

01

NEWSLETTER

IMPROVING RESILIENCE OF SENSITIVE INDUSTRIAL PLANTS &
INFRASTRUCTURES EXPOSED TO CYBER-PHYSICAL THREATS



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833088



Table of content

Page 3-4	Message from the project Coordinator By Lorenzo Sutton, Engineering Ingegneria Informatica
Page 5.	InfraStress in a Nutshell
Page 6-7	InfraStress demonstrations in operational environments By Eleni Psychia, Motor Oil Hellas
Pages 8-10	Smart detection tools: By Vinod Ahuja, Dr. Frucht Systems Ltd (DFSL)
Page 11.	Resilience-enhancing services: the organizational dimension By Renaud Vidal, ATRISC
Page 12.	InfraStress community enrollment campaign will start soon ! By Denis Čaleta, Institute for Corporate Security Studies
Pages 13-14	Recent and upcoming events
Page 15.	InfraStress Partners

MESSAGE FROM THE PROJECT COORDINATOR

*By Lorenzo Sutton
Engineering Ingegneria
Informatica*

To all of our **readers**, welcome to the 1st issue of the **InfraStress Newsletter**! InfraStress is a research project co-funded by the EC through the **H2020 Framework Programme** which brings together **27 international partners** from industry and academia addressing the security and resilience of Industrial Critical Infrastructure.

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

In the InfraStress project our value proposition is to improve the **security and resilience** of **Sensitive Industrial Plants and Sites (SIPS)**. These include petrol/chemical storage and processing sites, large manufacturing plants and connected infrastructure (such as water supply and municipalities). Our aim, in fact, is to provide **innovative tools** for such types of infrastructure embracing a **holistic** and **resilience-oriented** approach where one of the main features is to consider **cyber and physical security at the same level** with the objective to overcome the current ‘silo approach’. Indeed, we have fully entered the ‘digital everywhere’ age where everything is virtually controlled by a digital (i.e. computer) system: from our personal banking to our monthly gas bill, from opening a location entrance to a video-surveillance system, from a valve in an industrial machine to a sensor in a pipe system.

And in order to overcome this ‘monochromatic vision’ approach and provide adequate tools to SIPS in InfraStress we have decided to give a leading role to our **user partners**, trying to craft our innovative **technologies and solutions** (presented in the InfraStress in a Nutshell article) to support these actors in the **real world** addressing all of the challenges needed to improve their resilience, which is indeed already rather high in certain domains such as safety, in a bottom-up manner helping them decide which solutions to invest in and where. In fact, the **InfraStress solutions are being tested in 5 different Pilot scenarios** embracing a representative sample of European SIPS. ►

MESSAGE FROM THE PROJECT COORDINATOR

*By Lorenzo Sutton
Engineering Ingegneria
Informatica*

In this issue we present a contribution by our partner **Motoroil Hellas**, one of the leading petroleum companies in Europe, which in InfraStress is leading the overall pilot work, explaining some of the key features and approaches adopted in such a complex project to effectively demonstrate InfraStress in operational environments.

For our readers who are enthusiasts of technology and innovation we also feature an article by partner **DFSL**, a leading company in the development of **innovative detection tools**, where Smart detection tools are presented.

The COVID-19 pandemic and related crisis, we are hopefully starting to recover from, has highlighted on the one hand how all of our **infrastructure** at European (but even global) level is **actually interconnected**, meaning that issues at one point may propagate throughout the rest of the system (travel probably being one of the most affected sectors); and on the other hand it dramatically highlighted how much **a culture of resilience and risk management is needed**: today we need to be prepared, and prepare our infrastructure (and its people) to potential threats, sometimes unknown or unexpected. And in InfraStress we aim at endorsing a culture of participatory security, enabling to share effective risk-related information among relevant stakeholders and viewing **risