is a collaborative Innovation Action H2020 project aiming to develop a holistic framework to protect EU Ground Segments of Space Systems (GSSS) facilities against cyber and physical threats. Specifically, in the new security landscape of Europe, the GSSS appear as potential "new targets" for "new threats", especially the combined cyber-physical (C/P) ones. A C/P attack on their installations or communication networks, respectively, would cause cascading impacts and affect the public safety and security of European citizens on one hand and other European Critical Infrastructures (CIs) on the other hand. Hence, the main objective of the 7SHIELD project is to encapsulate mature solutions that are enabled to confront complex threats by covering all the macro stages of crisis management, namely Pre-crisis, Crisis and Post-crises phases, in order to protect GSSS infrastructures and strengthen their resilience.

To achieve this objective, a series of innovation objectives (IO) have been consolidated (Figure 38) including:

- ***IO1 – Prevention technologies for physical and cyber threats***: the deployed technologies contribute to the pre-crisis phase by involving the vulnerability assessments of the GSSS assets, secure authentication mechanisms for data access and cascade effects analysis from combined cyber-physical attacks, as well as threat intelligence on cyber-physical threats to enhance the current situational picture with new insights.
- ***IO2 – Detection technologies for physical and cyber threats***: state-of-the-art detections technologies have been encompassed to seamlessly and accurately identify potential physical or/and cyber threats to Space Systems, Ground Segments and Satellite data assets.
- ***IO3 – Response technologies***: innovative technologies to monitor the evolvement of C/P attacks, to strengthen responsiveness and social awareness have been tailored.
- ***IO4 – Mitigation technologies for physical and cyber threats***: the appropriate actions to mitigate the consequences of C/P attacks, focusing on the services continuity have been consolidated.

The 7SHIELD Logic Architecture (Figure 39) is a multi-layered architecture in which all the modules and technologies for Pre-crisis, Crisis and Post-crisis phases are integrated into a highly modular, flexible and easily customised framework which integrates twenty (20) Key Results (technology bricks). Seventeen (17) of them are related to prevention (4), detection (7) and response and mitigation (6) technologies. The rest of them concerns the data models, the system integration and the User Interfaces.

The **Cyber-Physical Layer** contains all the data sources that provide to the 7SHIELD platform raw data which are captured from cyber and physical sensors located in the field. *Information sources,* such as drones, CCTVs, thermal and near-infrared sensors, laser fences, etc. from physical world and spam, logs, antivirus, etc. from cyber part will be used to collect data in terms of physical and cyber threats and attacks to the GSSS assets.

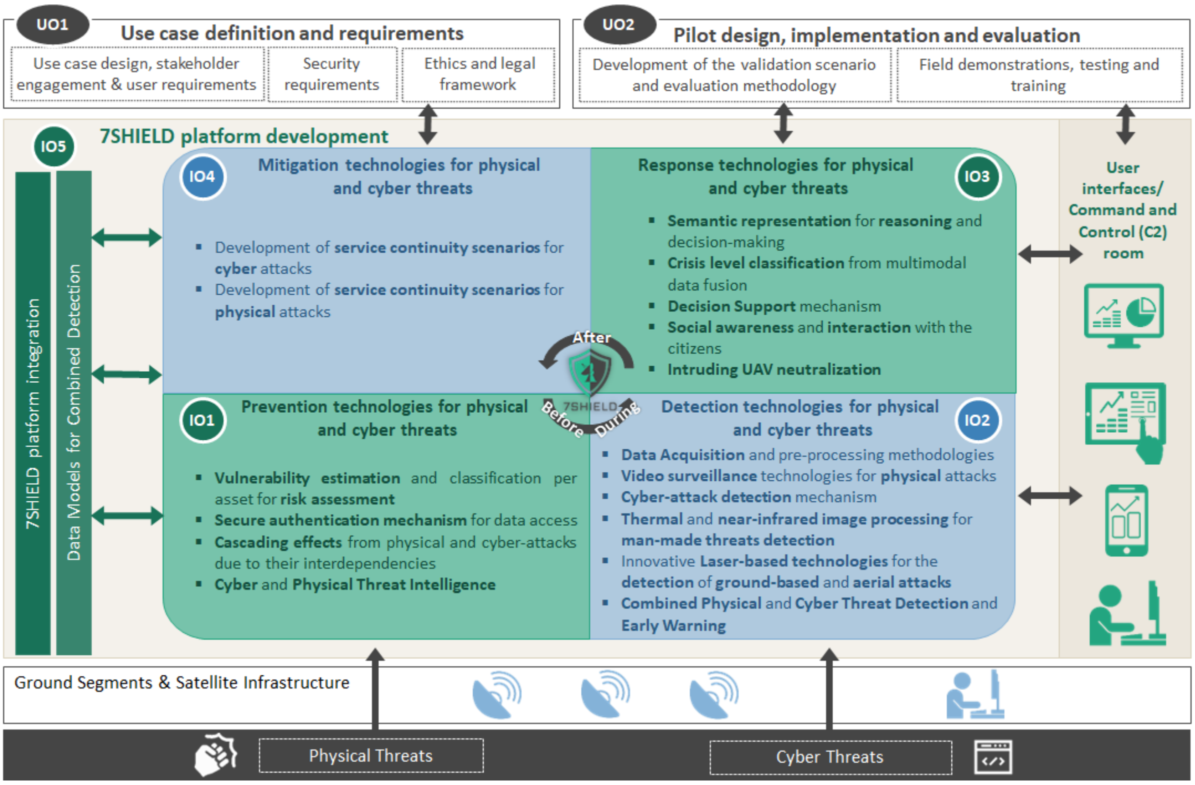

UO1
Use case definition and requirements
Use case design, stakeholder engagement & user requirements
Security requirements
Ethics and legal framework
UO2
Pilot design, implementation and evaluation
Development of the validation scenario and evaluation methodology
Field demonstrations, testing and training
IO5
7SHIELD platform development
7SHIELD platform integration
Data Models for Combined Detection
IO4
Mitigation technologies for physical and cyber threats
Development of service continuity scenarios for cyber attacks
Development of service continuity scenarios for physical attacks
Response technologies for physical and cyber threats
IO3
Semantic representation for reasoning and decision-making
Crisis level classification from multimodal data fusion
Decision Support mechanism
Social awareness and interaction with the citizens
Intruding UAV neutralization
After
Before
During
7SHIELD
IO1
Prevention technologies for physical and cyber threats
Vulnerability estimation and classification per asset for risk assessment
Secure authentication mechanism for data access
Cascading effects from physical and cyber-attacks due to their interdependencies
Cyber and Physical Threat Intelligence
Detection technologies for physical and cyber threats
IO2
Data Acquisition and pre-processing methodologies
Video surveillance technologies for physical attacks
Cyber-attack detection mechanism
Thermal and near-infrared image processing for man-made threats detection
Innovative Laser-based technologies for the detection of ground-based and aerial attacks
Combined Physical and Cyber Threat Detection and Early Warning
User interfaces/ Command and Control (C2) room
Ground Segments & Satellite Infrastructure
Physical Threats
Cyber Threats

Figure 38 - 7SHIELD objectives

The **Detection Layer** encompasses innovative detection tools that enable the identification of abnormal events, cyber and physical threats, and raise alerts. These tools concern the *Data collection from UAVs and edge processing* to detect objects and persons, the *Video surveillance technologies* to detect and recognize faces of suspicious individuals, identify and track objects of interests via processing video streams from surveillance cameras, the *MultiModal Automated Surveillance (MMAS)* system to detect the presence of intruders, such as moving objects and people, within the boundaries of an area under surveillance using thermal and near-infrared sensors coupled with computer vision algorithms, the *Laser-based detection system* detects ground based and aerial intrusion using LIDAR technology. Furthermore, the *Cyber-Attack Detection Framework* is based on the collection of information at several architectural levels (namely: Physical, Network, Operating System, Data Base, Application, and Business Process). The so obtained information will be processed by employing sophisticated data analysis techniques for cyber-attack detection.

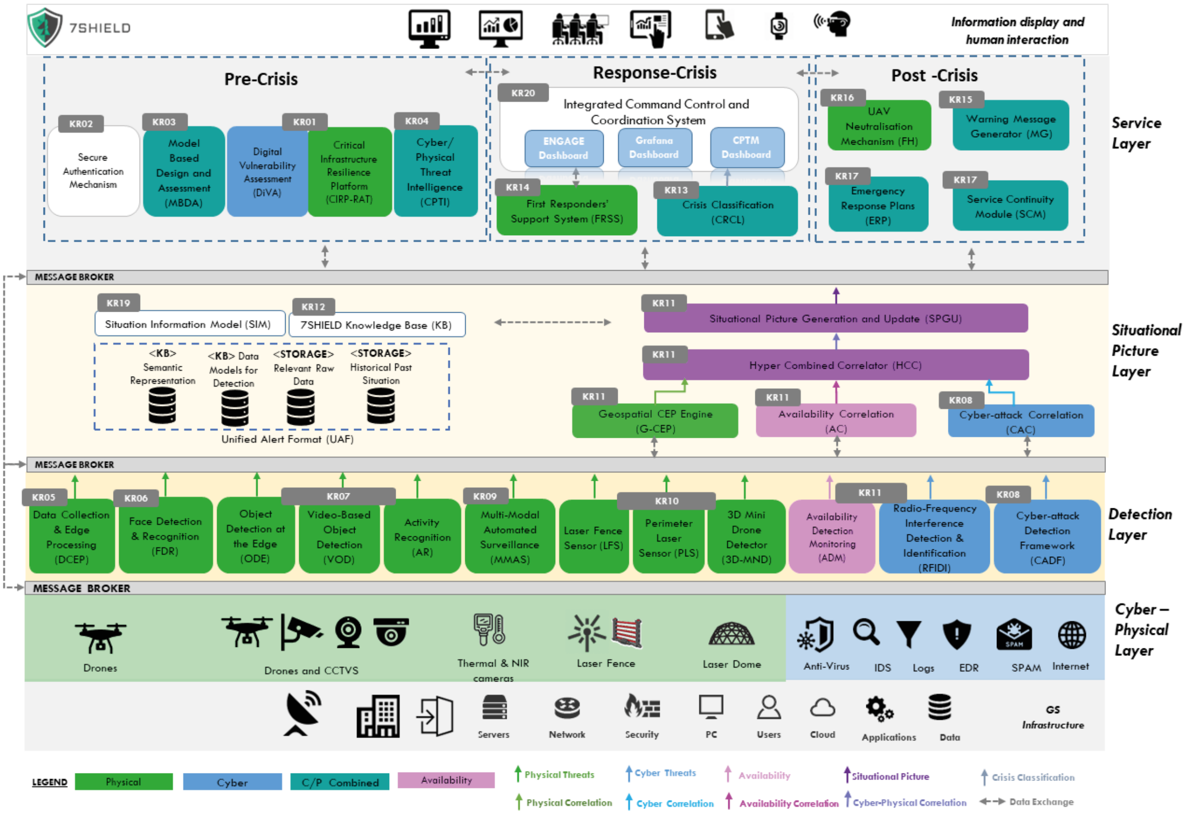

7SHIELD
Information display and human interaction
Pre-Crisis
KR02
Secure Authentication Mechanism
KR03
Model Based Design and Assessment (MBDA)
Digital Vulnerability Assessment (DiVA)
KR01
Critical Infrastructure Resilience Platform (CIRP-RAT)
KR04
Cyber/ Physical Threat Intelligence (CPTI)
Response-Crisis
KR20
Integrated Command Control and Coordination System
ENGAGE Dashboard
Grafana Dashboard
CPTM Dashboard
KR14
First Responders' Support System (FRSS)
KR13
Crisis Classification (CRCL)
Post -Crisis
KR16
UAV Neutralisation Mechanism (FH)
KR15
Warning Message Generator (MG)
KR17
Emergency Response Plans (ERP)
KR17
Service Continuity Module (SCM)
Service Layer
MESSAGE BROKER
KR19
Situation Information Model (SIM)
KR12
7SHIELD Knowledge Base (KB)
<KB> Semantic Representation
<KB> Data Models for Detection
<STORAGE> Relevant Raw Data
<STORAGE> Historical Past Situation
Unified Alert Format (UAF)
KR11
Situational Picture Generation and Update (SPGU)
KR11
Hyper Combined Correlator (HCC)
KR11
Geospatial CEP Engine (G-CEP)
KR11
Availability Correlation (AC)
KR08
Cyber-attack Correlation (CAC)
Situational Picture Layer
MESSAGE BROKER
KR05
Data Collection & Edge Processing (DCEP)
KR06
Face Detection & Recognition (FDR)
Object Detection at the Edge (ODE)
KR07
Video-Based Object Detection (VOD)
Activity Recognition (AR)
KR09
Multi-Modal Automated Surveillance (MMAS)
Laser Fence Sensor (LFS)
KR10
Perimeter Laser Sensor (PLS)
3D Mini Drone Detector (3D-MND)
Availability Detection Monitoring (ADM)
KR11
Radio-Frequency Interference Detection & Identification (RFIDI)
KR08
Cyber-attack Detection Framework (CADF)
Detection Layer
MESSAGE BROKER
Drones
Drones and CCTVS
Thermal & NIR cameras
Laser Fence
Laser Dome
Anti-Virus
IDS
Logs
EDR
SPAM
Internet
Cyber – Physical Layer
Servers
Network
Security
PC
Users
Cloud
Applications
Data
GS Infrastructure
LEGEND
Physical
Cyber
C/P Combined
Availability
Physical Threats
Cyber Threats
Availability
Situational Picture
Crisis Classification
Physical Correlation
Cyber Correlation
Availability Correlation
Cyber-Physical Correlation
Data Exchange

Figure 39 - 7SHIELD high level architecture

The **Situational Picture Layer** contains modules to process (validate and correlate) and analyse the real time cyber and physical events in order to identify potential complex cyber and physical attacks. At this level, the obtained information assists operators to comprehend the current *situational picture* which is homogenised and enriched semantically by the 7SHIELD Knowledge Base and Data Models. After that, the updated situational picture proceeds to the Service Layer.

In general, the **Service Layer** contains all the services used by the experts to prevent, manage and mitigate the threats associated with cyber-physical attacks in the Satellite Ground Segment domain. Hence, it encompasses technologies for the *prevention and preparedness activities (pre-crisis phase)* to assess the risk of natural, physical and cyber threats, to model complex CIs and analyse the cascading effects caused by threats into their assets. Furthermore, services for the analysis of social network to support the evaluation of the likelihood of cyber threats are included. A Secure Authentication Mechanism has been adopted to assure that the authentication to these services is performed in a secure way. It facilitates the smooth and secure authentication of users and services to the 7SHIELD framework in a privacy-preserving manner. Other services concern the real-time assessments of the severity level of the ongoing C/P attacks to enrich further the current situational picture, the *First Responders Support System (FRSS)* to enhance field operations and mission coordination of the First Responders (FRs). It enables FR teams to be self-aware and have more information to support effective decision making in the field.

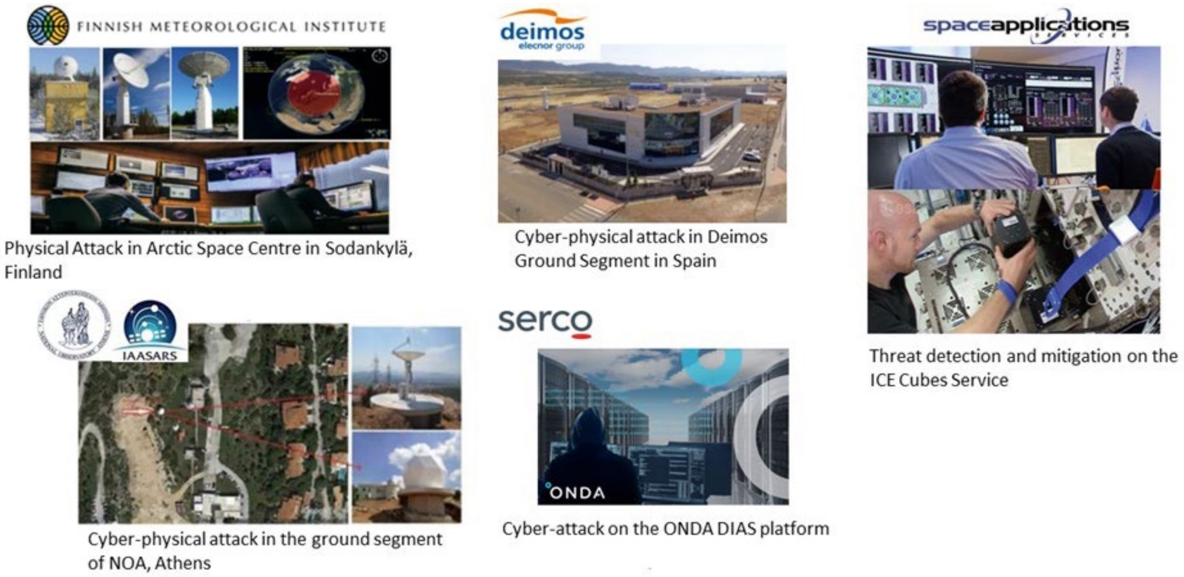
To empower the *responsiveness and social awareness*, a set of innovative technologies will be tailored into the 7SHIELD framework aiming to tackle effectively C/P attacks including the tools to identify and analyse social media posts and create template of emergency messages for engaging citizens and other stakeholders, as well as neutralisation methods of the intruding UAVs. Besides pre-crisis and crisis services, in this layer there are also *post-crisis services* that provide a concrete support to the appropriate actions to mitigate the consequences of physical and cyber-attacks. The *Emergency*

Response Plans from C/P attacks and *service/business continuity scenarios* for each pilot site are capable to analyse GSSS peculiarities and potential exposures to C/P attacks.

The above technologies and tools will be integrated in a harmonized way in the *7SHIELD Command Control and Coordination System (C3)* which provides an advanced Physical Security Information Management System and Interactive User Interfaces especially suited to support operators of the Ground Segments of Space Systems.

The 7SHIELD project has been planned to be evaluated by five use case pilots (PUCs) as shown in Figure 40, and are as follows:

- PUC1 - Physical Attack in Arctic Space Centre in Sodankylä, Finland
- PUC2 - Cyber-physical attack in Deimos Ground Segment in Spain
- PUC3 - Cyber-physical attack in the ground segment of NOA, Athens
- PUC4 - Threat detection and mitigation on the ICE Cubes Service
- PUC5 – Cyber-attack on the ONDA DIAS platform



Physical Attack in Arctic Space Centre in Sodankylä, Finland

Cyber-physical attack in Deimos Ground Segment in Spain

Threat detection and mitigation on the ICE Cubes Service

Cyber-physical attack in the ground segment of NOA, Athens

Cyber-attack on the ONDA DIAS platform

Figure 40 - Pilot Use Cases of the 7SHIELD project

So far, the four operational tests in ONDA-DIAS (Italy), in ICE Cubes Services (Belgium), in NOA (Greece) and DEIMOS (Spain) Ground Segments were carried out. During these evaluation cycles, the 7SHIELD tools were gradually integrated and tested over different scenarios and countries aiming to identify gaps or issues that should be improved for the next releases of the system. After the release of the final 7SHIELD framework, three (3) demonstration scenarios will be realised in NOA, FMI and SPACEAPPs premises.

6. Panel and Round Tables Discussions

Panel title: Cybersecurity and the NIS2 Directive: regulatory aspects and sectoral perspectives
Panel by KU Leuven CiTiP researchers involved in SAFECARE/ ENSURESEC/ PRAETORIAN: Maria Avramidou, Elisabetta Biasin, Erik Kamenjašević, Eyup Kun, Maja Nišević.

Moderator: Erik Kamenjašević

6.1 Introduction

The year 2022 is significant for the EU agenda on cybersecurity since EU policymakers will most probably adopt new legislation in the second half of the year. With a particular focus on cybersecurity in the context of e-commerce, airports, ports and medical devices, this contribution aims to provide an overview of several key forthcoming regulatory challenges based on the research conducted in the context of the ENSURESEC, PRAETORIAN and SAFECARE projects.

In brief, instead of the current identification of individual operators at a national level under the NIS Directive, the NIS2 Directive proposal introduces a size-cap rule to cover, within the selected sectors, all medium and large enterprises as defined under EU law. At the same time, it leaves flexibility for the Member States to identify smaller entities with a high-security risk profile. Moreover, the NIS2 Directive proposal no longer distinguishes between operators of essential services and digital service providers but instead classifies entities between essential and important categories. Additionally, the NIS2 Directive proposal broadens the extra-territorial effect, i.e., selected providers of digital infrastructure or digital services which do not have an establishment in the European Union, but offer services in the EU, will also fall under the scope of the NIS2 Directive proposal. At the same time, it provides for higher penalties and EU Member States would be required to provide for administrative fines up to at least EUR10 million or 2% of the total worldwide turnover.

6.2 E-commerce: Eyup Kun (ENSURESEC): Evolution of the Cybersecurity Responsibilities: From NIS-to-NIS Directive 2 and its impact on E-commerce

Online marketplaces constitute an important part of the e-commerce from NIS to the proposed NIS2 Directive. Online marketplaces are considered digital service providers (DSPs) according to Annex III of the NIS Directive. The evolution of cybersecurity responsibilities of online marketplaces from the NIS Directive to the proposed NIS2 Directive has four main dimensions: change in the harmonization level, change in the scope of risk management and notification requirements, and additional responsibility of managerial bodies for the cybersecurity and possibility of information-information sharing.

Change in the harmonization level: As opposed to the operators of essential services, the responsibilities imposed upon online marketplaces are subject to maximum harmonization at the EU level, according to Article 16(10) of the NIS Directive. Thus, the Member States cannot impose further cybersecurity responsibility upon digital service providers, including online marketplaces. In contrast, the proposed NIS 2 Directive considers the online marketplaces as digital providers as the subset of the important entities. No maximum harmonization is foreseen for important entities' responsibilities, including online marketplaces, in the proposed NIS2 Directive. It means that they can be subject to further cybersecurity responsibilities under national law under Article 3 of the proposed NIS2 Directive.

Change in the scope of risk management and notification requirements: Article 16 of the NIS Directive stipulates the general legal framework of the responsibilities of digital service providers (DSPs). These responsibilities are mainly risk management responsibilities and notification requirements which can be criticized for their uncertainty and vagueness [Kun 2021]. Per Article 16(8), the EU Commission adopted Implementing Regulation (EU/2018/151) to provide further clarity regarding both risk management responsibilities and notification requirements for these responsibilities of DSPs., Thus, the DSPs, including online marketplaces, shall take this Implementing Regulation into account in compliance with Article 16 of the NIS Directive.

Concerning the evolution of responsibilities, the proposed NIS2 Directive retains similar responsibilities of risk management (Article 18 of the NIS2 Directive proposal) and reporting obligations (Article 20 of the proposed NIS 2 Directive). However, the scope of the requirement differs in particular regarding the reporting obligation (three different reporting: initial reporting within 24 hours after the awareness of the incident, intermediary reporting, and final reporting within one month).

The additional responsibility of managerial bodies: In addition to the retained framework, Article 17(1) of the proposed NIS2 Directive brings the responsibility to the management bodies of essential and important entities to approve cybersecurity risk management measures and be accountable for non-compliance. Furthermore, Article 17(2) stipulates that the management bodies shall follow the training regarding cybersecurity to gain sufficient knowledge and practices regarding cybersecurity risk management responsibilities.

Information-sharing arrangements: Another novelty of the proposed NIS2 Directive is to provide the framework for the Member States to incentivize information-sharing among the important and essential entities. According to Article 26 of the proposed NIS2 Directive, Member States shall ensure that important and essential entities might share relevant cybersecurity information among themselves, which respects the EU law.

The impact on the e-commerce sector: the online marketplaces continue to be considered digital providers as a subset of important entities. The additional responsibility of managerial bodies of online marketplaces can contribute to the overall cybersecurity of the e-commerce sector as managerial bodies are directly involved in cybersecurity. Furthermore, the Member States might impose further cybersecurity responsibilities on these marketplaces since the proposed NIS2 Directive foresees the minimum harmonization for important entities, including online marketplaces. Thus, online marketplaces should follow these developments.

6.3 Airports and ports: Maria Avramidou and Maja Nišević (PRAETORIAN): The Cybersecurity of airports and ports under the proposed NIS2 and CER Directives.

The NIS2 Directive proposal, similarly to the NIS Directive, classifies **transport services** including air carriers, airport managing bodies, traffic management control operators, inland sea and coastal passenger and freight water transport companies, managing bodies of ports and operators of vessel traffic services as essential entities. Therefore, these entities are subjected to a number of obligations in order to enhance their cybersecurity and resilience.

In light of the obligations enshrined in the NIS2 Directive proposal, some challenges arise for its implementation in the airports' and ports' context. Precisely, the NIS2 Directive proposal obliges essential entities to adopt cybersecurity risk measures and notify incidents or significant cyber threats. In this respect, Article 2(6) of the NIS2 Directive proposal prescribes that when it comes to the adoption of cybersecurity risk measures and the incident or significant threat notification provisions of sector-specific acts of Union law. These sector-specific provisions will apply instead of the provisions of the NIS2 Directive proposal as long as the requirements set in that sector-specific legislation are "**at least equivalent" in effect to the obligations laid down in the NIS2 Directive proposal**. However, there is some unclarity in the element of "at least equivalent", which could be misconceived as it leaves room for interpretation regarding the determination of equivalent requirements from other sectoral legislation. Moreover, it remains **unclear** how the **medium and large companies size-cap** for entities subjected to the NIS2 Directive proposal will be **translated into airports' and ports' managing bodies context** [ESPO 2021]. **Uncertain remains also the basis** that the Member States should use **to designate** certain airport and port managing bodies as **essential or as smaller entities with a high-security risk profile.** To tackle these challenges, we suggest that guidelines should be issued, clarifying the element of "at least equivalent" and the basis to define which ports or airports in a given Member State should be designated as essential entities or as smaller entities with a high-security risk profile.

It is worth noting that alongside the NIS2 Directive proposal, the European Commission proposed the Directive on the resilience of critical entities, also known as CER Directive proposal. The simultaneous proposal aims to ensure full coherence on the Critical Infrastructures protection both against physical and cyber threats, and to guarantee that cyber-resilience obligations under the NIS2 Directive proposal will also apply to critical entities, including airports and ports, identified under the CER Directive proposal.

6.4 Medical Devices: The impacts of the NIS2 Directive proposal on medical device manufacturers and the challenges concerning incident reporting/notification

Compared to the previous NIS Directive, the NIS2 Directive proposal **expanded its scope of application for the healthcare sector** [Biasin 2021, Biasin 2022]. The NIS2 Directive proposal added new types of entities by including medical devices. Notably, Annex II of the NIS2 Directive proposal considers medical devices and in vitro diagnostic medical devices' manufacturers as **important entities**. EU reference laboratories, entities carrying out R&D activities of medicinal products, entities manufacturing basic pharmaceutical products and preparations manufacturers of medical devices considered critical during a public health emergency are enlisted as **essential entities**.

The NIS2 Directive proposal, therefore, entails **new requirements for medical device manufacturers**. For example, the Member States shall ensure that essential and important entities adopt cybersecurity risk management measures, such as risk analysis and information system security policies; incident handling; business continuity and crisis management; vulnerability handling and disclosure (Article 18, NIS2 Directive proposal). Article 20 of the NIS2 Directive proposal requires the Member States that essential and important entities shall notify, without undue delay, of any **incident** having a significant impact on the provision of their services.

Nevertheless, while these requirements add new layers that are certainly **helpful for enhancing the cybersecurity of network and information systems in the healthcare sector**, some regulatory challenges may arise. As the research by Biasin & Kamenjašević [Biasin 2022] suggests, there could be regulatory uncertainty concerning the NIS2 Directive proposal incident notification requirements **due to potential overlap with the Medical Device Regulations (MDR)** requirements on the serious incident notification. In other words, it is not clear whether, once a cyber incident occurs to a medical device, the NIS2 Directive or the MDR would apply or both simultaneously.

To mitigate this challenge, it is desirable to explain the meaning of '**at least equivalent**' in the NIS2 Directive proposal in more detail. Furthermore, it is important that the NIS2 Directive or following guidance indicates more specifically whether or when the MDR should apply or prevail in case of a security incident to a medical device [Biasin 2022].

6.5 Conclusion

The NIS2 Directive proposal introduced an array of **changes**, also impacting the e-commerce, the airports and port, and medical device sectors. The panel illustrated the changes in the harmonization level of the Directive, the new scope of risk management, the additional responsibility of managerial bodies and information sharing agreements. At the same time, some elements of the NIS2 Directive proposal may entail **legal challenges**. We argued that the level of specification of risk management responsibilities in the new Directive and its implementing regulation remains vague. Further, we underscored the challenges of incident notification requirements (regarding port and airport security and medical device). The formulation of how the NIS2 Directive should interact with sector-specific legislation may lead to regulatory uncertainty (see the notion of 'at least equivalent'). Finally, the panel found that issues may remain for companies' size-cap for entities due to the unclear formulation of the NIS2 Directive proposal.

In conclusion, the NIS2 Directive proposal has set new and additional requirements that may be **beneficial for maintaining a high level of cybersecurity** for many operators in the EU. However, some remaining challenges may bring regulatory uncertainty for many stakeholders, such as those in the e-commerce, port and airport, and medical device sectors.

7. Thematic Presentations

7.1 Ethical and legal aspects of cybersecurity

By Dimitra Stefanatou (Arthur van der Wees), Arthur's Legal B.V

7.1.1 Abstract

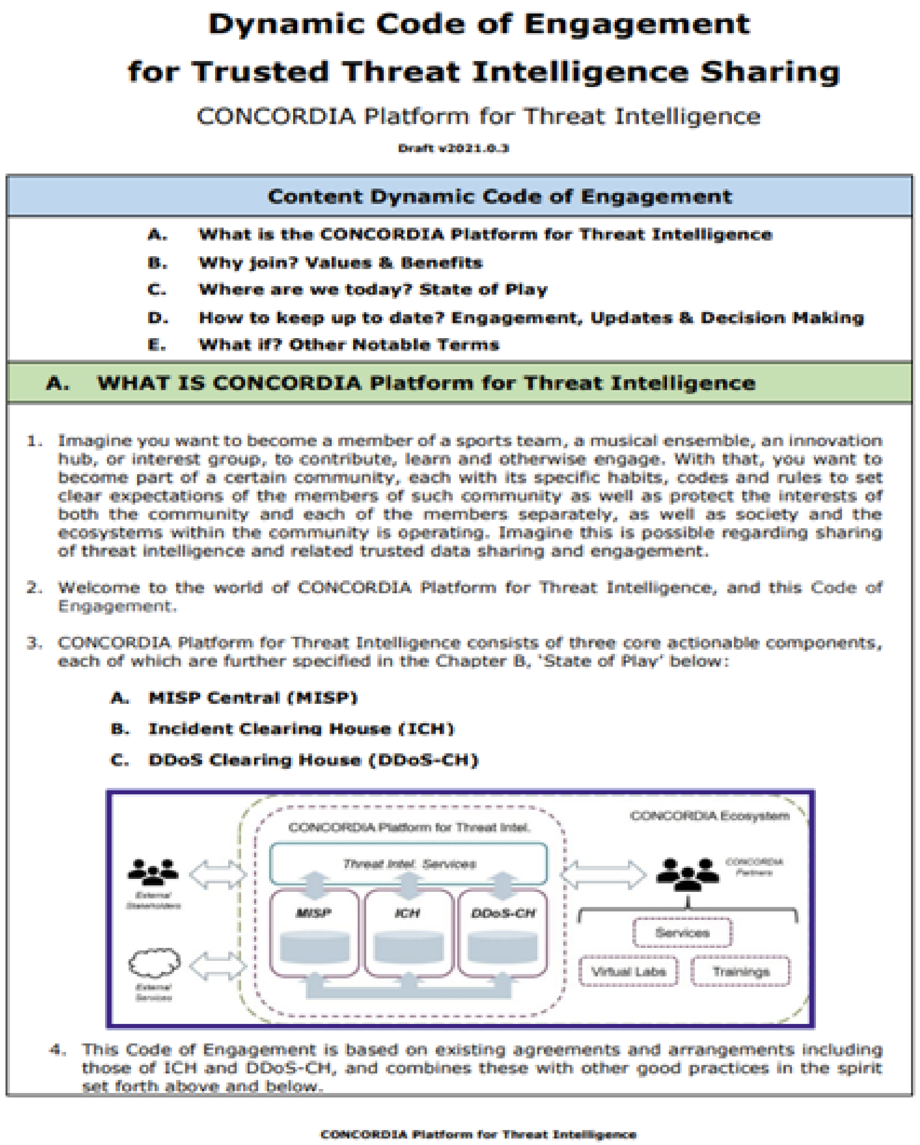
Building and maintaining security in cyber-physical systems, which increasingly often involve Internet-of-Things infrastructure and automation, requires legal governance that considers in an appropriate manner the respective particularities. To effectively govern such systems and develop solutions to mitigate the risks and potential harms, it is important to take a holistic approach that embraces both law and ethics. In the context of critical infrastructure, the legal domain may provide for instruments that can contribute to the real protection of the rights and interests involved, while the domain of ethics may further contribute to the effectiveness of the applicable law. In this respect and in order to foster data sharing and cooperation on threat intelligence, an instrument, namely a Code of Engagement for Threat Intelligence Sharing, based on both law and ethics, could offer guidance for multi-stakeholder cooperation by focusing on the principles of trust and transparency. Further, the IoT risks models could enable stakeholders to systemise and gain awareness of potential risks in hyperconnected environments. By providing tools for multi-dimensional risk-mapping, the Code of Engagement for Threat Intelligence Sharing could facilitate the implementation of future-proof solutions to protect systems against threats.

7.1.2 The complementing instruments of the Rule of Law

From a legal viewpoint, key questions with respect to the protection of critical infrastructure involve, among other, 'how are decisions made when it comes to incident reporting?' and 'what are appropriate measures to implement when facing cybersecurity issues?'. These questions illustrate that the Rule of Law does not only provide for law and regulations but also for standards and certificates, official policies, case law, self-regulatory instruments such as s code of engagement, risk allocation and assurance. Note that cybersecurity is a 'horizontal', a reoccurring theme among different types of EU legal and policy instruments. There is a significant overlap between the legal and ethical aspects of cybersecurity, which evolves for a large part around issues related to accountability. In light of the above, the discussion below elaborates on self-regulatory legal instruments and risk allocation models as supplementary legal tools for governing cybersecurity issues and proposes a set of ready-to-use instruments and tools for critical infrastructure protection in cyber-physical systems.

7.1.3 Code of Engagement for Threat Intelligence Sharing

In the context of Horizon2020 project CONCORDIA [CORDIS, CONCORDIA] which aims to build, among others, a competence network that fosters the EU's digital sovereignty, a group of experts developed an instrument for Threat Intelligence Sharing. This instrument called the 'Code of Engagement' sets forth certain principles and rules adhering parties will have to agree upon. The 'Code of Engagement' provides the conditions for trusted data sharing, digital engagement, communication of good practices and multi-stakeholder cooperation on threat intelligence issues (Figure 41). Overall, the Code of Engagement is designed to facilitate oversight, insight, expectations, and trust, while serving as a tool to arrange stakeholder relationships and dataflows.



Dynamic Code of Engagement
for Trusted Threat Intelligence Sharing

CONCORDIA Platform for Threat Intelligence

Draft v2021.0.3

Content Dynamic Code of Engagement

- **A. What is the CONCORDIA Platform for Threat Intelligence**
- **B. Why join? Values & Benefits**
- **C. Where are we today? State of Play**
- **D. How to keep up to date? Engagement, Updates & Decision Making**
- **E. What if? Other Notable Terms**

A. WHAT IS CONCORDIA Platform for Threat Intelligence

1. Imagine you want to become a member of a sports team, a musical ensemble, an innovation hub, or interest group, to contribute, learn and otherwise engage. With that, you want to become part of a certain community, each with its specific habits, codes and rules to set clear expectations of the members of such community as well as protect the interests of both the community and each of the members separately, as well as society and the ecosystems within the community is operating. Imagine this is possible regarding sharing of threat intelligence and related trusted data sharing and engagement.

2. Welcome to the world of CONCORDIA Platform for Threat Intelligence, and this Code of Engagement.

3. CONCORDIA Platform for Threat Intelligence consists of three core actionable components, each of which are further specified in the Chapter B, 'State of Play' below:

   A. MISP Central (MISP)

   B. Incident Clearing House (ICH)

   C. DDoS Clearing House (DDoS-CH)

4. This Code of Engagement is based on existing agreements and arrangements including those of ICH and DDoS-CH, and combines these with other good practices in the spirit set forth above and below.

CONCORDIA Platform for Threat Intelligence

Figure 41 - CONCORDIA Platform for Threat Intelligence

In Figure 41, the technical platform architecture consists of 3 elements: MISP, Incident Clearing House (ICH) and DDoS Clearing House (DDoS-CH) (under 3). MISP is the main gateway, that collects information on malware, vulnerabilities, target attacks etcetera. ICS shares information on vulnerable and compromised systems with resources owners. So-called 'DDoS fingerprints', descriptions of characteristics of the DDoS attacks. are collected in the DDoS-CH [CONCORDIA 2018].

7.1.4 IoT risks models for Critical Infrastructure Protection

In most of the already applicable and forthcoming regulations, the EU Regulator chooses to take a risk-based approach, where the risks that can potentially occur are taken as a starting point. This approach was taken, in combination with digital data, in the highly influential General Data Protection Regulation [EU 2016] (GDPR) published in 2016. The GDPR dictates, for instance, the implementation of the appropriate technical and organizational measures based on the occurring risk pertinent to specific processing operations. The NIS2 Directive [NIS2 2016], agreed upon in Spring 2022, and the currently proposed Artificial Intelligence Act [AI Act 2021], take a more radical risk-based approach, and are mostly principle-led.

In general, risk depends on the (a) probability of occurrence or event, (b) the level of adverse impact, and (c) the context. In principle, risk-based approaches recognise the complexity of modern-day cyber-physical systems and the importance of accountability. However, there remains some uncertainty around how to define and address risk in these connected environments. Key considerations are the notions that there are many different types of risks, with different impacts, that each require different mitigation measures.

Critical infrastructures increasingly often consist of connected electronic devices. For example, connected devices can be found in healthcare, electricity grids, financial services and government facilities. In contexts where multiple different machines are collecting, processing and exchanging data, and bringing about changes in the environments, defining risks can be complex, and holding someone accountable for the risks will be even more challenging. Such contexts are often called Internet-of-Things (IoT), a term used for connected systems that facilitate the continuous exchange of various sets of data. This can involve personal data including special categories of personal data that require a higher level of protection such as health data, as well as large amounts of metadata that allow for accurate user profiling. Therefore, addressing security risks in this context is highly relevant.

Arthur's Legal, SGS and AIOTI developed a Device-Centric IoT Security Risk Mapping Tool, that allows relevant stakeholders to capture risk systematically and holistically in highly complex and layers IoT infrastructure environments. This tool is specifically designed for manufacturers, customers, procurement departments and policy makers and authorities. The mapping tool consists of four components:

1. Device-Centric IoT Security Risk Spectra (Figure 42)
2. How to Use Guide (7 steps protocol)
3. Risk Level Definitions
4. IoT Security Mapping Table

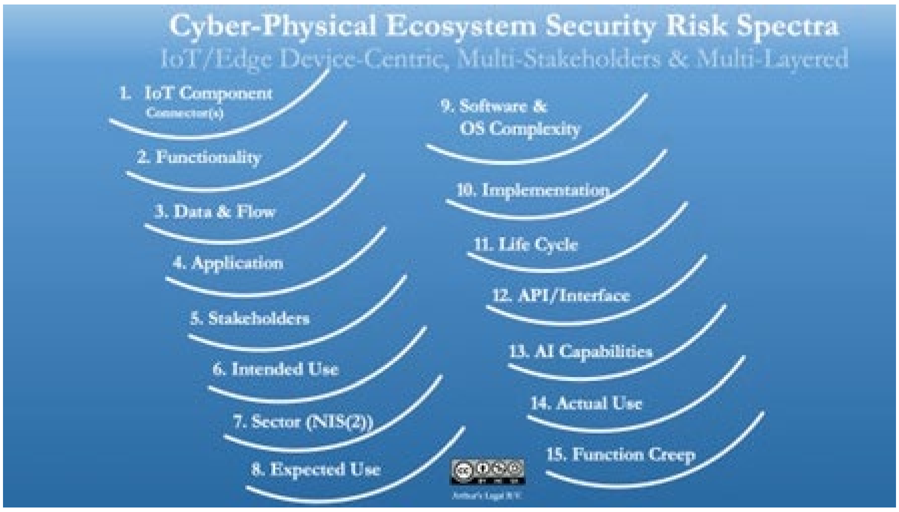


Figure 42 - Overview of different layers of risks that can occur in cyber-physical systems

Systematically monitoring each of the dimensions listed in Figure 42, will allow relevant stakeholder groups to anticipate risks that can occur throughout the full lifecycle of cyber-physical systems. Further, it captures different elements of these systems, including hardware, software, firmware, data flows, user interfaces, etcetera, and implements feedback loops with recognition that systems are subject to continuous change.

7.1.5 Conclusion

The legal and ethical domains provide for complementing instruments that can serve, also, from a strategic point of view, as effective tools to prevent and address cybersecurity issues. As our critical infrastructure becomes ever more hyperconnected, it is of paramount importance to acknowledge that for managing cyber-physical systems and anticipating risks taking measures beyond mere compliance towards accountability is essential. Embracing ethical approaches, multidisciplinary cooperation and careful risk assessment is, thus, critical to protect human rights and vital societal interests in the digital age.

7.2 Combating Hybrid Threats to Critical Infrastructures

Innovations to counter hybrid threats by Souzanna Sofou, Satways (EU-HYBNET) Sofou, Souzanna (Satways Ltd), Pickl, Stefan and Pham, Son (COMTESSA Competence Center, Bundeswehr University Munich), Marina Alonso (JRC), Aggelos Aggelis, Leonidas Perlepes, Antonis Kostaridis, Dimitris Diagourtas (Satways Ltd.)

7.2.1 Abstract on the EU-Hybnet projects' main objectives

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties [EU 2016]. The EU-Hybnet project brings together pan-European practitioners and stakeholders to identify the challenges in countering hybrid threats. Thorough research activities are conducted for the identification of innovations to counter hybrid threats, and training events are organised to test innovations and proceed with recommendations for their uptake, industrialization, and standardization. The project results are shared with EU practitioners and policymakers, which has a positive influence on the public procurement process.

This paper focuses on the main results of EU-Hybnet Work Package (WP) 3, which aims in monitoring and selecting innovative solutions that can be utilised to counter hybrid threats, based on the priorities identified for the latter in WP2 (Gaps & Needs of European Actors). The gaps and needs and the innovations mapped to them, are presented according to the EU-Hybnet project four core themes: future trends of hybrid threats; cyber and future technologies; resilient civilians, local level and administration; and information and strategic communications. For each of the project core theme, three primary contexts were studied, and innovations and solutions were suggested for each of the twelve cases. Figure 43 summarizes the main outcomes derived from the study. In this paper, emphasis is given to innovations proposed to counter Hybrid threats related to Critical Infrastructures.

CORE THEME	**PRIMARY CONTEXT**	**IDEA/ INNOVATION PROPOSED**
1. FUTURE TRENDS OF HYBRID THREATS	1.1 Trend: Official strategic communication losing power	Guides to identify fakes
		Hybrid online dilemma game
	1.2 Trend: Big data as a new power source	Countering disinformation with strategic personalized advertising

		Automated detection of hate speech in social media
	1.3 Trend: increasing strategic dependency of critical services	A blockchain-based real-time information management and monitoring system
		A crawler and real-time search engine for investors
2. CYBER AND FUTURE TECHNOLOGIES	2.1 GAME CHANGERS: QUANTUM AS A DISRUPTIVE TECHNOLOGY	Open European Quantum Key Distribution Testbed
		Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
	2.2 HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER	Efficient cyber threat information sharing through Hyper Connectivity networks
		Cross sector cyber threat information sharing
		Public-private information-sharing groups developing collaborative investigations and collective action
	2.3 THE INDIVIDUAL AS A DIGITAL ENTITY	Fake news exposer
		Factcheckers communities
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1 DISTRUST AND STRESS IN POLITICAL DECISION-MAKING	Resilient democracy infrastructure platform
	3.2 RELIANCE ON CRITICAL SERVICES & TECHN. SYSTEMS	Early or Rapid Damage Assessment System
		Smart message routing and notification service
	3.3 GLOBALIZATION VS. LOCALISATION	Tool that monitors and detects the population's response to the information being published
4.INFORMATION AND STRATEGIC COMM	4.1 GOING VIRAL	Journalism trust initiative
		Debunking of Fake News
		Non-partisan native-language news channels for most interdependent abroad regions

UNICA TIONS	4.2 DIGITAL MONOPOLIES & MASSIFICATION OF DATA	Fair Trade Data Program
	4.3 DETERIORATION OF THE QUALITY OF CONTENT	Training application for media literacy
		Automated fact-checker

Figure 43 - Ideas and Innovations proposed to counter Hybrid Threats, EU-Hybnet Deliverable 3.3 [EU-Hybnet 2020]

7.2.2 Innovations to counter Hybrid Threats: Critical Infrastructures

With respect to the increasing strategic dependency that governments have on critical services (See Figure 43, Primary Context 1.3.) growing concerns have been raised the past years regarding certain foreign investors' efforts seeking to acquire control of or influence in European firms whose activities have repercussions on critical technologies, infrastructure or sensitive information, thus putting security or public order at risk. The new Regulation (EU) 2019/452 includes an indicative list of factors that Member States and the Commission may take into account when assessing foreign direct investment (FDI) [EU 2019]. The cooperation mechanism established under the EU framework on FDI screening applies from October 2020. As stated in a working paper on the Global FDI network by the International Monetary Fund [IMF 2017], in order to describe a globalized world, where national borders are less relevant, economic statistics also need to adapt: information on the "national economy" needs to be supplemented with information on global interconnectedness.

For that reason, a blockchain-based real-time information management and monitoring system is proposed to verify the origin of the investment and help prevent future critical foreign investments. All entities (companies and governments) would be invited to contribute to these systems by sharing their information, and the latter can be partly anonymized. The investment transactions in the system should be verified based on the blockchain technology. Each member of the system would have two main tasks: sharing the information and verifying the investments based on the system's information. Only verified investments would then be allowed to be executed. Verification can be done by government/EU officials. The system's information should be continuously updated and visualized/monitored, so that any member of the network can easily access important information. In the beginning, the entities (companies, governments) would have to verify the investment transactions manually, but then, when enough data is shared/collected, the system can work (semi-)automatically. A threshold can be defined regarding when the system can automatically verify and when the entities should do it manually.

Additionally, a focused Crawler and a Real-Time Search Engine is proposed to be developed, only for information relevant to the investors, thus providing a quick overview for better evaluation of the latter. The crawler would be a combination of hard code rules model and Machine learning models, which allow the user to retrieve relevant results. This can also help in building a database of investors or detecting connections between them. The database created with the crawler can be used as the input for the idea presented above, the Blockchain-Based Real-Time Information Management and Monitoring System.

Regarding the reliance on critical services and technological systems (See Figure 43, Primary Context 3.2.), advances in technology have undoubtedly elaborated the automation in production units and the supply chain. Reliance on digital means can potentially decrease the resilience of the production units and the supply chain, as the digital world offers an attractive context for hybrid threats. The vital need for an uninterrupted operation of Critical Infrastructures and supply chains was also brought to the surface during the pandemic outbreak, due to the disruption of the global supply chain and the shortage in supplies as a result of closed borders and travel limitations.

Besides the legal and economic framework that will support public private partnerships, practitioners need to be involved in, and remain constantly updated on the protection of Critical Infrastructures and supply chains from cyber and physical events. This will allow practitioners to take appropriate actions and initiate strategically planned processes.

Rapid damage assessment enables operators to assess the expected structural damage in real-time and identify possible expected impacts. The algorithms for an automated rapid damage assessment system can automatize the reaction process during a severe event, i.e., propose automated reaction, optimize response (for example, areas in green can continue to operate, areas in yellow integrity can be assessed automatically, whereas the red areas should be investigated in detail before entering operational mode). A Critical Infrastructure Resilience Platform (CIRP) [Kostaridis 2017] when fed with real time nowcasting or forecasting data instead of a scenario hazard, can be turned into an Early or Rapid damage assessment system, respectively, thus providing the unique capability to initiate efficient response actions, right after (in case of now-cast data) or even before (in case of forecast data) the occurrence of catastrophic events. The solution has been evaluated by a big refinery case in Greece, where the impact of natural hazards (e.g., earthquake) was studied with respect to the resilience of the critical infrastructures (InfraStress H2020 project). Additionally, the same application will be used to study the impact of Natural hazards (earthquakes, extreme winds, floods) on buildings, and more specifically on a ground satellite station (7shield H2020 project). Based on the results, a thorough risk assessment will be conducted. Last but not least, the application has been used for the study of the impact of climate change on CIs (EU-Circle H2020 project).

Further to the Early or Rapid damage assessment system, it is suggested that a smart message routing and notification service is used for sharing the operational picture to every agency involved in the response at every level of coordination, thus enabling collaborative response and the proper alerting of personnel/practitioners/stakeholders. The Emergency Message Content Router (EMCR) developed by SATWAYS, can be used for various use cases, for both natural and man-made disasters. It is capable of sharing the operational picture (information related to the management and response to an emergency situation) by routing messages, among all responding teams involved. The EMCR tool has been used in the case of airports (SATIE H2020 project) in order to enable the communication (exchange of operational picture, collaboration) between airport operators and the public safety agency. The cooperation of the parties involved in cases of natural & man-made disasters is crucial for the ultimate use of resources- both human resources and state of the art technology- and for a fast & efficient response.

7.2.3 Conclusions and Future Work

This work has served to identify solutions for different dimensions of hybrid threats. It should be highlighted that a hybrid threat is considered to be multidimensional and time dependent. Therefore, in order to produce one holistic solution, we should be able to identify a hybrid threat, and then teach a computer how to respond to a multidimensional and time dependent situation. This is not yet easy to implement as patterns are not ready to be described. In the future, Artificial Intelligence tools and quantum technology, especially through Quantum Optimization Techniques, within smart Service Oriented Reachback Processes could be used to identify and respond to such threats in a timely manner. Current work related to proposing Innovations to counter Hybrid threats for CIs focuses on the Exploitation of Critical Infrastructure Weaknesses and Economic Dependencies.

7.2.4 Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054. This article reflects only the authors' views and the Research Executive Agency, and the European Commission are not responsible for any use that may be made of the information it contains.

7.3 Increased automation for detection, prevention and mitigation measures

The Role of OpenC2 in Cybersecurity Automation and Orchestration by Vasileios Mavroeidis, University of Oslo

The time adversaries need to execute cyber-attacks can be measured in seconds or minutes. In contrast, defenders find it challenging to respond effectively and in a timely manner. This asymmetry emanates from the fact that adversaries are well-informed and resourced, methodical, and utilize automation, whereas defenders are challenged by insufficient preparedness, including threat situational awareness, response procedures, and lack of automation.

To put the above into perspective, how you guide a response to a cyber-attack targeting a dam and the time spent accomplishing the mission can be the differentiating factors between a deadly cascading incident that can cost lives or protect your environment (e.g., organization, country, the EU as a whole).

Further, digital infrastructures are getting larger and are becoming more complex, comprising diversified systems and technologies (e.g., IT & OT) that also communicate. To secure their digital infrastructures, defenders rely on multiple tools to perform their operations and are necessitated to cooperate and develop an ecosystem where people, processes, and tools harmonically interact. Automation intersects this ecosystem and connects the pillars above, with the main focus being the automatic handling of security operations-related tasks without or with minimal human intervention. An integral part of this approach is the integration of cybersecurity tools and their orchestration driven by established processes and procedures (i.e., cybersecurity playbooks and workflows).

Integrating different cybersecurity tools requires connecting proprietary interfaces and making customized integrations, a complex and costly course that also requires continuous maintenance. This complexity also has resulted in an increased vendor dependency (vendor lock-in) since vendors capitalize on this challenge and offer unified solutions or more dedicated technology known as security orchestration, automation, and response (SOAR). The strength of a SOAR solution lies in its range of pre-built integrations that speed and ease the deployment of cybersecurity operations playbooks and workflows.

To establish resilient and sustainable cybersecurity operations (defence) ecosystems and in support of automation and orchestration, we need tools that can interoperate out of the box without the need for customized integrations, i.e., a plug-and-play approach to product integration. For instance, when we replace a firewall with another in the ecosystem (see Figure 44), the change should be performed seamlessly "without the need for any reconfiguration".

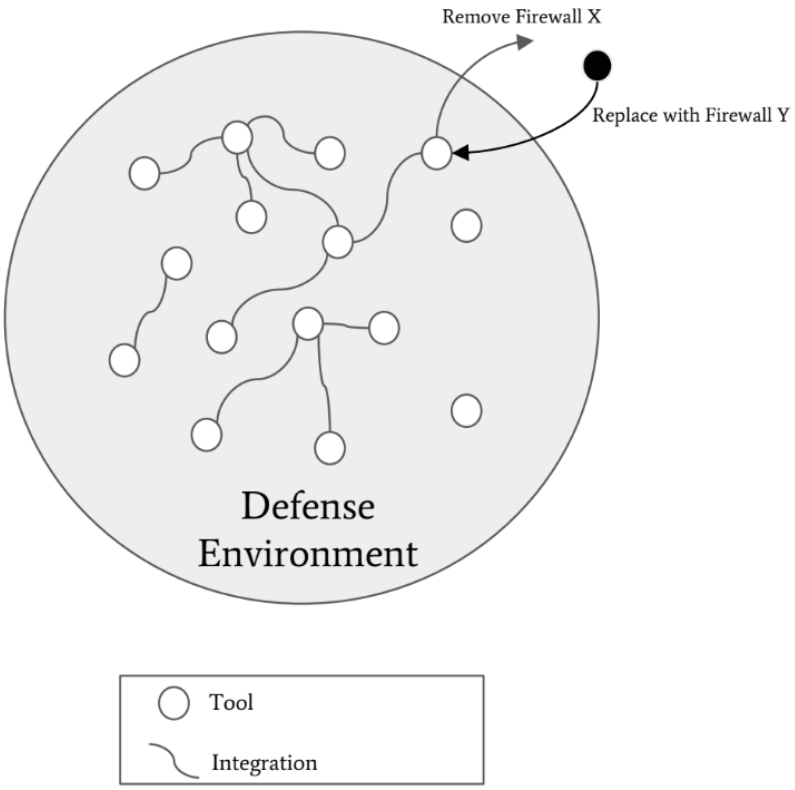


Figure 44 - "Ecosystem" of Cybersecurity Tools: Replacing a Firewall

Achieving this level and type of interoperability across cybersecurity tools requires introducing standardized interfaces for command and control (C2). One technology focusing on this aspect is Open Command and Control (OpenC2) from OASIS [OpenC2]. This ongoing standardization effort creates a vendor- and tool-agnostic C2 language for technologies that provide or support cybersecurity. To achieve this, OpenC2 adopts a function-centric approach. A cybersecurity tool is characterized by the operations it performs and its functions and thus supports particular subsets of the OpenC2 language applicable to the C2 of these functions [Mavroeidis 2020]. For instance, a firewall product would support an OpenC2 interface for "Packet Filtering", i.e., it would implement the "OpenC2 Packet Filtering Actuator Profile".

OpenC2 is defined across a family of specifications:

- The **OpenC2 Architecture Specification** describes the fundamental structures of OpenC2 and provides a blueprint for developing Actuator Profiles and Transfer Specifications.
- The **OpenC2 Language Specification** provides the semantics for the essential elements of the language, the structure for Commands and Responses, and the schema that defines the proper syntax for the language elements that represent the Command or Response.
- **OpenC2 Actuator Profiles** specify the subset of the OpenC2 language relevant in the context of specific actuator functions and often define additional relevant and/or unique elements to that function.
  Note that cyber defence tools are likely to implement multiple profiles based on the functions they perform.

- **OpenC2 Transfer Specifications** utilize existing protocols and standards to implement OpenC2 message transfer in specific environments.

In addition, OpenC2 is designed to be:

- **Technology Agnostic:** The OpenC2 language defines a set of abstract atomic cyber defence actions in a platform- and implementation-agnostic manner.
- **Concise:** A Command is intended to convey only the essential information required to describe the activity to be performed and can be represented in a very compact form for communications-constrained environments.
- **Abstract:** Commands and Responses are defined abstractly and can be encoded and transferred via multiple schemes as dictated by the needs of different implementation environments.
- **Extensible:** While OpenC2 defines a core set of Actions and Targets for cyber defence, the language is expected to evolve with cyber defence technologies and permits extensions to accommodate new cyber defence technologies.

To sum up, effective and efficient cybersecurity operations require establishing a symbiotic function across tools, processes, and people. Cybersecurity automation intersects the above pillars and, via orchestration, enables the (as per need) automatic execution of cybersecurity processes. In this regard, the underlying challenge is the complexity of architecting, deploying, and maintaining such environments due to the need for customized integrations and their dependence on proprietary interfaces. In response to this challenge, OASIS OpenC2 is a standardization work that introduces an interoperable, function-centric, vendor- and tool-agnostic machine-readable language for the command and control of cybersecurity tools.

Acknowledgments

This work was supported by the Norwegian R&I company Cyentific AS; the JCOP project, funded by the European Health and Digital Executive Agency under agreement number INEA/CEF/ICT/A2020/2373266; and PHOENI2X, funded by the European Union's Horizon Europe Programme under agreement number 101070586.

7.4 Information sharing techniques, rules, and repository to exchange knowledge

Decentralized Identities and the role of this technology in CI protection and information sharing by Michele Nati, IOTA

In the e-commerce infrastructure, in order to guarantee the integrity of data shared in the e-commerce ecosystem and to control access to it by authorized parties, an Identity and access management system is needed. To guarantee user-centricity a decentralized identity tool can be used. This is made more important in light of the system of systems nature characterizing e-commerce. Conversely, using an off-the-shelf IdM/IAM will only satisfy the need for a close consortium and not of an open one, where new systems can be added in a trusted way to share critical information in the e-commerce monitoring infrastructure. Moreover, a single centralized IdM will both add the complexity of integration, and a single point of failure. For this Decentralized Identities tool will increase the trust and security of critical infrastructure information sharing.

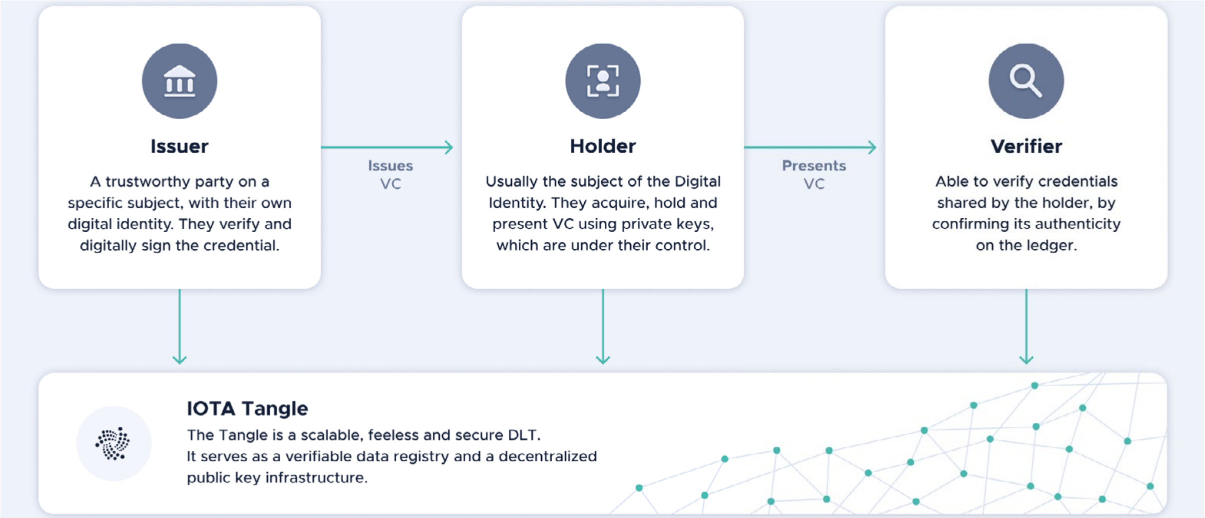

Issuer
A trustworthy party on a specific subject, with their own digital identity. They verify and digitally sign the credential.
Issues VC
Holder
Usually the subject of the Digital Identity. They acquire, hold and present VC using private keys, which are under their control.
Presents VC
Verifier
Able to verify credentials shared by the holder, by confirming its authenticity on the ledger.
IOTA Tangle
The Tangle is a scalable, feeless and secure DLT.
It serves as a verifiable data registry and a decentralized public key infrastructure.

Figure 45 - IOTA Identity Roles

The ENSURESEC project explored the impact of decentralized identities in the e-commerce infrastructure.

What are decentralized identities and how do they work?

In order to build a decentralized Identity tool for the ENSURESEC project we used the IOTA Identities. IOTA Identity provides a standardized framework for integrating decentralized digital identity. In a decentralized identity ecosystem, the following roles are identified:

1. *Holders:* Holders are the owners of digital identities. They have ultimate control over their data and choose how much and with whom they share their data with.
2. *Issuers:* Issuers are trusted third parties or authorities that generate and issue credentials to holders, such as health records or identity documents.
3. *Verifiers:* Verifiers are any third parties that need to verify the authenticity of a holder's data. A verifier might, for example, need to validate that the holder owns a driving license or is above eighteen years of age.

Decentralized identities use the ledger immutability to generate Decentralized Identifiers. Such identifiers serve as a reference to a DID Document stored on the tangle. This document contains data such as public keys, enabling the holder to prove ownership over their identifier and personal data. This is possible because keys are unique, and the private key is secretly stored by the owner. In addition, DID documents can be seen as a folder that references Verifiable Credentials (VCs). Verifiable Credentials are claims about the holder. They can be verified online or in person, and the holder decides who to share them with. Examples of VC’s are driving license, university degree etc., such credentials can be attached to the unique decentralized identifier. The claims of verifiable credentials are not stored on the Tangle, only identifiers needed to verify the credentials are stored on the Tangle. In this case, a verifiable credential can even contain personal information without violating the GDPR compliance.

Two use cases where a Decentralized Identities tool can be employed in the e-commerce domain are described below.

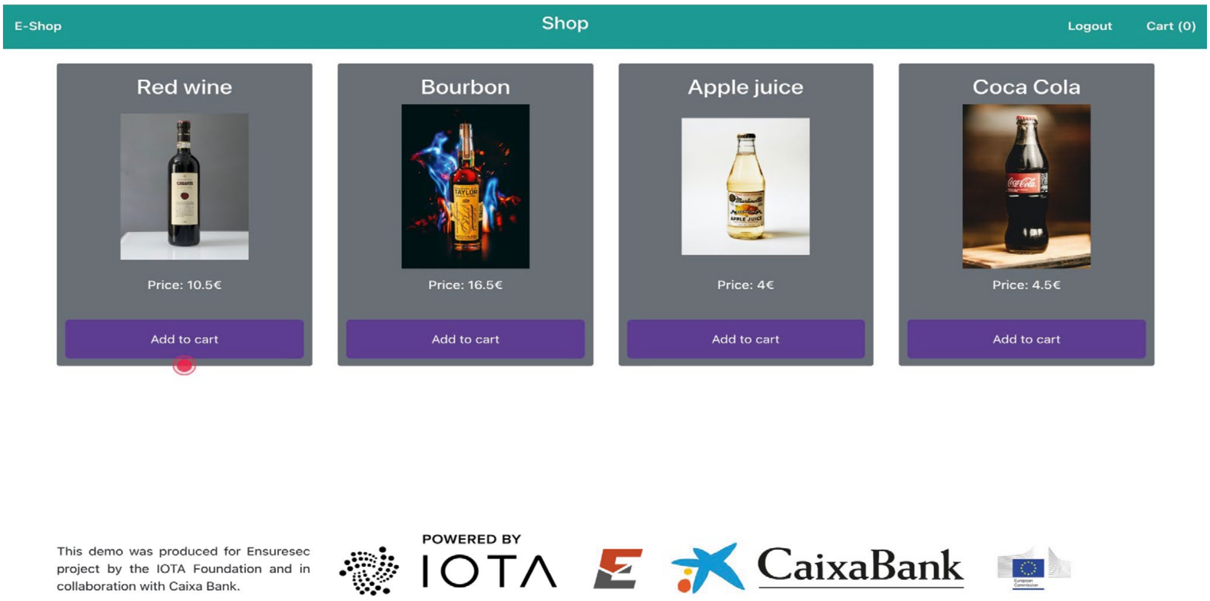
7.4.1 Tools verification and authorization

A tool owner belonging to Company X wants to register the identity of its tool so that any party can verify the source of information shared using the Audit Trail and trace it back to a tool belonging to Company X and prevent impersonation and man-in-the middle attacks. For this, Company X registers a company identity. An authorized Company X employee then registers an identity for each of the company tools. The tool signs each message shared using the Audit Trail using the tool identity. The same process can be repeated for Company Y and its tools. Company Y tools can verify the source of information generated by Company X tools by verifying the signature of messages generated by the given Company X tool. Company X tool creating the given Audit Trail log can authorize access to tools belonging to Company Y by simply verifying the identity of such tools and this is derived from the identity of Company Y.

7.4.2 Customer identity and credential (age) verification

Problem: Verify customer identity and avoid collecting and storing personal information; increasing compliance and reducing liability for e-commerce and small sellers. In the context of ENSURESEC e-commerce ecosystem, the proposed use case will make use of the Decentralized Identities tool to implement the following workflow:

- An authorized bank employee registers an organization decentralized identity (DID) for its bank;
- A customer creates a decentralized identity (DID) using a mobile application (a standalone credential wallet or an e-commerce shopping app);
- The customer requests an issuer (e.g., the bank) to issue a credential staying her age;
- The issuer uses information about the user held on local record (and previously verified) and the Decentralized Identities tool to create and issue a Verifiable Credential to the customer;
- The customer (namely Owner) downloads the credential in her app, using a credential wallet;
- The customer purchases an item that requires age verification on an e-commerce site;
- The customer provides her credential to the e-commerce website using the Decentralized Identities tool;
- The e-commerce site uses the Decentralized Identities tool to verify the credential and authorize the purchase.



This demo was produced for Ensuresec project by the IOTA Foundation and in collaboration with Caixa Bank.

Figure 46 - Secure Age Verification in online shopping

A similar scenario can be applied in case of online purchase (Figure 46) of dedicated drugs for specific health conditions. The customer can be issued with a credential from her GP stating her condition.

7.4.3 Decentralized Identities tool implementation

The ENSURESEC Decentralized Identities tool allows users to create Self-Sovereign Identities, linking Decentralized Identifiers (DIDs) to their specifications. DIDs are public/private key pairs and can be created for organizations, individuals and objects. Each identity is represented by a unique public key immutably stored in the ledger (in our case the IOTA Tangle). Identities and public keys are used to anchor off-chain Verifiable Credentials, certificates containing identity attributes and signed by an issuer identity (using its private key).

The issuer itself is an entity with its own decentralized identity. The Bridge allows an identified trust root to verify users' identity. Verified identities can then propagate this verification to other entities (organizations, individuals, objects) using a network of trust approach (see Figure 47).

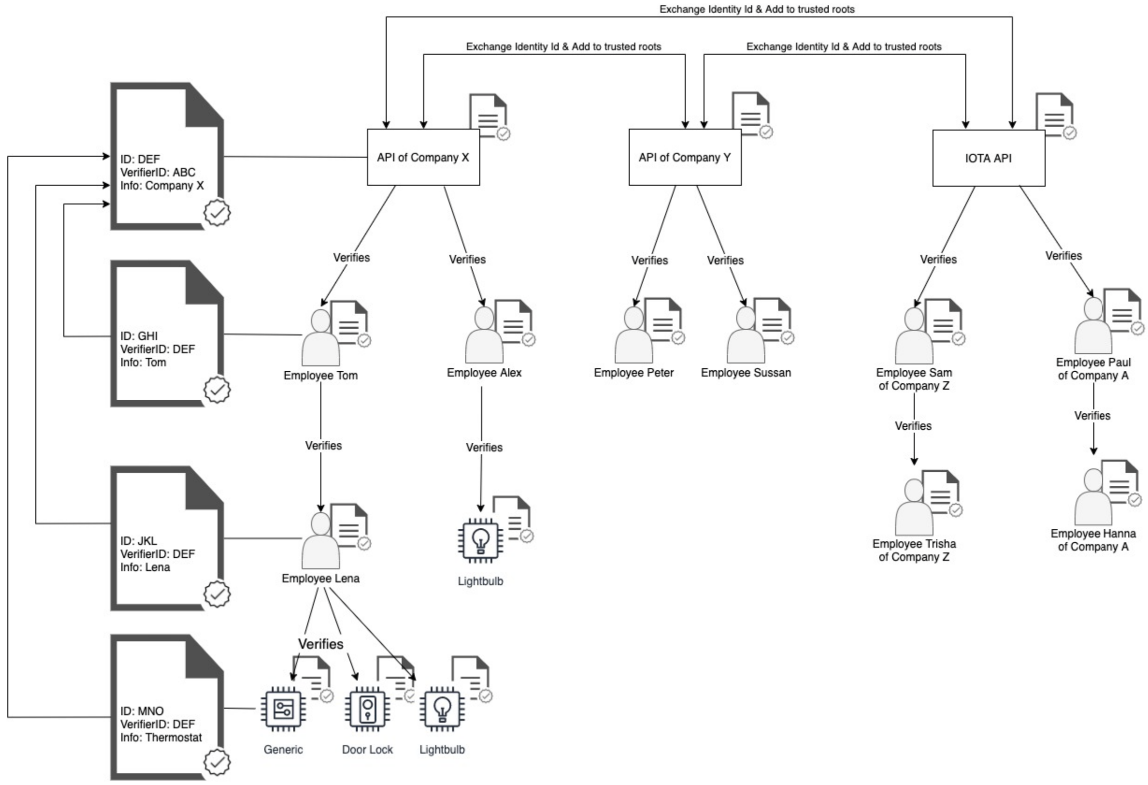


Figure 47 - SSI Bridge Network of Trust [3]

The Bridge also allows issuers to issue Verifiable Credentials for selected identity owners (identified by a decentralized identity) and owners to present them to verifiers. Verifiers can use the Decentralized Identities tool APIs to verify credentials authenticity. This requires verifying that a credential contains the identifier (DID) of the owner presenting it, and it is signed by an authorized Issuer. This requires accessing the information stored in a ledger. The image below shows the interaction between Issuer, owner, verifier and the ledger to manage the lifecycle of decentralized identities and verifiable credentials.

7.4.4 Conclusions: Security and Privacy considerations

The Decentralized Identity tool provides a thin layer of APIs that allow to create and manage decentralized identities and verifiable credentials, based on IOTA Identities libraries.

As a tool to provide decentralized Identity & Access Management for the e-commerce critical infrastructure the Decentralized Identity Service will only manage tools and organizations identities and as such it will not process any personal data. The service is stateless and as such does not require storing any information about an identity or credential state. It has an optional field called claim which can be used to store specific details to the identity, for instance this claim can be used to create a verifiable credential representing the identity. The claim won't be stored on the immutable ledger and will be removed if the identity gets deleted at the service level. However, in case of individuals' identities, credentials are always stored off-chain (by the identity owner) and the ledger is only used for anonymous identifiers (as described previously).

Decentralized Identities offer a secure and privacy preserving way to manage information sharing in the e-commerce ecosystem, to guarantee integrity and auditability of shared data as well as reducing collection of personal data, in particular from small businesses.

For more information can be found in
https://wiki.iota.org/integration-services/explanations/services/SSI-bridge/introduction

7.5 Standards and Regulations for the Protection of Critical Infrastructures

Panel and discussion led by Loredana Mancini (InlecomSystems) standard and policy management for PRECINCT project

Standard and Regulation are an important aspect when speaking of Critical Infrastructure, it is key that in case of design, development, evaluation and above all attacks and problems in this area a common "language" and model to adhere to exists.

This type of alignment is not always easy as national and international standards, in particular outside European countries, can be different and on top of this aspects also language and cultural barriers can slow down the communications and can create problems during the reactions and protection phases.

The standards in CI areas should look at the different needs, examples are in the communication and standard symbols and language, in the set-up and testing phase, in the creation of integrated testing labs and exercises. These actions can be designed and organised according to a specific calendar and thus create a model to be used, checked, and improved.

Another important area is the Subsidiarity aspects that can create strong connections and protection among different CI.

During the session on Standards and Regulations for Protection of Critical Infrastructure different experiences were presented and discussed, looking at this aspect from different perspectives, presenting lessons learned and project outputs and results.

7.5.1 Industrial Cybersecurity Testing Methodology on LSPs

PHOENIX – Industrial Cybersecurity Testing Methodology on LSPs by Ganesh Sauba, DNV

PHOENIX aims at providing a cyber-shield armour to European Electrical Power and Energy Systems (EPES) infrastructure enabling it to detect and survive large-scale, combined, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens in the vicinity and the end-users at a reasonable cost. The effectiveness of the PHOENIX framework is being validated across 5 European Large-Scale Pilots (LSPs) in Italy, Germany, Slovenia, Greece and Romania involving the complete end-to-end generation, transmission, distribution and prosumption value chain. Here an insight is being given on the industrial cybersecurity testing methodology on these LSPs that is currently being undertaken for the PHOENIX project.

Recently a wave of attacks was detected on windfarms and over a short period of a few months the following breaches were catalogued:

1) In November 2021, Vestas in Denmark was partly hit by a ransomware attack and as a result, hackers leaked a substantial amount of stolen personal data.
2) In March 2022, China was accused of long-term hacking on the Indian power grid although not directly related to windfarm as such, it has had profound effects on operational aspects in that country.
3) During the period of March to April 2022, 3 attacks towards different windfarm operators were reported in Germany and all these happened since the Russian invasion of Ukraine.

To prepare against these types of attacks on the LSPs in the PHOENIX project, penetration tests have been planned and is being carried out on these assets. Below is a location map and a short outline of the security aspects to be investigated for each of the LSPs being pentested.

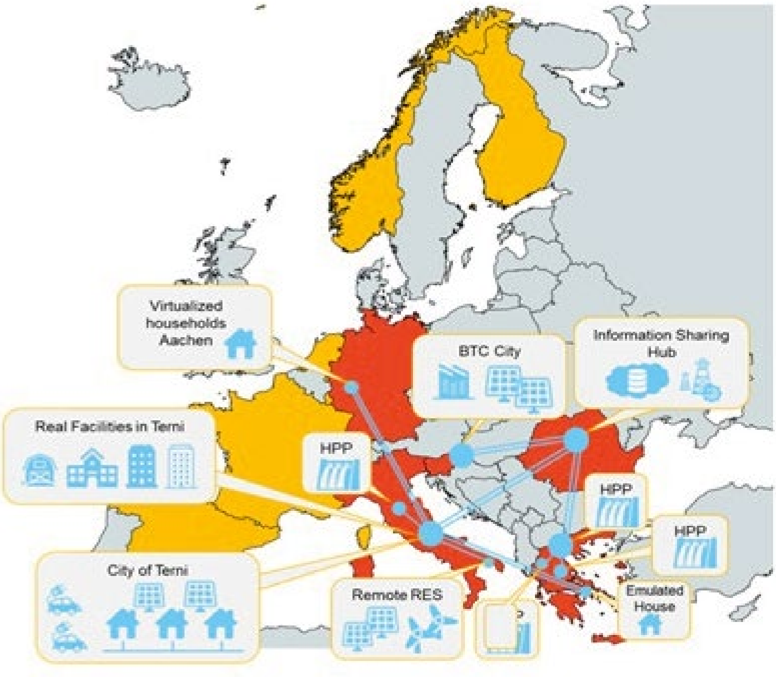


Figure 48 - PHOENIX Large Scale Pilots

LSP1 Multi-utility/Multi-owner RES cyberthreats and data breach detection (Italy)

- Securing MV/LV and generation asset and Preventing data breaches.
- Securing collaboration mechanisms among DSO, RES manager, eMobility and other critical infrastructures.

LSP2 National-wide cooperative remotely controlled HPP (Greece)

- Preventing data breaches.
- Cybersecurity attack scenarios on HPP generation – transfer power grid.

LSP3 Collaborative Microgrid-enabled cyber risks mitigation (Slovenia)

- Cybersecurity attacks on MV/LV EPES assets and AMI.
- Demonstration of on how can the microgrid contribute to the resiliency of the DSO network by utilizing the microgrid energy loads via appropriate power flow rerouting patterns.

LSP4 Collaborative / DSO flexibility vs cybersecurity and privacy (Italy, Germany, Greece)

- Securing sensing infrastructure and control modules.
- Securing Demand Response system.

LSP5 National vs Pan-European cooperative cyber threat information sharing (Romania)

- Hosting I2SP platform to be used by all other PHOENIX LSPs.
- Simulating a standard internet infrastructure of an EPES and getting data from real internet common cyberattacks for Phoenix tools.

The penetration testing work for the PHOENIX LSPs will be based on requirements from the ISA/IEC 62443 standard series and the following topics are being tackled to address standard compliance:

I. Securing Zones & Conduits

- Assessment and analysis of the current network architecture with respect to zones and conduits (IEC 62443-3-2)

II. Evaluation of Security Level targets & capabilities

- Gap analysis towards the requirements in IEC 62443-3-3
- Documentation review and test plan

III. Attestation of Compliance

- Physical testing of each requirement
- Issue Attestation of Compliance to IEC 62443, and to Security Level achieved

The pentest program carried out for the PHOENIX LSP1 site followed the following steps:

- Mapping each attack tree node with applicable DNV security tests
- Main focus on the red line nodes
- Planning our pentest according to test scenarios depicted
- Team discussions on previous experience with the categories in the attack trees.

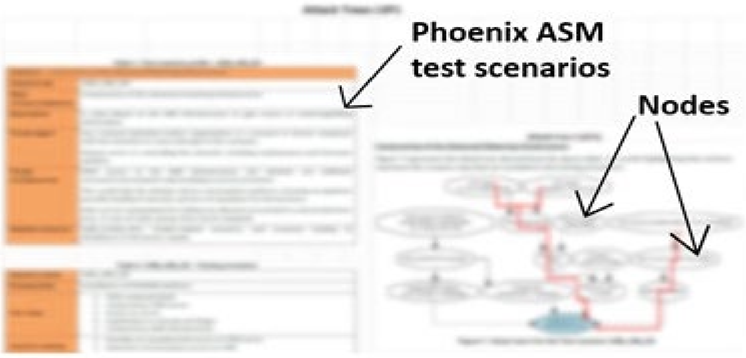


Figure 49 - Example of DNV test program for LSP1

Below are some of the findings form penetration testing work carried out on a windfarm as part of the LSP1 site in Italy:

- Weak physical security of wind turbines; there is no cctv, may be possible for unauthorized personnel to enter turbine with some imagination and connect to the system
- Lack of segmentation between turbines in windfarm; it is possible to reach all turbines from connecting to one, i.e., possible to see traffic, scan network and see each open service and ports, such as FTP, SSH, Telnet, etc.
- SCADA servers are running obsolete Windows XP with critical vulnerabilities that easily can be exploited if attacker somehow can reach it from external or internal network. Thereby impacting the entire windfarm.
- Violation of the principle of least privilege e.g., user on SCADA server is running as Administrator.
- Leaked or default credentials were discovered, especially for the remote IP CCTV monitoring of the windfarm. This may be used to propagate further into the control systems.
- Overall weak password policy into different services

Below are some pictures from the windfarm that was penetration tested.

Primary substation
Hacking SCADA
Turbines are interconnected by fibre-optic cables (no segmentation)

Figure 50 - PHOENIX LSP1 Windfarm Test Site

For further information, please visit: https://phoenix-h2020.eu.

7.5.2 Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released

Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released by CISA and NIST in the United States by Dr. Ilesh Dattani, Assentian

In July 2021 the United States Federal Government published The National Security Memorandum. It establishes a voluntary initiative which is aimed at driving collaboration between the Federal Government and the critical infrastructure community to improve the cybersecurity of control systems. It instructs the Department of Homeland Security (DHS) to lead the development of preliminary cross-sector control system cybersecurity performance goals as well as sector-specific performance goals within one year of the date of the National Security Memorandum. These goals are intended to provide a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety [CISA 2021].

These performance goals are based on a broad spread of standards and good practices produced by both the public and the private sector. This included the following standards [DHSNIST 2021]:

CISA Cyber Essentials (https://www.cisa.gov/cyber-essentials)
CISA Cybersecurity Best Practices for Industrial Control Systems (https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems)
CISA Pipeline Cyber Risk Mitigation Infographic (https://www.cisa.gov/publication/pci-cyber-risk-infographic)
CISA Recommended Practice: Defense in Depth (https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_CONTROL SYSTEM-CERT_Defense_in_Depth_2016_S508C.pdf)
Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards Guidance (https://www.cisa.gov/publication/cfats-rbps-guidance)
NRC Draft Regulatory Guidance (DG)-5061, "Cyber Security Programs for Nuclear Power Reactors." (https://www.nrc.gov/docs/ML1801/ML18016A129.pdf)
NIST SP 800-82, Rev 2, "Guide to Industrial Control Systems (ICS) Security." (https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final)
NISTIR 8183, Rev 1, "Cybersecurity Framework Version 1.1 Manufacturing Profile." (https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final)

This has resulted in a set of nine preliminary performance goals [Johnson 2021]

1. Risk Management and Cybersecurity Governance

GOAL: To Identify and document cybersecurity risks to control systems using established recommended practices (e.g., NIST Cybersecurity Framework, NIST Risk Management Framework, International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443, NIST Special Publication (SP) 800-53, NIST SP 800-30, NIST SP 800-82) and provide dedicated resources to address cybersecurity risk and resiliency through planning, policies, funding, and trained personnel.

RATIONALE: A formal risk management process provides a consistent standard terminology, documents risks, identifies roles and responsibilities, and can be used by management to understand, articulate and manage risks, estimate impacts, and define and plan responses to incidents.

2. Architecture and Design

GOAL: Integrate cybersecurity and resilience into system architecture and design in accordance with established recommended practices for segmentation, zoning, and isolating critical systems (e.g., Industrial Control Systems-Computer Emergency Response Team Defence in Depth guide, Purdue Diagram) and review and update annually to include, as appropriate, any lessons learned from operating experience consistent with industry and federal recommendations.

RATIONALE: Integrating cybersecurity and resilience into system architecture and design is intended to prevent, detect or delay, respond to, and mitigate the consequences of malicious acts or other acts that could compromise cybersecurity. Properly segmenting a network provides increased access control, making it easier to restrict and monitor user access to systems. Network segmentation and segregation, with air gaps and properly implemented Access Control Lists (ACL), can help limit the scope of an incident and can also improve network performance because broadcast domain traffic can be minimized.

3. Configuration and Change Management

GOAL: Document and control hardware and software inventory, system settings, configurations, and network traffic flows throughout control system hardware and software lifecycles.

RATIONALE: Configuration and change management ensures that the organization’s cybersecurity program objectives remain satisfied by ensuring that new systems are deployed in a secure consistent state and maintain this state as changes are made throughout their lifecycles. It reduces the risk of outages due to configuration issues and security incidents through improved visibility and tracking changes to the system.

4. Physical Security

GOAL: Physical access to systems, facilities, equipment, and other infrastructure assets, including new or replacement resources in transit, is limited to authorized users and are secured against risks associated with the physical environment.

RATIONALE: Limiting physical access to only authorized individuals protects against malicious actors gaining physical access to control system components. These protections also help prevent unintentional damage.

5. System and Data Integrity, Availability, and Confidentiality

GOAL: Protect the control system and its data against corruption, compromise, or loss.

RATIONALE: Protecting the control system and its data against corruption, compromise, or loss is vital to its operation.

6. Continuous Monitoring and Vulnerability Management

GOAL: Implement and perform continuous monitoring of control systems cybersecurity threats and vulnerabilities.

RATIONALE: Continuous monitoring ensures that the periodic review and testing of security controls, processes, and procedures are conducted to confirm that the established security controls remain in place and that change in the system, network, environment, or emerging threats does not diminish the effectiveness of these controls, processes, or procedures. Vulnerability management ensures that the technical and operational elements are sufficiently protected against adversaries' attack methods, which often include targeting outdated and unpatched systems.

7. Training and Awareness

GOAL: Train personnel to have the fundamental knowledge and skills necessary to recognize control system cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.

RATIONALE: Comprehensive cybersecurity awareness training is one of the best ways to help protect against and mitigate cyber-attacks and prevent possible breaches.

8. Incident Response and Recovery

GOAL: Implement and test control system response and recovery plans with clearly defined roles and responsibilities.

RATIONALE: Dedicated resources and established plans limit the impacts of a cyber-attack and minimize the time to reconstitute critical systems and functions.

9. Supply Chain Risk Management

GOAL: Risks associated with control system hardware, software, and managed services are identified and policies and procedures are in place to prevent the exploitation of systems through effective supply chain risk management consistent with best practices (e.g., NIST SP 800-161).

RATIONALE: Commercially available technology solutions (hardware, software, and services) present significant benefits including lower cost, rapid innovation, product feature variety, and ability to choose from competing vendors. However, acquiring these solutions introduces additional risk to the organization because of decreased visibility into how the solutions are developed, integrated, and deployed, as well as the processes to ensure the security, resilience, reliability, integrity and quality of the solutions. The intent of this goal is to ensure that items and services are procured from trusted sources and have traceability through the use of a trusted distribution path.

Each of the nine goals described above includes specific objectives that support the deployment and operation of secure control systems that are further organized into baseline and enhanced objectives

Observations and Conclusions

This represents the start, not the end of an effort by the United States Federal Government to enhance the cyber security maturity of critical infrastructure and from the perspective it provides some insight into the approach going forward which may guide future regulation and good practice [NSM 2021]. Standards provide a strong starting framework for how to deliver and strengthen cyber security, however the standards landscape is increasingly complex and fragmented which if anything leads to confusion as opposed to providing a standardised consistent framework that all critical infrastructure owners and managers to work towards. The consolidated goals provide a framework that is based on a broad spread of standards and good practice but simplifies what the key requirements are into these performance goals and underlying objectives for each one of them. It also means that if an organization has already aligned itself with the NIST Cybersecurity Framework, the Financial Services Sector Coordinating Council Cybersecurity Profile, or the NERC Critical Infrastructure Protection standards, its cybersecurity program likely has a strong foundation to achieve these goals [Dembosky 2021]. Critical infrastructure entities should consider these objectives against what is already in place and identify any differences as potential areas of growth.

7.5.3 Standards and NIS compliance

Standards and NIS compliance by Argyro Chatzopoulou, TÜV TRUST IT GmbH

7.5.3.1 The AI4HealthSec Project

The EU-funded AI4HEALTHSEC project will develop a solution that improves the detection and analysis of cyberattacks and threats on HCIIs. The aim is to build situational awareness and incident handling and risk assessment among HCIIs. Another important step is providing health operators the capability to react in case of security breaches. AI4HEALTHSEC will also ensure the exchange of reliable and trusted incident-related information, among ICT systems and entities making up the HCIIs.

AI4HEALTHSEC proposes a state-of-the-art solution that improves the detection and analysis of cyber-attacks and threats on HCIIs and increases the knowledge on the current cyber security and privacy risks. Additionally, AI4HEALTHSEC builds risk awareness, within the digital Healthcare ecosystem and among the involved Health operators, to enhance their insight into their Healthcare ICT infrastructures and provides them with capability to react in case of security and privacy breaches. Last but not least AI4HEALTHSEC fosters the exchange of reliable and trusted incident-related information, among ICT systems and entities composing the HCIIs without revealing sensitive corporate details.

7.5.3.2 Main idea

In preparation of the implementation of the project work, the project team of the AI4HEALTHSEC, run an analysis of existing and developing standards in the focus areas of the project. The objective of this analysis was to become acquainted with the state of the art, to collect valuable information, to build upon them and to identify possible shortcomings.

After the initial analysis that provided the foundation for the first deliverables of the project, the project team decided to enrich this analysis and map standards to all the proposed measures of the NIS Cooperation Group (Reference document on security measures for Operators of Essential Services, CG Publication 01/2018 [NIS 2018]).

The analysis was implemented according to the following parameters:

- The SDOs (Standard Developing Organizations) that were included in the analysis were at least the following: CEN and CENELEC, ETSI (CYBER), IEC, OASIS, ISO/IEC, IEEE, NIST. (Some exceptions of other SDO’s were allowed in cases where a specific standard on the subject is well known or recognized.)

- To these SDOs, organizations like ENISA and specific Cybersecurity Authorities were added, since it was found that specific guidance documents were provided specifically on the subject of Network and Information Security.
- The standards identified are in their majority not sector specific.
- The standards identified are in their majority not technology specific.
- The standards identified are viewed from the perspective of the provision of guidance to the organizations (independent of size). This means that standards presenting the scientific basis of a security measure where not included. E.g., For the Cryptography security measure, standards like ISO/IEC 15946-1:2016 Cryptographic Techniques Based on Elliptic Curves -- Part 1: General [ISO-IEC 2016] (standard that describes the mathematical background and general techniques necessary for implementing the elliptic curve cryptography mechanisms) are not included. Whereas NIST, SP 800-57 Part 1 Revision 5 – General, cryptographic key-management guidance [SP 800-57 2020] was included since it provides guidance on key management practices.

7.5.3.3 Results

The analysis described in Section 7.5.3.2 above, resulted in the identification of 349 cases of standards mapped to the security controls of the “Reference document on security measures for Operators of Essential Services, CG Publication 01/2018”.

Figure 51 is a representation of the results per measure and section (while the detailed information was collected and is maintained by the project team).

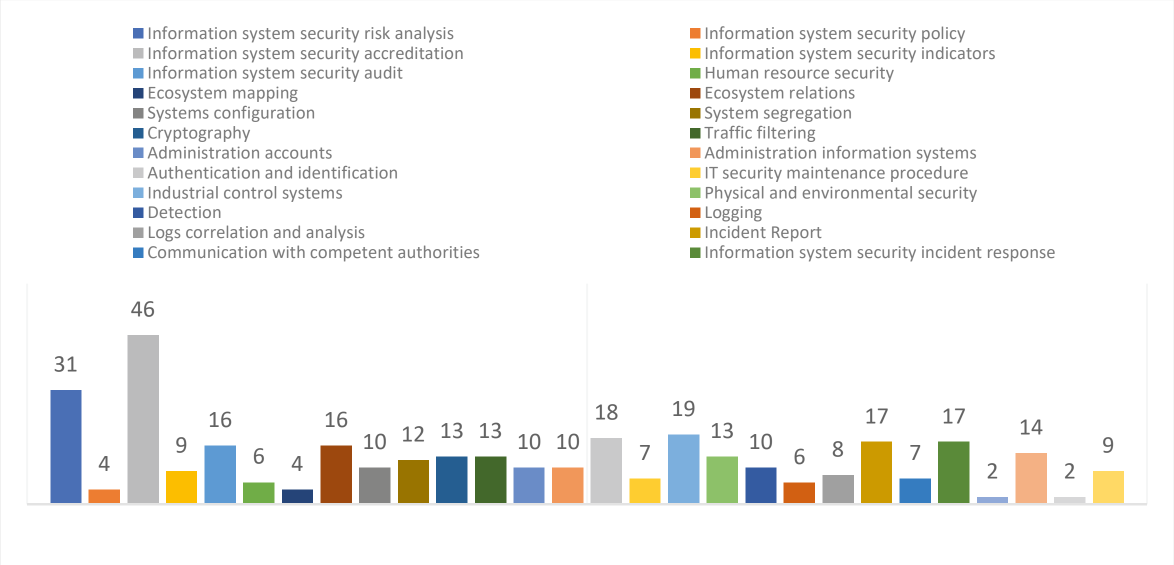


Figure 51 - A representation of the standards analysis results per measure and section

7.5.3.4 Conclusions

The analysis performed and described above, revealed that there is a variance in the number of standards that exist per security measure as proposed by the “Reference document on security measures for Operators of Essential Services, CG Publication 01/2018”.

There are areas where a high number of standards were identified by the project team e.g., Information system security risk analysis, Industrial control systems and Authentication and identification and other areas where a low number of standards were identified by the project team e.g., Crisis management organization and Disaster recovery management.

It is the opinion of the project team that the following should be carried out in support of the NIS compliance:

- Conduct further analysis on the reasons behind these fluctuations. This would allow for the implementation of solutions that would fit the cause of the problem and provide value to the entire market
- Conduct studies on the interoperability among standards that cover the same area (like INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK. Methodology for and assessment of interoperability among risk management frameworks and methodologies, JANUARY 2022. ENISA [ENISA 2022-2]). These studies will provide the market with a way to correlate between the different standards and provide also the policy makers and SDOs with information on existing gaps and opportunities for improvement.
- Especially for the areas where a limited number of standards have been identified, the SDOs and other interested parties should further investigate the situation and develop specific standards to fill these gaps if needed.
- Further research needed to promote the direct communication between the stakeholders, by facilitating security-related information sharing through standards and decentralized coordination and improving the overall cyber-situational awareness of the digital ecosystem.
- The digital SC ecosystems raise the need for advanced self-healing and self-repairing processes, which facilitate the automatic recovery and reconfiguration of their IT/OT components in order to guarantee the business continuity in the IT-interconnected networks. In this context, further research needed to improve the cybersecurity practices, enhance the business continuity and disaster recovery processes of the digital infrastructures by empowering them with new advanced self-healing capabilities.
- Finally, and in alignment to the Rolling Plan for ICT Standardization, efforts should be invested in the identification, development and communication in an easy and straight forward way of standards for SMEs.

7.5.3.5 Acknowledgements

The work carried out within the AI4HealthSec project in general and as analysed within this document has received funding from the European Union’s Horizon 2020 research and innovation programme, under Grant Agreement 883273.

7.6 Common Platform for Cascading Effects on the Different Critical Infrastructures

7.6.1 Synergies and Challenges towards the integration of Safety and Security requirements in Critical Infrastructure Protection: Examples from the SecureGas and Infrastress projects

Synergies and Challenges towards the integration of Safety and Security requirements in Critical Infrastructure Protection: Examples from the SecureGas and Infrastress projects by Clemente Fuggini (RINA Consulting)

Managers of critical infrastructures (CI), of whatever sphere, no longer want to check individual risks but to analyse combined risks, so assessing and modelling critical infrastructure assets, vulnerabilities, combined risks and threats, to improve the synergic management of safety and security issues, without affecting the core business (and the continuity of the business) of the CI operator.

One of the mistakes, or wrong considerations, is to consider safety and security. Safety Report is based on the assessment of probability and consequences for events deemed "credible", which aims to demonstrate that major-accident hazards have been identified and necessary measures are taken to prevent or limit their consequences. Major accident risk companies have different regulations for safety actions and multiple standards as guidelines for various risk analyses.

There is not currently a reference standard for security, the approach in use is risk-based, and customised according to needs. However, The Plan-Do-Check-Act (PDCA) cycle is the operating principle of several management systems applied to industries including BS OHSAS 18001 (Occupational Health and Safety) and ISO/IEC 27001 (Information security).

Safety and Security were and are effectively separated but follow parallel paths. Separation is due to different reasons: cultural, socio-politic and technological aspects.

Security is a much newer field (especially cybersecurity) and is mandatory only in specific sectors such as Critical Infrastructures, Maritime, and dangerous goods transportation.

Safety standards and associated engineering work practices are mature and well-established. Occupational Health and Safety and Major Hazards Control disciplines are regulated by laws applied to all industry sectors.

Some recent regulatory frameworks consider both disciplines and require avoiding any conflict between safety and security (in case of conflict, safety shall prevail).

Finally, nowadays there is a recognition that a cybersecurity attack could compromise the safety of sensitive industries (i.e., pose at high-risk).

In the European Infrastress project, whose objective was to 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 the continuity of operations, while minimizing cascading effects in the infrastructure itself, the environment, the other CIs, and the citizens in the vicinity, at a reasonable cost, compared the existing methodologies of risk analysis and emergency management with the new InfraStress methodologies to verify the level of resilience of the Sensitive Industry Sites and Plants (SIPS).

This activity is linked to the translation into operational procedures and knowledge creation, (especially the InfraStress methodology), to be afterwards transposed into new practice for industry

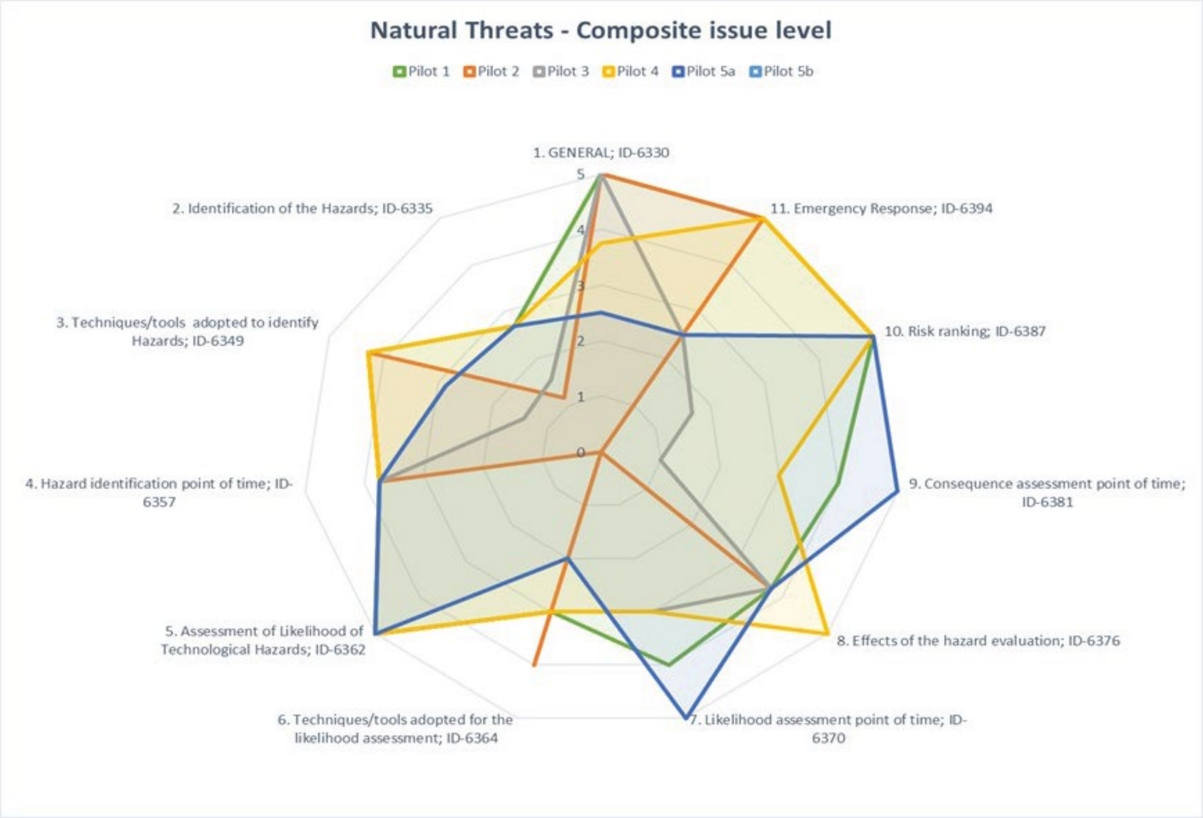


Figure 52a - Comparison of Infrastress methodology (H2020 Infrastress)

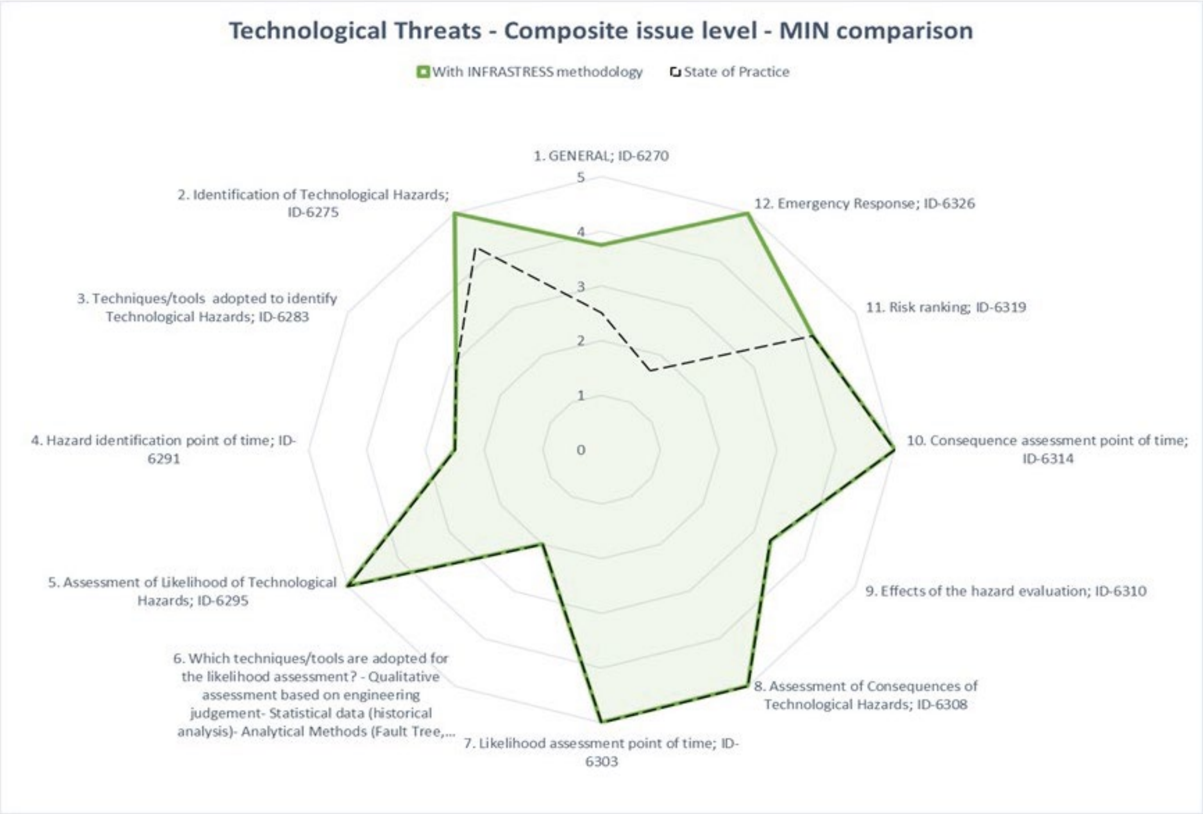


Figure 53b - Comparison of Infrastress methodology (H2020 Infrastress)

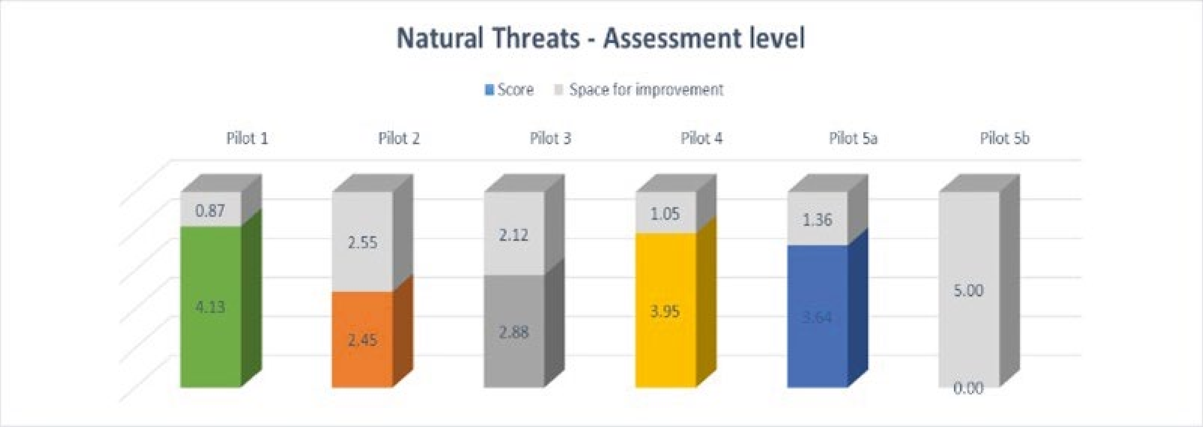


Figure 54c - Comparison of Infrastress methodology (H2020 Infrastress)

In the European SecureGas project, whose scope was the definition, design, development, testing and validation of the Conceptual Models and High-Level Reference Architecture where Safety and Security synergies are taken into account since the design stage, taking one of the case studies as an example, working with a drone equipped for gas detection, testing the leakage of methane gas from the pipeline due to manumission or an accidental incident. These operations involve the synergy of safety & security because:

- Safety issue: safe flight planning and related risk analysis
- Security issue: control of the drone and capture of data by cyber-criminals

7.6.2 Simulation Framework for Cascading Effects among Urban Critical Infrastructures

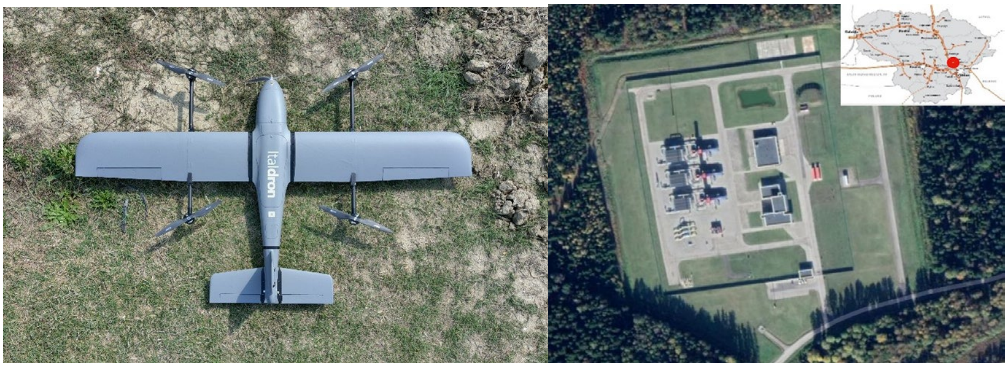
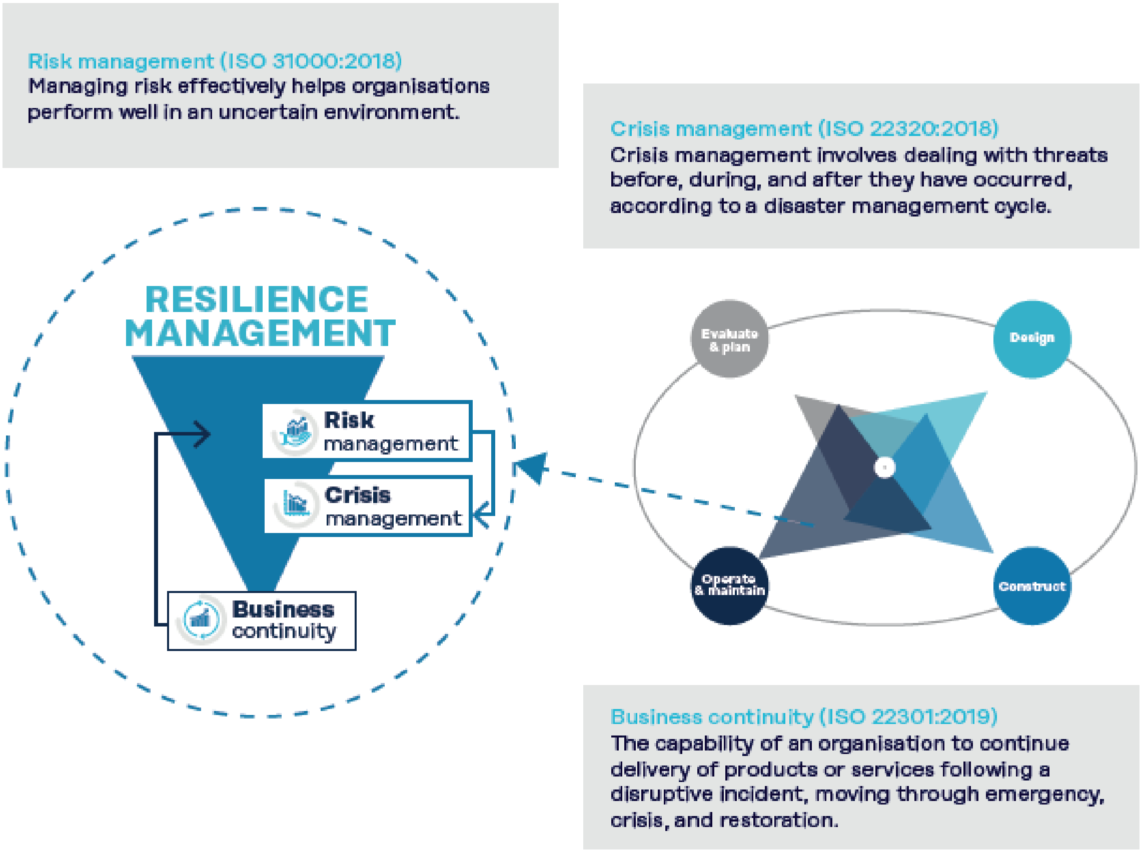


Figure 55 - Test Case about drone inspection (H2020 SecureGas)

Integrating safety and security is a very realistic challenge from the point of view of success. however, there are some considerations to mention. No legislation obliges the operator to implement security measures in safety plans, but it is understood that physical protection of the installation is the first form of control. It is clear that business continuity plans must include everything necessary to respond to physical attacks (attacks, sabotages, etc.) in order to protect personnel and the environment. Therefore, including a security analysis in the safety plans leads the manager to have a global and unique vision of the risks without divisions and fragmentations. So safety and security cannot be considered separately. Safety methods do not provide protection against intentional events: safety measures cannot protect the integrity of the plant if the security methods fail.

There are so many standards for security (ISO 27001 ISO 31000 ISO 45001 etc.), but all of them are stand-alone and do not take into account the synergies between them. The interconnection of the critical infrastructure network implies an extension of risks to and from everything connected to it. Those who prepare an attack have the advantage of time to prepare, but those who react to the attack must do so immediately and well.

Risk management, business continuity and resilience are interrelated as they have a common goal, Risk management does not eliminate risks, which is why there is the study of business continuity and Also business continuity does not eliminate the risk of disruption (even if it is reduced) and there is a need for a resilient approach that allows companies to adapt and respond to unusual and unexpected circumstances, and looking-forward to anticipate future trends and risks. These must follow a cycle, as shown in Figure 56, in order to have cyclic continuity of analysis



Risk management (ISO 31000:2018)
Managing risk effectively helps organisations perform well in an uncertain environment.

Crisis management (ISO 22320:2018)
Crisis management involves dealing with threats before, during, and after they have occurred, according to a disaster management cycle.

Business continuity (ISO 22301:2019)
The capability of an organisation to continue delivery of products or services following a disruptive incident, moving through emergency, crisis, and restoration.

Figure 56 - How RINA intent resilience management for CI operators

7.6.3 Simulation Framework for Cascading Effects among Urban Critical Infrastructures

Simulation Framework for Cascading Effects among Urban Critical Infrastructures by Stefan Schauer (AIT Austrian Institute of Technology GmbH)

In large cities and metropolitan areas, Critical Infrastructures (CIs) from different sectors are located in a geographically narrow space. They are required to maintain essential services like the supply of power, water, food, or communication and thus represent the backbone of social life in that area. Due to the high interdependencies among each other, a single incident within one CI can have wide-ranging cascading effects among the entire CI network and thus affects society in that area to a large degree. Cyber-attacks in the past years, e.g., the hacking of the Colonial pipeline in 2021 [Bing 2021], have underlined that. In the PRECINCT project, we tackle this problem by developing an integrated platform that builds on a structural representation of the CIs within a city and provides algorithms to analyse threats, simulate the potential cascading effects stemming from those threats, compute a resilience measure for the CIs and the entire city and uses Digital Twin and Serious Game technologies to develop effective countermeasures to increase the CIs' and the city's resilience.

The approach applied in PRECINCT to capture the interrelations among the CIs is to create a novel form of CI Interdependency Graphs (CIIGs). Such a graph represents the individual CIs (or specific critical assets within them) as nodes and describes the dependencies among them as directed edges. PRECINCT extends this standard notion by introducing the concept of "operational states" for each CI (i.e., for each node of the CIIG), which captures the CI's functionality in an abstract way. A core focus of this model is to describe the expected behaviour of a CI affected by an incident occurring either in the CI itself or in one of its suppliers. For example, a power grid outage may not instantly affect a connected hospital, but may do so with a certain temporal delay, once the emergency power supply runs out of fuel. The mathematical models for the general stochastic processes to describe such time-dependent dynamics are based on artificial neural networks (cf. Figure 57). They are trained to be simplified Digital Twins of individual domains, which learn the behaviour of the underlying CIs or critical entities, provided that the required data are made available by the operators of the respective infrastructures. Thus, these neural networks form a realistic representation of the individual entities to facilitate the analysis of the effects and resulting impacts of incidents on them.

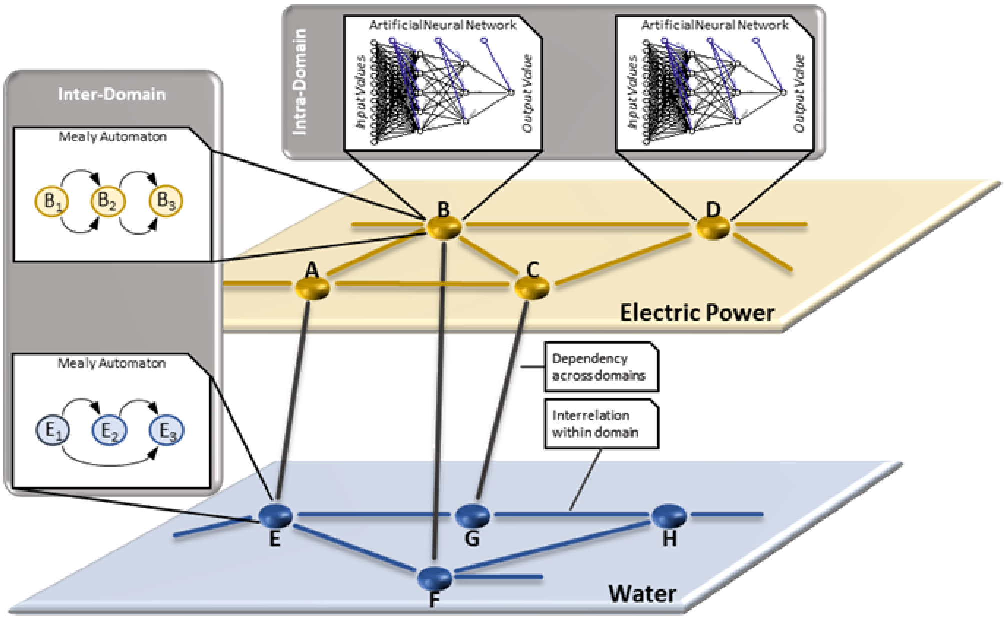


Figure 57 - Illustration of the Intra- and Inter-Domain Simulation Model

For the description of the dynamics across the individual domains, an innovative approach is applied in which the behaviour and functionality of the respective systems are represented by a probabilistic Mealy automaton with multiple states [König 2019]. Each state of an automaton represents its degree of functionality, e.g., ranging from "normal operation" to "complete breakdown". The central aspect to describe the dynamics are the transitions between the different states. They characterize how a system reacts due to an incident taking place in another system or domain. A change of the operational state can then either occur internally as dictated by the specific neural network describing the CI’s behaviour over time (Intra-Domain Model in Figure 57), or externally, if a supplier node changes its state, and communicates this information as a signal through the Mealy automaton (Inter-Domain Model in Figure 57). The external influences of the incident together with the current state (the current functionality) of the critical entity determine the new state of the entity.

In case there is not enough data on a CI’s response behaviour available to train an artificial neural network or if the dynamics are highly uncertain, the transitions between the states of the Mealy automaton can also be based on probabilities that are estimated by experts, e.g., from the CIs. This adds flexibility to include a large variety of domains, combining areas where the physical dynamics are well known (such as water, energy, etc.), with others, where the dynamics does not admit an accurate mathematical description (such as people’s risk response, social media/press reception, and others). Having such an integrated model covering all CIs in a metropolitan area significantly simplifies their assembly into a joint co-simulation framework and provides sufficient information on potential cascading effects for decision makers as well as a strategic defence planning.

The vision of PRECINCT is to develop a simulation framework that is not only capable to compute potential cascading effects of an incident happening in a city but also to visualize these effects in a geo-located form (cf. Figure 58). Therefore, PRECINCT plans to use existing geo-located data either from open sources (e.g., Google Maps or OpenStreetMap) or already existing Digital Twins. In this way, the severity of the impact (e.g., indicated by colour coding) and the overall timeline of the cascading effects would be easier to comprehend and understand by decision makers. Furthermore, the aim is to simulate multiple incidents as part of one scenario to capture complex crisis situations as well. Additionally, the underlying CIIG will be flexible such that decision makers can change the graph’s structure in the model to virtually analyse countermeasures and evaluate their effectiveness as part of a training session (i.e., a Serious Game).

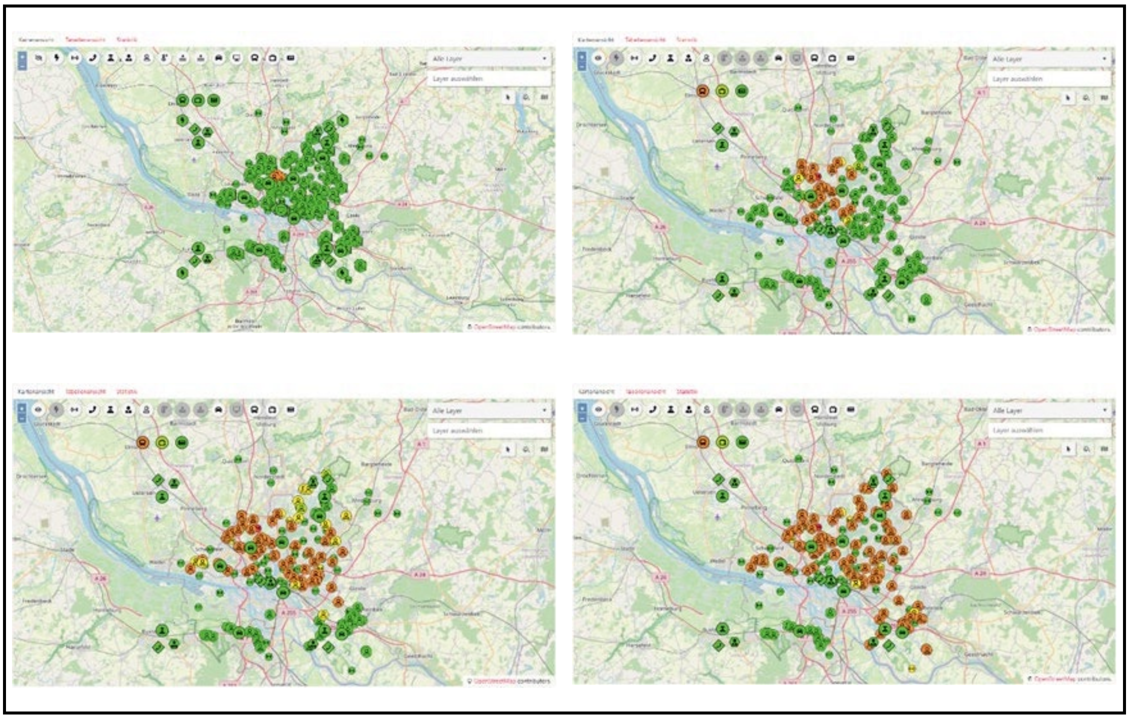


Figure 58 - Future concept for cascading effects simulation in PRECINCT

The overall goal of the PRECINCT project is to support crisis managers – and decision-makers in general – within metropolitan areas in preparing for critical incidents and crisis situations. The simulation framework sketched above represents a core building block to achieve that, as it allows decision-makers to simulate cascading effects that might happen in a specific crisis. Further, the framework is integrated into the computation of PRECINCT's overall resilience measure for the entire metropolitan area, i.e., capturing all CIs as a complex network and considering the cascading effects among them as well. Additionally, the framework is an important part of PRECINCT's Serious Game as well, since the computation of the cascading effects is necessary to estimate the effectiveness of the countermeasures, which the "players" of the Serious Game can choose to reduce the impact of the modelled incident.

7.7 Combined Safety and Security for European Critical Infrastructures

7.7.1 Integrated Security, Safety and Risk Assessment for CIs

Integrated Security, Safety and Risk Assessment for CIs by Antonis Kostaridis (SATWAYS)

It is acknowledged that climate-related and natural hazards have the potential to substantially affect the lifespan and effectiveness or even destroy European Critical Infrastructures (CI). In this context, modelling the impact of climate change to CIs is on vital importance.

i-RISK (Critical Infrastructure Risk Assessment Platform) is a collaborative software environment that aims to create new capabilities for CI policymakers, decision-makers, and scientists by allowing them to use different and diverse modelling and risk assessment solutions, to develop risk reduction strategies and implement mitigation actions that help minimise the impact of climate change and natural hazard on CIs. This can help improve the understanding of system interdependencies by providing decision-makers with the latest tools, based on the best scientific and engineering principles, as they emerge. From the policy and decision-maker perspective, the platform capabilities are offered as a toolbox that consists of a collection of diverse Risk and Resilience analyses of Critical Infrastructures that are exposed to the direct and indirect effects of the aforementioned hazards.

The i-RISK has been initially used in H2020 EU-CIRCLE project, further expanded within INFRATRESS and finally and finally advanced within PANOPTIS project (http://www.panoptis.eu/), the latter of which aims to develop a Decision Support System for increasing the Resilience of Transportation Infrastructure based on the combined use of terrestrial and airborne sensors and advanced modelling tools. The main objectives of the project contain the following:

- use high-resolution modelling data for the determination and assessment of the climatic risk of the selected transport infrastructures and associated expected damages
- use existing SHM data (from accelerometers, strain gauges etc.) with new types of sensor-generated data (computer vision) to feed the structural/geotechnical simulator
- utilize tailored weather forecasts (combining seamlessly all available data sources) for specific hot spots, providing early warnings with corresponding impact assessment in real time
- develop improved multi-temporal, multi-sensor UAV- and satellite-based observations with robust spectral analysis, computer vision and machine learning-based damage diagnostic for diverse transport infrastructures
- design and implement a Common Operational Picture, including an enhanced visualization interface and an Incident Management System
- design and implement a Holistic Risk Assessment Platform environment as an innovative planning tool that will permit a quantitative resilience assessment through an end-to-end simulation environment

The last of the above objectives has been delivered by the i-RISK platform (called HRAP in the framework of the project), the scientific workflow is presented in Figure 59, which is based on the commonly known risk function depicted below

RISK = HAZARD x EXPOSURE x VULNERABILITY

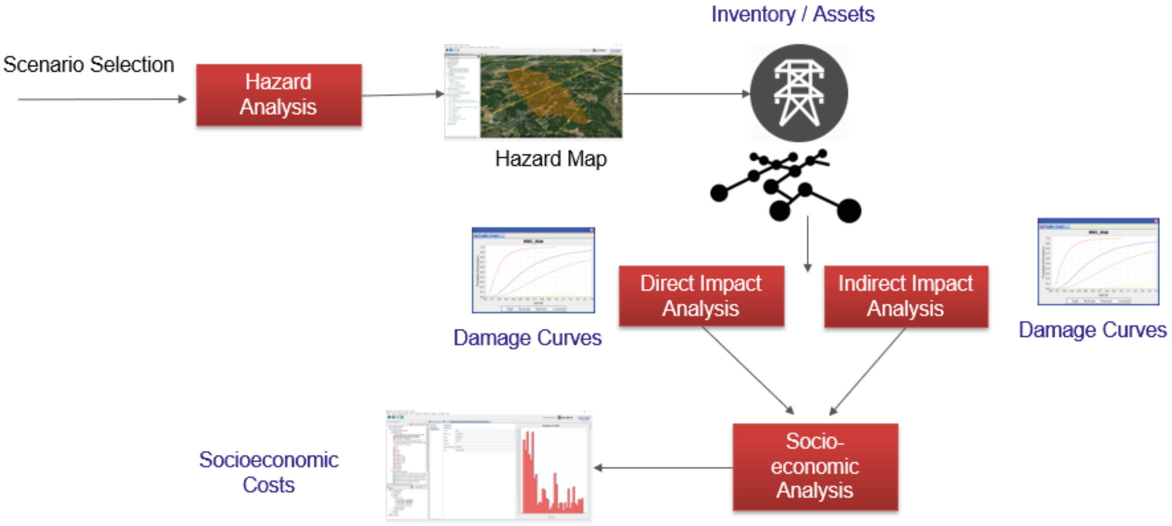
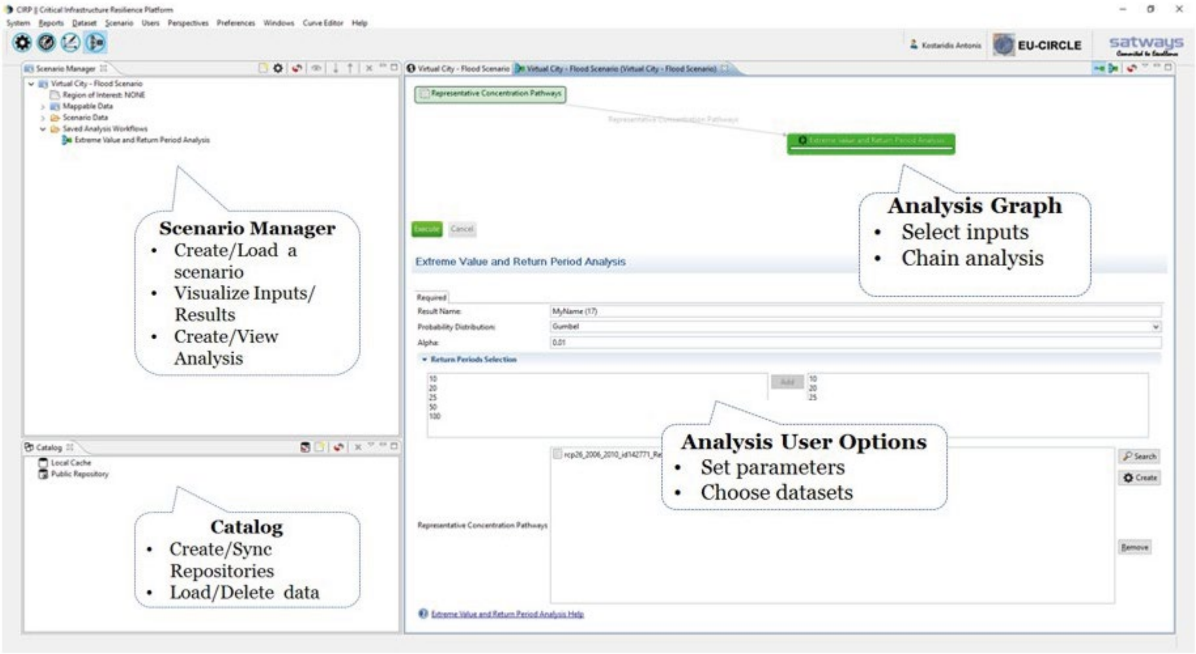


Figure 59 - i-RISK scientific workflow

From the design point of view, one of the main goals was to have a user interface as friendly and customizable as possible, which includes a menu, toolbars (top, left, right and bottom), the perspective area and the main toolbar where the users will be able to navigate between the different perspectives. A description of the application screen and navigation icons is provided in Figure 60.


CIRP || Critical Infrastructure Resilience Platform
System Reports Dataset Scenario Users Perspectives Preferences Windows Curve Editor Help
Kostaridis Antonis
EU-CIRCLE
satways
Scenario Manager
Virtual City - Flood Scenario
Region of Interest: NONE
Mappable Data
Scenario Data
Saved Analysis Workflows
Extreme Value and Return Period Analysis
Virtual City - Flood Scenario
Virtual City - Flood Scenario (Virtual City - Flood Scenario)
Representative Concentration Pathways
Extreme Value and Return Period Analysis
Execute
Cancel
Required
Return Periods Selection
Add
rcp26_2006_2010_id142771_Re
Representative Concentration Pathways
Search
Create
Remove
Catalog
Local Cache
Public Repository
Extreme Value and Return Period Analysis Help

Extreme Value and Return Period Analysis

Result Name: MyName (17)
Probability Distribution: Gumbel
Alpha: 0.01

10
20
25
50
100

10
20
25

Scenario Manager
- Create/Load a scenario
- Visualize Inputs/ Results
- Create/View Analysis

Analysis Graph
- Select inputs
- Chain analysis

Analysis User Options
- Set parameters
- Choose datasets

Catalog
- Create/Sync Repositories
- Load/Delete data

Figure 60 - i-RISK user interface

The most commonly displayed views of the i-RISK User interface are:

- Local Scenario Manager View – enlists all available scenarios (local scientific workflows, input datasets, output datasets) and provides functions to create and edit scenarios and depict datasets on the map.
- Local Workflow View – displays a selected local scientific workflow and provides the means to select input datasets from Local or Remote Data Repositories, select analysis parameters and execution of workflows.
- Catalog View – allows the management of repositories (Local or Public) and their datasets.
- Curve Dataset View – This view depicts fragility/damage curves datasets.
- Chart View – This view depicts bar charts statistics based on selected attribute of feature layers.
- Curve Data Table View – Depicts the x, y-axis value pairs of damage/fragility curves
- 2D Map View – Depicts raster and feature datasets (input and outputs of scientific workflows) overlaid on a 2D map.
- Static Information Layers View – Enlists in a hierarchical manner all the map layers whose map features do not change properties over time (e.g., transport network, road infrastructure elements etc.).
- Dynamic Information Layers View – Enlists in a hierarchical manner all the map layers whose map features change properties over time (e.g., meteorological stations).
- 3D Map View – Depicts raster, feature datasets (input and outputs of scientific workflows), 2D and 3D objects overlaid on a 3D terrain.

Through the usage of i-RISK functionalities, CI operators and other practitioners can estimate the impact of a hazard on the CIs, making use of a set of chained analysis available from the respective toolbox that estimate damage, losses, vulnerable components, etc. which are finally offered to the user though 2D and 3D environment, but also result statistics for the damage analysis.

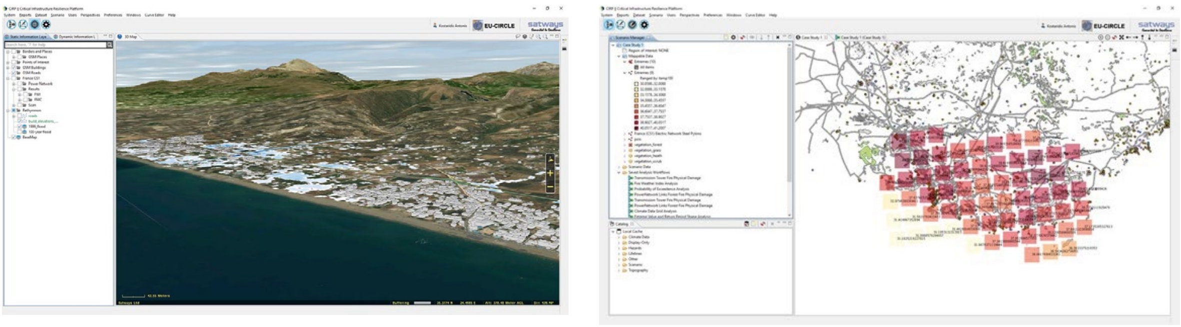


Figure 61 - Risk assessment examples

To sum up, i-RISK provides all the means to execute scientific workflows in “what-if” mode, as well as remote workflows in “what-is” mode as it can automate the execution of workflows based on real-time sensor data inputs. In addition, it allows the execution of Remote Scientific Tools and Workflows according to the Grid Computing principles. In PANOPTIS, with the appropriate selection of model chains, hazard, data, i-RISK can prove to be a valuable decision support tool for CI operators and decision makers as it offers a user-friendly application that enables the intuitive design and analysis of modelling scenarios created for any combination of natural hazard and CI assets. In this way, users can understand the impact of various adaptation strategies or to quantify the potential impact of a catastrophic event on society.

7.7.2 Pan-European cybersecurity information and incidents sharing and management for Energy Infrastructures

Pan-European cybersecurity information and incidents sharing and management for Energy Infrastructures by Sofia Tsekeridou (Netcompany - Intrasoft)

The Electrical Power and Energy System (EPES) is considered among the most complex Cyber-Physical systems with huge cascading effects to other critical infrastructures, such as water supply, communications, transportation, industry, finance, health, and has already experienced complex cyber-attacks. Considering further that Smart Grids are nowadays realized via modern EPES physical/digital systems while connectivity and increased Internet usage have spread to improve relevant operations and services, one may easily understand that more vulnerabilities of EPES CIs are exposed in this way, offering even more opportunities for coordinated complex attacks to such Critical Infrastructures.

To address such challenges and provide for increased cybersecurity, the European Commission and relevant Agencies such as ENISA, ENTSO.E, ACER have been constantly investing efforts in defining relevant policies and regulations in the sphere of security and cybersecurity, such as:

- **The EU Cybersecurity Strategy**, that proposes building a European Cyber Shield via a network of Security Operations Centres across the EU
- **The Cybersecurity Act**, that aims to promote ICT certification at EU level
- **The NIS Directive** - Directive on Security of Network and Information Systems, that underlines the significance of joint activities and knowledge sharing among the relevant stakeholders and establishes the CSIRTs Network
- **The NIS2 Directive**, an updated version of NIS, that further expands its scope on new CI sectors in accordance with their critical role, imposes stronger security requirements and enhances information sharing and cooperation through the establishment of the European Cyber Crises Liaison Organisation Network (EU - CyCLONe)
- **NCCS - the Network Code for cybersecurity aspects of cross-border electricity flows**, that outlines cross-border electricity flow governance policies for cybersecurity risk management, risk assessment, evaluation, and treatment. It further introduces the essential information flows and dictations for incident and crisis management in its Articles 37-42, such as the role of Public Authorities concerning information sharing (Art. 38), or the provisions for an early warning system for threat information gathering, processing, notification, providing the right information to the right people at the right time (Art. 42). It further details liaison with CyCLONe, the Joint Cyber Unit and the CSIRT Network.

In the context of the H2020 PHOENIX Project, following closely the respective policies and regulations, even at their early stages of drafting,

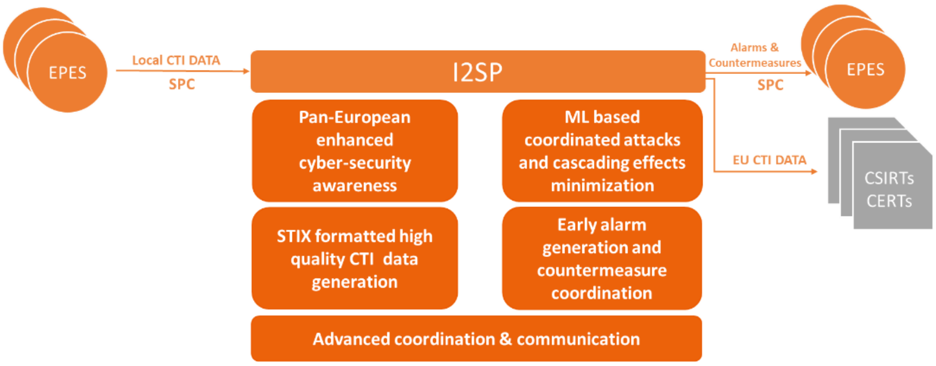

EPES
Local CTI DATA
SPC
I2SP
Alarms & Countermeasures
SPC
EPES
Pan-European enhanced cyber-security awareness
ML based coordinated attacks and cascading effects minimization
EU CTI DATA
CSIRTs
CERTs
STIX formatted high quality CTI data generation
Early alarm generation and countermeasure coordination
Advanced coordination & communication

Figure 62 - I2SP – Distributed Incidents Information Sharing Platform, License: CC BY-NC

Focusing on the information sharing capabilities of I2SP, which is a primary target of cybersecurity policies and regulations, particularly NCCS, which is focused on cybersecurity in the Energy sector, I2SP has been one of the first implementations of such functionalities. Information sharing from an EPES node to the I2SP local/central node, in the distributed I2SP architecture, as well as from the I2SP local/central node to relevant other EPES nodes and CERT/CSIRT authorities, is governed by the mutually agreed "Sharing Manifest". The latter information sharing path is driven by the formed Trust Circles – a Trust Circle is defined as a group of entities that have agreed to share information with I2SP and among themselves. The term originates from MeliCERTes. Trust Circles and Sharing manifests are pre-configured in accordance to involved entities governance and data sharing policies. The same applies to Pan European attack trees in order to infer coordinated attacks and relevant alarms and recommend mitigation actions and counter measures that are also shared securely through the Information Sharing Engine of I2SP. To allow interoperability with existing CTI information sharing tools, the most widely used by CIRTs/CSIRTs being MISP, integration of I2SP with MISP has been undertaken, developing translation functionalities of STIX data to MISP objects.

I2SP finally provides a fully-fledged control centre providing role-/rights-based information visualization, situational awareness, alerting and decision support, reaching up to pan-european level, as shown in Figure 63 (*information is blurred on purpose, although only fake data are used, due to its sensitivity*). Specifically, it supports interactive visualizations of identified attacks on a map, supporting clustered report aggregates, and tabular visualization of the last-identified and historical attacks. It further provides a full-page overview of the identified attacks, including information about the identified attack campaign and its related attacks, the timing and the location of the attacks, the mitigation information (description, risk without mitigation, residual risk), and visualization of the EPES attacked in the specific campaign. It further generates graphical reports regarding the identified attacks rates. It finally provides functionalities for managing and visualizing in tabular form the Trust Circles and the connected organizations.

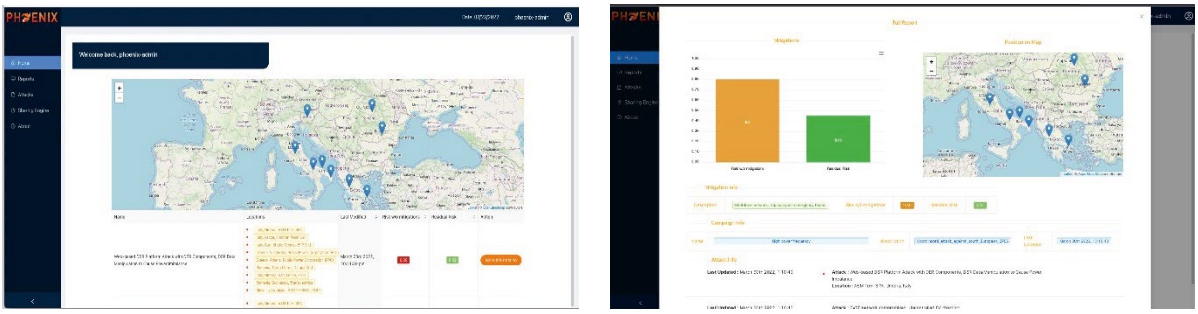


Figure 63 - I2SP – Control Centre: Homepage and Full Report, License: CC BY-NC

7.8 Cyber Security Awareness

Cyber security awareness in critical infrastructures by Christos Angelidis (konnektable)

The SIEM solution aims to combine security information management (SIM) with security event management (SEM), forming a single collaborative security management system. It consists of the following:

- **Wazuh Agents:** Installed on the monitored endpoints such as servers, routers, laptops, and forward events to a centralized cluster.
- **Wazuh Cluster:** A group of Wazuh managers that work together, divided by a master node

and worker nodes

- **Elasticsearch Cluster:** A collection of one or more nodes that communicate with each other to perform read and write operations on indexes
- **Kibana Server:** A flexible and intuitive web interface for mining, analyzing, and visualizing data and end-user interactions with the system.

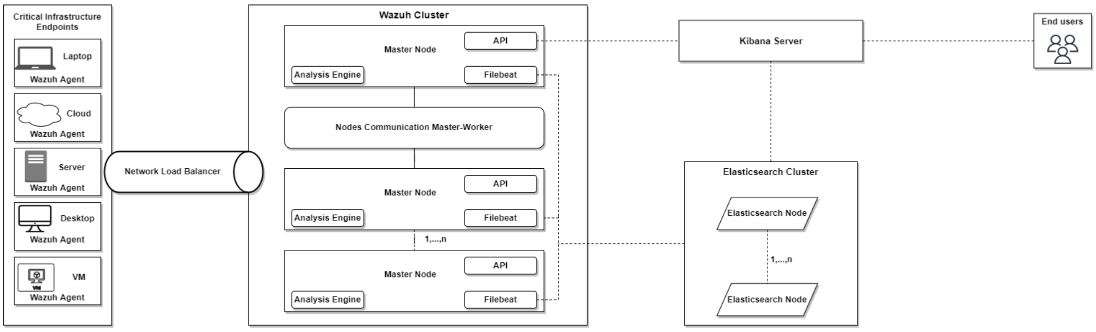
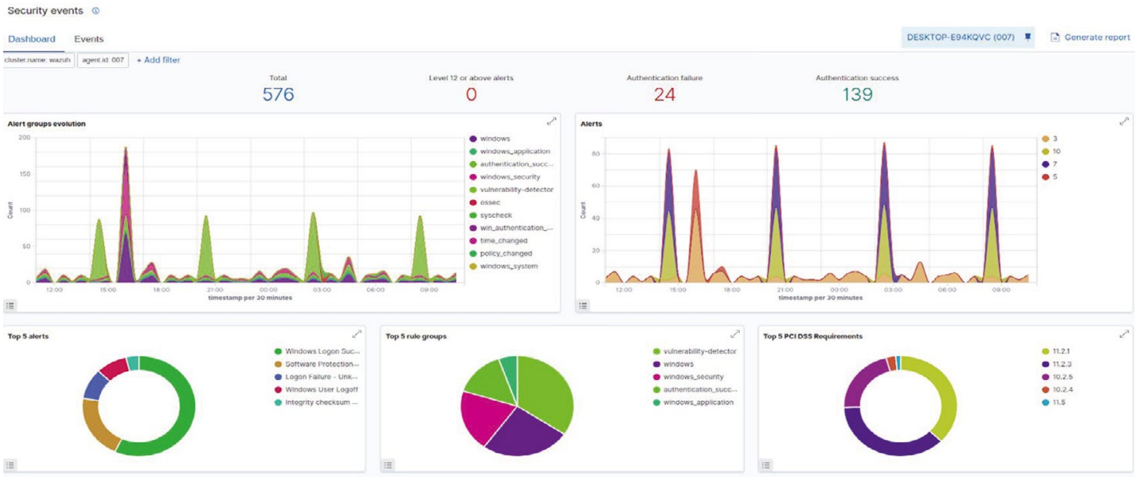


Figure 64 - SIEM as a standalone tool

It can be installed in any Critical Infrastructure, in order to protect it from any malicious activities. More specifically, SIEM will detect and monitor the infrastructure's endpoint activities. The endpoints, where the SIEM's agent can be installed, are Servers, VMs, laptops, or Desktops.


Security events

Dashboard Events

cluster.name: wazuh | agent.id: 007 | + Add filter

DESKTOP-E94KQVC (007) | Generate report

Total	Level 12 or above alerts	Authentication failure	Authentication success
576	0	24	139

Figure 65 - Agents Dashboard

Also, it, in detecting attacks, is considered an essential solution to protect critical Infrastructures against a variety of threat scenarios. It can identify anomalies in the system. As a result, alarms can be raised when a deviation is detected, and valuable information is provided to the SOC Analyst that can help to mitigate and manage detected attacks.

To dive deeper into the SIEM solution and its architecture:

- Wazuh consists of its agents that are the monitoring endpoints,
- Wazuh server to collect and analyze the incoming events from the agents and
- Filebeat, a dedicated module that securely forwards the detected alerts to Elasticsearch.

Wazuh comes with a default group of rulesets, in which alerts are triggered on the selected endpoints. These rules can be further and subjectively enhanced, depending on the system's needs. Moreover, SIEM consists of the ELK-STACK with specialized features depending on the system's needs. ELK-STACK consists of:

- **Elasticsearch**: Elasticsearch is a distributed search and analytics engine based on Apache Lucene. Elasticsearch is a NoSQL database. After adding data, actions such as full-text searches, search by field, search multiple indices, aggregate results, and more can perform
- **Logstash:** Logstash, as a data pipeline, provides a broad array of input, filter, and output plugins for collecting, enriching, and transforming data from a variety of sources
- **Kibana**: Kibana is an open-source data visualization dashboard for Elasticsearch, with a Wazuh UI, embedded as a plugin. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster
- **Beats**: Beats are shippers that get and deliver data from distinct sources (e.g Metricbeat)
    - **Metricbeat**: This agent comes with internal modules that collect metrics from services and statistics for every process running on the systems.
    - **Auditbeat**: This agent collects logs directly from the Linux and Unix Kernel, by using the audit daemon. Can be easily expanded with rules and highly valuable information in a security context.
- **Suricata**: It is an endpoint agent which is installed in the monitored system and detects suspicious Network Activity

A typical implementation and deployment of the SIEM SOLUTION, dockers, containers, and images can be used to adapt and customize the aforementioned features via environmental variables, volumes, scripts, and other adaptations. A minimum installation of the SIEM solution should have:

- Division of two Clusters, one Wazuh cluster with master and worker nodes, and one elastic cluster with three nodes.
- Agent configurations in endpoints such as laptops and servers in order to monitor them
- Creation of necessary certificates (such as SSL certificate)
- Establishment of Communication between components through Logstash and Filebeat.
- Installation and configuration of MetricBeat, Suricata agents, and communication via Filebeat,
- Installation and configuration of Kibana

The goal is to detect any abnormal behaviour from the endpoint, that is monitored.

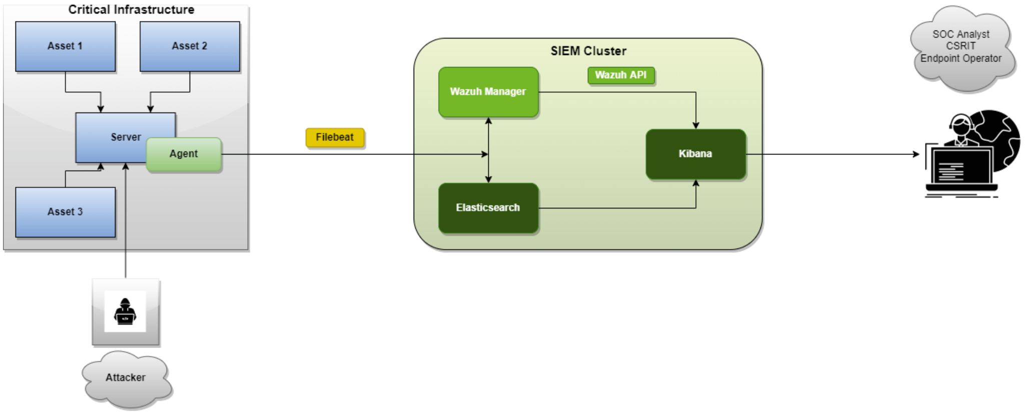


Figure 66 - Logs, Events & Alerts from the Infrastructure Endpoint to SOC analysts

The main capabilities of the SIEM solution are the following:

- **Log Data collection:** This feature is the real-time process of getting logs and events generated by the monitoring endpoints, where the agents are installed.
- **Distributed Data Storage:** SIEM provides distributed data storage by using Elasticsearch. SIEM uses Elasticsearch to store the log data.
- **Integrity Monitoring:** The File Integrity Monitoring is located in the monitoring endpoint via the Wazuh agents, where periodic scans are running inside specified directories, in order to trigger alerts when these files are modified.
- **Secure Authorization**: SIEM uses Role-based access control (RBAC) in order to secure the system. Role-based access control (RBAC) refers to the idea of assigning permissions to users based on their role within an organization. It provides fine-grained control and offers a simple, manageable approach to access management that is less prone to error than assigning permissions to users individually.
- **Vulnerability Detection:** SIEM is capable to detect vulnerabilities in the applications installed in agents using the Vulnerability Detector module. This software audit is performed through the integration of vulnerability feeds indexed by Canonical, Debian, Red Hat, and the National Vulnerability Database.
- **Incident Response (Countermeasures):** SIEM has enabled the Active Response to well-known attacks. Furthermore, the collected information on the incidents firing a rule triggers an Active Response (e.g., host-deny, firewall-drop, etc.).
- **Alerting:** Alerting provides the capability to take action based on changes in the data.
- **Visualization:** The Visualization component of SIEM, based on Kibana, provides an advanced way to visualize and analyse SIEM alerts stored in Elasticsearch.

The SIEM solution could be a part of a cyber security solution in critical infrastructures because Critical Infrastructures rely on distributed communication, which opens various cybersecurity risks. As a result, the SIEM solution could be capable of addressing several critical aspects of critical infrastructure, using the presented components, and their features, evolving, depending on the new needs, and finally delivering safety to each sector.

To conclude, the SIEM solution provides a holistic and all-around approach to alerting, monitoring, detecting, and actively responding to cybersecurity crime in critical infrastructures. SIEM solution could be capable of addressing several critical aspects of critical infrastructure, providing valuable defensive capabilities on several essential services like Generation/ Production, Transmission, Distribution, Management of the critical infrastructure, Storage facilities, etc.

7.9 Advanced Combined Cyber and Physical Threats

7.9.1 Visible and Emerging Vulnerabilities in Critical Energy Infrastructures

Visible and Emerging Vulnerabilities in Critical Energy Infrastructures by G. Stergiopoulos (Univ. of the Aegean), D. Gritzalis (Athens Univ. of Economics & Business)

Critical Infrastructures are defined as the “asset, system or part thereof located in EU Member States essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions” (Council of the European Union 2008). Critical Energy Infrastructures (CEIs) emphasize on the provision of essential services and continuity. CEIs in general support all other infrastructures in every societal aspect. The Industry 4.0 evolution along with its IoT wave of devices has greatly augmented the abilities to monitor and operate CEIs. For operators of critical infrastructures in the Gulf Cooperation Countries (GCC), Industry 4.0 solutions provide a wealth of benefits, including enabling both remote monitoring and remote outages, and facilitating greater power plant optimization. This includes optimization in storage capacity, reducing fuel consumption, and lowering NOx gasses and CO2 emissions and less spending on maintenance.

Yet, this digital evolution exposes Operational Technology (OT) infrastructures to multiple new attack surfaces and vectors [Siemens2021]. Reports from numerous international bodies and organizations state that, even though attacks on interconnected industrial systems can lead to incidents with severe economic and societal impact, still the security readiness and resilience of such infrastructures is considerably low.

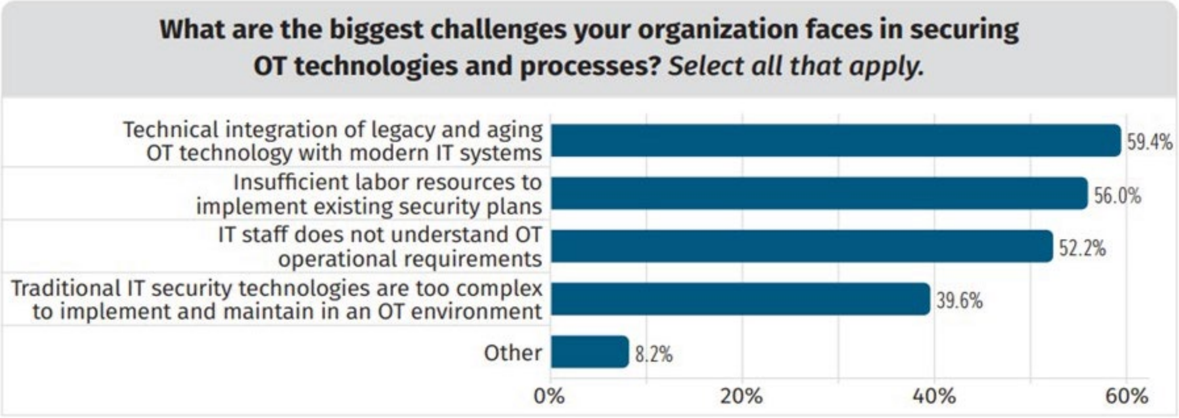


Figure 67 - SANS Survey 2021 - OT ICS Cybersecurity Nozomi Networks [SANS2021]

In our paper [StergiopoulosIEEE2020] we focused on analysing and classifying such types of known and existing cyberattacks, along with emerging types of attacks in CEIs that had or may have extensive or severe impact either to society or to the industry. We also took into consideration interconnected infrastructures often supporting other infrastructures that may have consequently been affected by such attacks. We relied on the Common Attack Pattern Enumeration and Classification (CAPEC) and MITRE ATT&CK taxonomies to introduce basic attack types for energy systems and developed a taxonomy of vulnerabilities per layer specifically for oil and gas infrastructures that can also be applied to any energy infrastructure. This culminated in an extended catalogue of real attacks, along with a methodology for impact analysis that utilizes the above-mentioned taxonomy and an impact assessment method to assess real attacks on Energy Infrastructures.

Attacks analysed in this paper mostly referred to closed-loop control systems, also known as feedback control systems. Such systems implement one or more feedback loops between input and output data to support automatic decision making. This means that parts of the output data are fed back to the monitoring and control system as input to form a part of the systems decision-making algorithm. Feedback control systems are designed to automatically achieve and maintain desired infrastructure states without manual intervention. Closed-loop SCADA systems imply that a highly configurable set of industrial software applications is used to support the management of processes in production.

Our analysis concluded that, a decade ago, most security weaknesses stemmed from the lack of basic security controls, even in critical systems. Even though CPS in the O&G sector have come a long way and nowadays most infrastructures follow basic cybersecurity concepts, it is still evident that most security weaknesses stem from poor security designs, lack of systematic use of information security management systems, as well as critical dependencies of equipment to third-party components and services, mainly telecoms. Most attack techniques used by threat actors against O&G CPS follow the statistics of regular ICT systems. They can be properly mitigated to a degree through the implementation of controls and standardized procedures documented in relevant best practices and standards. The fact that most infrastructures lack basic security procedures and controls affect the number of vulnerabilities present and the severity of potential attacks. This is supported by the fact that most worst-case scenario attacks that have happened involved critical systems and procedures that were insecurely interconnected to remote networks through telecom or third-party services. Also, proper network segregation and isolation of critical machinery and procedures seems to be a very effective way to reduce the number of vulnerabilities and attack paths for adversarial groups. Network monitoring seems ineffective due to the high number of false-positives and the distributed nature of processes in the O&G infrastructure. Instead, monitoring third-party services and isolating critical equipment has literally saved operators, as documented in Iran and the US. Employee awareness is one of the top issues in ICS security and seems to be as important for the O&G sector. Email phishing and information spoofing seems to be the most frequent attack techniques. One of the most alarming issues in O&G systems is the extended and regular use of legacy equipment and software in CI. Although operators seem to be in a process of updating systems and services, still many infrastructures deploy old components that have either no support (end-of-life) or limited ratios of patches issued per vulnerabilities detected [StergiopoulosIEEE2020].

Finally, another type of attack was highlighted by researchers back in 2018. Authors published alarming findings on mapping entire infrastructures and building cyberattacks offline from the ground up, using just public information [Maniatakos 2019]. Their research demonstrated back in 2018 that a real, large-scale power system can be remodeled offline, by leveraging OSINT resources to construct the power system model, validate it, and finally process it for identifying its critical locations. Authors demonstrated the feasibility of conducting elaborate studies leveraging public resources and organizing cyberattacks step by step using public data [Maniatakos 2019].

These trends are increasing at an alarming rate, and without proper mitigation and awareness, it is only a matter of time before we witness major CEI disruptions due to cyberattacks that may have international impact.

7.9.2 Modeling cyber and physical threats in IT&OT integrated systems

Modeling cyber and physical threats in IT&OT integrated systems by Aida Akbarzadeh and Sokratis Katsikas, Norwegian University of Science and Technology - NTNU

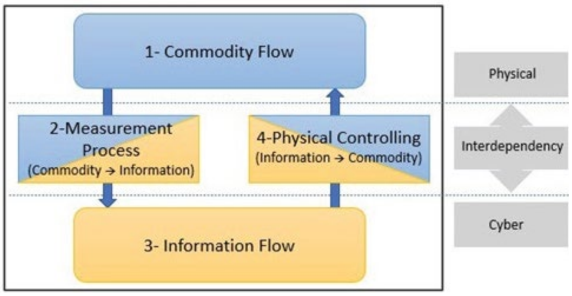
Cyber-Physical Systems (CPSs) are systems that integrate computation, communication, and controlling capabilities of Information and Communication Technology (ICT), with traditional infrastructures. This integration facilitates the monitoring and controlling of objects in the physical world as one of the essential requirements of different Critical Infrastructures (CIs), such as manufacturing, healthcare, transportation and the energy sector, to name a few. However, this integration has significantly increased the number of connections among the system components, and this in turn has expanded the attack surface of CIs and has led to making possible complex cyber, and cyber-physical attacks such as Stuxnet and the attacks against the Ukraine's power grid. Cyber-physical attacks have highly increased in recent years in numbers and intensity.

Interactions within a CPS can be classified to cyber–physical, physical–cyber, cyber–cyber, and physical–physical; this also implies that different types of dependency exist in CPSs. As a result, one may attack a CPS in a variety of ways. Nevertheless, not all aspects of cybersecurity in CPSs have received equal attention; the focus has mainly been on information security, protecting access, and ensuring secure delivery of packets, rather than on securing process operations.

The integration of Information Technology (IT) and Operational Technology (OT) causes operators to lose a comprehensive understanding of functions and interdependencies within a CPS, and this may lead to incomplete risk assessment. Moreover, IT and OT experts normally utilize different system models; this may infer different views of the same system. To tackle this challenge, it is required to develop a generic, yet easy to understand model to represent physical and logical facets as well as the interactions within the system components. This will enable both IT and OT experts, and in general members of a cybersecurity team with different backgrounds, to work on the same model and will allow them to identify and predict new complex cyber-physical attacks.

In our paper [Akbarzadeh 2022] we use bond graphs (BGs) to create unified IT&OT models of CPSs. A BG is a graphical representation of a physical dynamic system in the form of a directed graph. A BG is composed of *bonds (edges)* and *elements*. BG modeling is based on the power transfer principle between the different components of a system, since in each energy domain, the amount of power transferred is equal to the product of two physical quantities, i.e., Power = Effort × Flow. Therefore, the physical interaction among components of a system is done by the allocation of Effort (e) and Flow (f) variables on them. In a BG, each bond represents the power exchange between the connected elements. In other words, bonds represent the bilateral signal flow of the power-conjugate variables *effort* and *flow*.

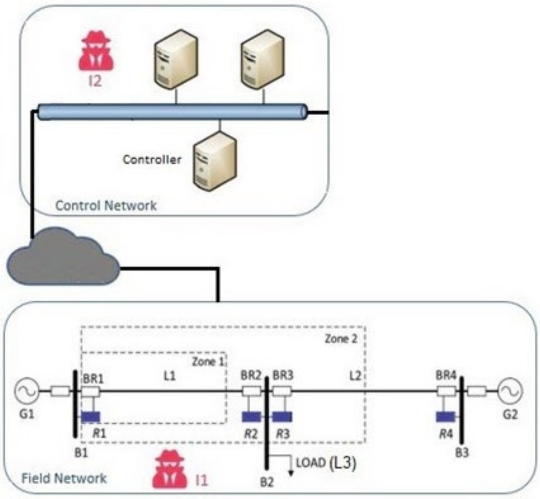
To model a CPS based on the BG approach, it is required to expand the approach to include cyber aspects of CPSs as well. To this end, we need two additional types of flow to model CPSs, namely *commodity flow* and *information flow*. The figure below demonstrates the flows and interactions within a CPS. The method we propose for modeling a CPS using a BG works in six steps, as follows:


1- Commodity Flow
2-Measurement Process (Commodity → Information)
4-Physical Controlling (Information → Commodity)
3- Information Flow
Physical
Interdependency
Cyber

1. Model the system
2. Attach the causal strokes (these indicate the direction of each flow variable)
3. Select the target element (X_i).
4. Extract the characteristics of the target element.
5. Write the constitutive equations.
6. Investigate possible combinations of faults and cyber-attacks.

In [Akbarzadeh 2022] we applied the proposed method to detect cyber physical attacks in a typical power system, shown in the figure below. This system consists of two network zones: a field network, and a control network to control the system. The field network is a three-bus two-line transmission system that is a modified version of the IEEE nine-bus three-generator system and includes several components. G1 and G2 are power generators, L1 and L2 are transmission lines, BR1 through BR4 are circuit breakers and R1 through R4 are relays. Each relay includes integrated phasor measurement unit (PMU) functionality and can trip and open the related breaker when a fault occurs on a transmission line. Operators are also able to manually issue commands to each relay to trip and close the corresponding breaker. The same figure also depicts potential locations for the presence of an insider attacker in the system.

By applying the proposed method, we were able to investigate different cyber-physical attack scenarios on selected elements, and also to identify additional possible such attack scenarios. According to the proposed six-step method, one can follow the sequence of interactions based on the topological parts of the model and utilize corresponding equations to investigate dependencies and relations between the components of a CPS to extract potential fault points, attack surfaces, and the consequences of attacks. Considering the numerous components of large-scale CPSs, this investigation begins with the most critical components ranked in the list of target components that contribute to the optimization of the analysis. Modeling a CPS based on its fundamental object that represents the process physics of the system along with the cyber layer will help operators and the security team to discover potential complex attacks. The proposed approach can also contribute to sensitivity analysis of the interactions and system components in case of faults and attacks.



8. Concluding Remarks and Planning

8.1 Closing Remarks

Giannis Skiadaresis - Coordinator of Resilient Infrastructure Research (INFRA) / Unit F2 - Security Research and Innovation, DG HOME

Security research is playing 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 and complement other instruments that are used by the Commission to facilitate exchanges on innovation in security among relevant stakeholders, most notably the Community for European Research and Innovation for Security (CERIS). 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.

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. 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 at a very high-level and the process is already steered. Therefore, we need to speed up our efforts in order to protect the citizens and make our vital infrastructures more resilient.

8.2 Conclusions and Planning

8.2.1 Day 1

Conclusions and Collaboration Planning of Day 1, 27-04-2022

Session chair: Habtamu Abie, Norsk Regnesentral

1) Summary

It looks like we've come to the last session and I think we've covered everything on the agenda: Now we had (i) Welcome and opening remarks, (ii) a Keynote on Cybersecurity investments and good practices for cyber risk management in critical infrastructure, (iii) Two sessions on “The results of EU research on CI protection”, each presenting 8 projects and 5 projects, respectively, (iv) A panel discussion on Cybersecurity and the NIS2 Directive: regulatory aspects and sectoral perspectives, and (v) A thematic presentation on Ethical and legal aspects of cybersecurity.

2) Planning

Now we had all these nice presentations about common topics we foresee that the ECSCI Cluster can take up as future common activities. Example: a methodology for CI resilience, and Risk Assessment by Rita, Ganesh, and Gabriele. A question was raised: how to stimulate the uptake of project results and exploit synergies for building upon? It was made clear that the ECSCI cluster also serves as collaborative platform projects should collaborate more closely. These questions were also raised and discussed: Would you propose a follow-up workshop 3rd ECSCI Workshop? If so, who would be interested in joining the organizing committee? It was highly encouraged to use the publication channel of the CPS4CIP 2022 workshop, and more emphasis was put on the preparation of “Consolidated proceedings of 2nd ECSCI workshop” based on the written contributions from the presenters.

3) Conclusions

I guess that will be all for today. If no one has anything else to add, then I think we wrap this up. I personally wish to express my gratitude to you all for joining the 2nd ECSCI workshop and sharing your experiences and thoughts.

8.2.2 Day 2 and Day 3

Conclusions and Collaboration Planning of Day 3, 29-04-2022

Session chair: Habtamu Abie (Norsk Regnesentral), and Ilias Gkotsis, Satways Ltd, Organizing committee members

1) Summary

Now we've come to the last day and final session, I think we've covered everything on the agenda, we had (i) Welcome and opening remarks by Giannis Skiadaresis from DG Migration and Home Affairs, Unit B4 - Innovation and Security Research, (ii) Keynote on “The evolution of security and resilience of critical infrastructures in a challenging environment by Georgios Giannopoulos, JRC, which emphasized on the main key takeaway that there is a new way to do policy and research due to the consideration of security and resilience of CI as part of a bigger ecosystem, and (iii) Common Thematic Presentations, 17 presentations distributed over the following 5 sessions: Standards and regulations (4 presentations), Platform for cascading effects (4 presentations), Safety and security, a holistic approach (3 presentations), Cybersecurity awareness (2 presentations, 1 presenter didn’t show up), and Cyber and physical threats (3 presentations).

2) Planning

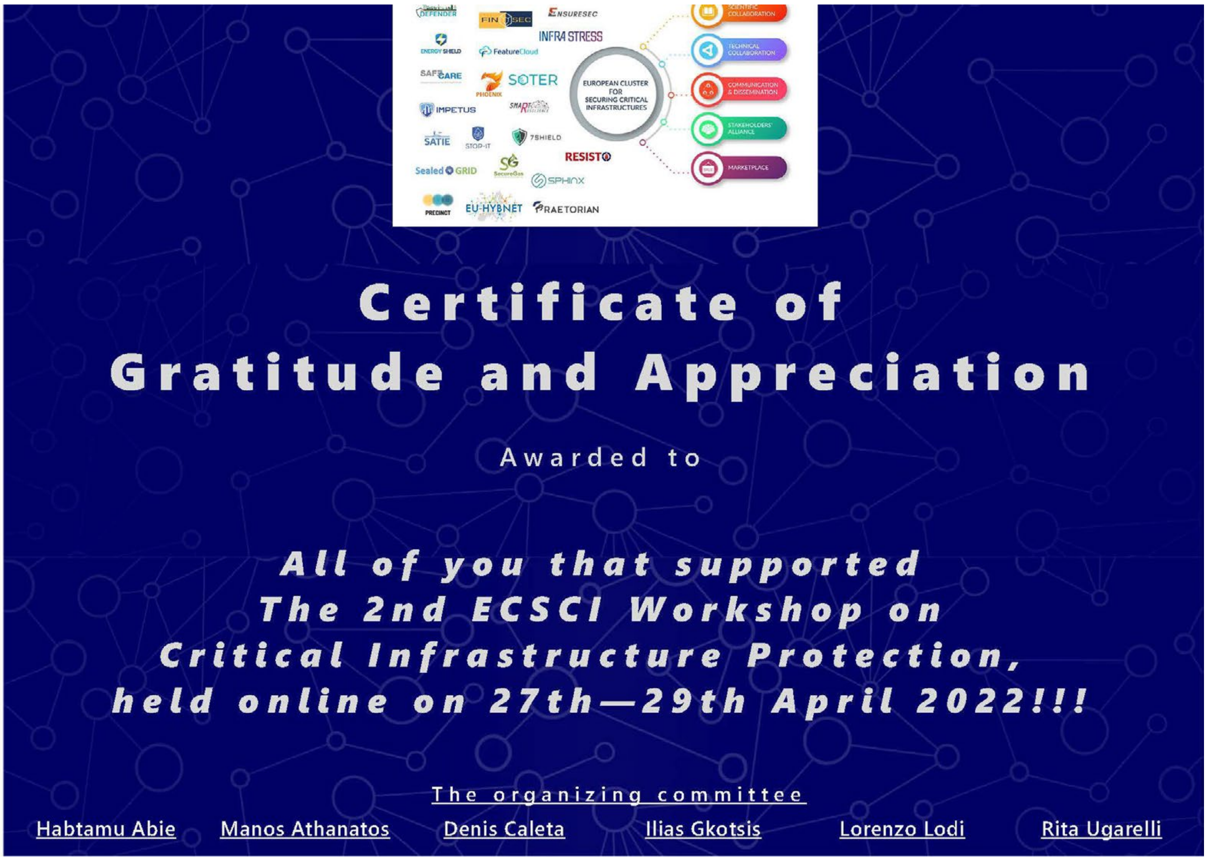
EU regulations and policy documents are already out there, for cyber-physical and hybrid threats (emerging threats that need more attention now). Research is a tool that brings together knowledge and expertise, in benefit of secure CIs and resilient communities. ECSCI is an initiative working in this direction, and synergies among its members are of high importance, so that it brings to the forefront the needs and requirements of this domain, but also provides lessons learned and recommendations. Following activities of ECSCI in this direction is the 3rd CPS4CIP 2022 is the next clustering/dissemination activity in which you are all invited and encouraged to participate and share findings/results, Submission deadline: 03.07.2022**.** Collaboration with EU organizations and agencies is another part that has been underlined and has been initiated through ECSCI, e.g., with ECSO, joining forces on policy documents. A final question was raised: Any views and feelings about the 2nd ECSCI workshop from any of the moderators, presenters, and/or audience? Positive, encouraging, and instructive feedback was given from the audience and continuation of the workshop was highly encouraged. In closing, the preparation of consolidated proceedings of the workshop was reiterated, stating also that we are looking forward to the ECSCI next event, and that the support of you all is needed, given that enhancing resilience, is a team effort. We are also looking for the start of EU-CIP (European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection)!

3) Conclusions

We guess that will be all for today, if no one has anything else to add, then we think we wrap this up by wishing to express our gratitude to you all for joining the 2nd ECSCI workshop and sharing your experiences and thoughts. Bye!

8.3 Concluding Remarks

The 2nd ECSCI Workshop on Critical Infrastructure Protection and Resilience came to its end. The organizing committee would like to say many thanks to all of you for your kindness and efforts to participate in this workshop and for getting along with the tough schedules. Special thanks to the EC for the encouraging and instructive opening and closing remarks, three keynote speakers for their stimulating talks, twenty-one project presenters, two roundtable and panel discussion panellists, and twenty-one thematic presenters for their excellent presentations.


DEFENDER
FINSEC
ENSURESEC
INFRA STRESS
ENERGY SHIELD
FeatureCloud
SAFECARE
PHOENIX
SOTER
IMPETUS
SMART RESILIENCE
SATIE
STOP-IT
7SHIELD
RESISTO
Sealed GRID
SecureGas
SPHINX
PRECINCT
EU-HYBNET
PRAETORIAN
EUROPEAN CLUSTER FOR SECURING CRITICAL INFRASTRUCTURES
SCIENTIFIC COLLABORATION
TECHNICAL COLLABORATION
COMMUNICATION & DISSEMINATION
STAKEHOLDERS' ALLIANCE
MARKETPLACE

Certificate of
Gratitude and Appreciation

Awarded to

All of you that supported
The 2nd ECSCI Workshop on
Critical Infrastructure Protection,
held online on 27th—29th April 2022!!!

The organizing committee

Habtamu Abie Manos Athanatos Denis Caleta Ilias Gkotsis Lorenzo Lodi Rita Ugarelli

Figure 68 - Certification of Gratitude and Appreciation

Acknowledgements

Part of this work has been carried out in the scope of the ANASTACIA (contract number 731558), CONCORDIA (contract number 830927), CyberSANE (contract number 833683), CyberSEAS (contract number 101020560), FeatureCloud (contract number 826078), EnergyShield (contract number 832907), ENSURESEC (contract number 883242), EU-HYBNET (contract number 883054), FINSEC (contract number 786727), IMPETUS (contract number 883286), InfraStress (contract number 833088), PANOPTIS (contract number 769129), PHOENIX (contract number 832989), PRAETORIAN (contract number 101021274), PRECINCT (contract number 101021668), RESISTO (contract number 786409), SAFECARE (contract number 787002), SATIE (contract number 832969), SealedGRID (contract number 777996), SecureGas (contract number 833017), SmartResilience (contract number 700621), SPHINX (contract number 826183), STOP-IT (contract number 740610), and 7SHIELD (contract number 883284) projects, which are co-funded by the European Commission in the scope of its H2020 program. The authors and editors gratefully acknowledge the contributions of the funding agency and of all the project partners. In closing, the editors wish to thank all the authors for their insights and excellent contributions to this report.

References

[Adhikari 2020] S. Adhikari and C. Davis, 2020. Reinforced learning and robotic automation based Cybersecurity. In *AIAA AVIATION 2020 FORUM* (p. 2929), doi: 10.2514/6.2020-2929.

[AI Act 2021] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts Com/2021/206 Final

[Akbarzadeh 2022] A. Akbarzadeh and S. Katsikas, "Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems," in IEEE Open Journal of the Industrial Electronics Society, vol. 3, pp. 318-328, 2022, doi: 10.1109/OJIES.2022.3178834.

[Aware] Be Cyber Aware videos - Cybercrime Awareness Training, https://www.youtube.com/channel/UCSAcOdvaGAU3q4PffI1lYDQ

[Biasin 2021) E. Biasin, 2021. The NIS2 proposal: Which regulatory challenges for healthcare cybersecurity? CITIP Blog. https://www.law.kuleuven.be/citip/blog/the-nis2-proposal-which-regulatory-challenges-for-healthcare-cybersecurity/

[Biasin 2022] E. Biasin and E. Kamenjašević, 2022. Cybersecurity of medical devices: New challenges arising from the AI Act and NIS 2 Directive proposals. International Cybersecurity Law Review, 3(1), 163–180. https://doi.org/10.1365/s43439-022-00054-x

[Bing 2021] C. Bing and S. Kelly, 2021. ‘Cyber attack shuts down U.S. fuel pipeline “jugular,” Biden briefed’, Reuters, May 08, 2021. Accessed: Mar. 19, 2022. [Online]. Available: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

[CEN-CENELEC-ETSI 2012] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Reference Architecture, November 2012, https://energy.ec.europa.eu/document/download/9ddd45d7-52eb-4541-85e4-ea58cfe9089b_en?filename=xpert_group1_reference_architecture.pdf

[CISA 2021] Critical Infrastructure Control Systems Cybersecurity Performance Goals and Objectives, https://www.cisa.gov/control-systems-goals-and-objectives, as of 9/21/2021

[CONCORDIA] CONCORDIA [project’s website]. Accessed at www.concordia-h2020.eu.

[CONCORDIA 2018] CONCORDIA, 2018. Deliverable D4.3: 3rd Year Report on Cybersecurity Threats. See section 6.2 and Appendix B. Accessed at concordia-h2020.eu.

[CORDIS] CORDIS, Cyber security cOmpeteNCe fOr Research anD InnovAtion (CONCORDIA). Grant agreement ID: 830927. Part of H2020-EU.2.1.1. - INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT) . Accessed at CORDIS.europa.eu.

[Dembosky 2021] L. Dembosky, A. Gesser, H.J. Brehmer, and A.S. Gutierrez, Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released by CISA and NIST, October 8, 2021, https://www.debevoisedatablog.com/2021/10/08/emerging-cybersecurity-standards-for-critical-infrastructure-lessons-from-recent-goals-released-by-cisa-and-nist/

[DHSNIST 2021] DHS, NIST Coordinate in Releasing Preliminary Cybersecurity Performance Goals for Critical Infrastructure Control Systems, https://www.nist.gov/news-events/news/2021/09/dhs-nist-coordinate-releasing-preliminary-cybersecurity-performance-goals, September 23, 2021

[ECB 2018] ECB report shows a fall in card fraud in 2016, 26 September 2018, https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180926.en.html

[Ecom 2019] Ecommerce News, Ecommerce in Europe: €621 billion in 2019, June 11, 2019, https://ecommercenews.eu/ecommerce-in-europe-e621-billion-in-2019/

[Ecom 2021] Ecommerce News, European ecommerce grew two- to threefold amidst pandemic, May 5, 2021, https://ecommercenews.eu/european-ecommerce-grew-two-to-threefold-amidst-pandemic/

[ENISA 2021] ENISA Report - Cloud Security for Healthcare Services, January 18, 2021, https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

[ENISA-1] ENISA Report - Good practices for the security of healthcare services, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health/good-practices-for-the-security-of-healthcare-services#/

[ENISA-2] ENISA Report - Cyber risk management for ports, https://www.enisa.europa.eu/cyber-risk-management-for-ports#/

[ENISA 2021-2] ENISA Report - Railway Cybersecurity - Good Practices in Cyber Risk Management, November 25, 2021, https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management

[ENISA 2022] ENISA Report - Zoning and Conduits for Railways, February 28, 2022, https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways

[ENISA 2022-2] ENISA Interoperable EU Risk Management Framework: Methodology for and assessment of interoperability among risk management frameworks and methodologies, Jannuary 2022, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework/@@download/fullReport

[ESET 2022] ESET research, Industroyer2: Industroyer reloaded, 12 Apr 2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[ESPO 2021] European Sea Ports Organisation, Position of the European Sea Ports Organisation on the NIS2.0 proposal, p.2. Available at: 2021.03.10 Position of the European Sea Ports Organisation on the NIS 2.0 proposal_1.pdf (espo.be)

[EU 2019] European Commission, MEMO - Frequently asked questions on Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union, 09 October 2020

[EU 2016] Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats, European Commission (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

[EU 2016] 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 repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016.

[EU-Hybnet 2020] EU-Hybnet H2020 project, Deliverable D3.3, First Report on Improvement, and Innovations (2020)

[Hauschild 2022] A.C. Hauschild et al., 2022. "Federated Random Forests can improve local performance of predictive models for various healthcare applications." Bioinformatics 38.8 (2022): 2278-2286.

[IMF 2017] IMF, WP/17/258, The Global FDI Network: Searching for Ultimate Investors, 2017

[ISO-IEC 2016] ISO/IEC 15946-1:2016, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General, 2016, https://www.iso.org/standard/65480.html

[Johnson 2021] S.D. Johnson, 2021. CISA Issues Preliminary Cross-Sector Cybersecurity Goals and Objectives for Critical Infrastructure Control Systems, September 22, 2021, https://www.akingump.com/en/experience/industries/energy/speaking-energy/cisa-issues-preliminary-cross-sector-cybersecurity-goals-and-objectives-for-critical-infrastructure-control-systems.html

[Kerner 2022] S.M. Kerner, 2022. Colonial Pipeline hack explained: Everything you need to know, 26 Apr 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

[König 2019] S. König, S. Rass, B. Rainer, and S. Schauer, 2019. 'Hybrid Dependencies Between Cyber and Physical Systems', in Intelligent Computing, vol. 998, K. Arai, R. Bhatia, and S. Kapoor, Eds. Cham: Springer International Publishing, 2019, pp. 550–565. doi: 10.1007/978-3-030-22868-2_40.

[Kostaridis 2017] A. Kostaridis et al, 2017. CIRP: A Multi-Hazard Impact Assessment Software for Critical Infrastructures, 2nd International workshop on Modelling of Physical, Economic and Social Systems for Resilience Assessment, 2017

[Kun, 2021] E. Kun, 2021. Strengthening the Supervision and Enforcement in the EU Cybersecurity Law: Are All Organisational Organizational Measures Created Equally? (June 15, 2021). Available at SSRN: https://ssrn.com/abstract=3933680 or http://dx.doi.org/10.2139/ssrn.3933680

[Maniatakos 2019] A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos, 2019. Open source intelligence for energy sector cyberattacks. In Critical infrastructure security and resilience (pp. 261-281). Springer, Cham.

[Markakis 2019] E. Markakis, Y. Nikoloudakis, G. Mastorakis, C.X. Mavromoustakis, E. Pallis, A. Sideris, N. Zotos, J. Antic, A. Cernivec, D. Fejzic, and J. Kulovic, 2019. Acceleration at the edge for supporting smes security: The fortika paradigm. IEEE Communications Magazine, 57(2), pp.41-47, doi: 10.1109/MCOM.2019.1800506

[Mavroeidis 2020] V. Mavroeidis and J. Brule, 2020. "A nonproprietary language for the command and control of cyber defenses–openc2." Computers & Security 97 (2020): 101999.

[Nasirigerdeh 2020] R. Nasirigerdeh et al., 2020. "sPLINK: a federated, privacy-preserving tool as a robust alternative to meta-analysis in genome-wide association studies." BioRxiv (2020).

[Nikoloudakis 2019] Y. Nikoloudakis, E. Pallis, G. Mastorakis, C.X. Mavromoustakis, C. Skianis, and E.K. Markakis, 2019. Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case. *Peer-to-Peer Networking and Applications*, *12*(5), pp.1216-1224., doi: 10.1007/s12083-019-0716-y.

[Nikoloudakis 2021] Y. Nikoloudakis, I. Kefaloukos, S. Klados, S. Panagiotakis, E. Pallis, C. Skianis, and E.K. Markakis, 2021. Towards a Machine Learning Based Situational Awareness Framework for Cybersecurity: An SDN Implementation. *Sensors*, *21*(14), p.4939., doi: 10.3390/s21144939.

[NIS 2021] NIS Investments Report 2021, https://www.enisa.europa.eu/publications/nis-investments-2021

[NIS 2018] NIS Cooperation Group, Reference document on security measures for Operators of Essential Services, CG Publication 01/2018, February 2018, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf

[NIS2 2016] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM/2020/823 final

[NSM 2021] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[OpenC2] OASIS Open Command and Control (OpenC2) TC, https://www.oasis-open.org/committees/openc2

[Polityuk 2017] P. Polityuk, O. Vukmanovic, and S. Jewkes, 2017. Technology News, January 18, 2017, https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

[RISE 2021] EU-HYBNET project, Deliverable D4.4, First Innovation Uptake, Industrialization and Research Strategy, by RISE (2021).

[SANS12021] M. Bristow, 2021. A SANS 2021 Survey: OT/ICS Cybersecurity, 2021, https://www.nozominetworks.com/downloads/SANS-Survey-2021-OT-ICS-Cybersecurity-Nozomi-Networks.pdf

[Siemens2021] Why energy companies must prioritize cybersecurity to leverage Industry 4.0, Siemens Energy, https://www.siemens-energy.com/mea/siemens-energy-in-middle-east/news/magazine/fully-benefit-from-industry-40-gccs-critical-must-ziad-al-sati.html

[Sofou 2017] S. Sofou, 2017. Innovation Management in Horizon 2020 Projects. Proceedings of the 14th International Conference on Nanosciences & Nanotechnologies, Thessaloniki, Greece, July 4th-7th, 2017

[SP 800-57 2020] SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General, May 2020, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[StergiopoulosIEEE2020] G. Stergiopoulos, D.A. Gritzalis, and E. Limnaios. "Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns." IEEE Access 8 (2020): 128440-128475.

[Zolotareva 2021] O. Zolotareva et al., 2021. "Flimma: a federated and privacy-aware tool for differential gene expression analysis." Genome biology 22.1 (2021): 1-26.

Catalogue of the projects participating in the 2nd ECSCI workshop

ANASTACIA project website - www.anastacia-h2020.eu

CONCORDIA project website - www.concordia-h2020.eu

CyberSANE project website - www.cybersane-project.eu

CyberSEAS project website - www.cyberseas.eu

FeatureCloud project website - www.featurecloud.eu

EnergyShield project website - www.energy-shield.eu

ENSURESEC project website - www.ensuresec.eu

EU project website -HYBNET – www.euhybnet.eu

FINSEC project website - www.finsec-project.eu

IMPETUS project website - www.impetus-project.eu

InfraStress project website - www.infrastress.eu

PANOPTIS project website - www.panoptis.eu

PHOENIX project website - www.finsec-project.eu

PRAETORIAN project website - www.praetorian-h2020.eu

PRECINCT project website - www.precinct.info

RESISTO project website - www.resistoproject.eu

SAFECARE project website - www.safecare-project.eu

SATIE project website - www.satie-h2020.eu

SealedGRID project website - www.sgrid.eu

SecureGas project website - www.securegas-project.eu

SmartResilience project website - www.smartresilience.eu-vri.eu

SPHINX project website - www.sphinx-project.eu

STOP project website - www.stop-it-project.eu

7SHIELD project website - www.7shield.eu

“Over the past decade, the EU has progressively tailored its research and innovation capacity to EU security policy priorities. This capacity plays a key role in addressing the current security challenges and is already helping us in finding solutions to several of the most pressing issue.” (EC staff working document “Enhancing security through research and innovation”, 2021) One of these security priorities is linked with strengthening the resilience of critical and digital infrastructures, which is now supported, at the policy level, by entering into force the two key directives of the EC, that of CER and NIS-2.

These two directives, but also recent attacks against critical infrastructures such as the acts of sabotage against the Nord Stream pipeline, underline the need for coordinated and integrated responses, not only at the policy level but also at the operational level through research and innovation outcomes (as indicated in the aforementioned EC staff working document), which must be disseminated and exploited further to the EU-funded projects’ frameworks or individual research studies’ reports, through raising awareness initiatives, such as the 2nd ECSCI Workshop on CIP.

In the frame of this workshop, the different approaches to security in several different industrial sectors (e.g. finance, healthcare, energy, transport, communications, water) were presented. 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 (related to security modelling, IoT security, artificial intelligence, combating hybrid threats, increased automation for threats detection, prevention and mitigation measures, information and knowledge sharing, etc.).

The workshop proceedings aim to share with scientists, experts, policymakers and other interested stakeholders in the field of critical infrastructure protection, resilience and security, the knowledge, outcomes and lessons learned, deriving from the keynote speeches, the twenty-one thematic presentations, and the panel discussions.

ISBN 978-3-95663-285-3

Steinbeis-Edition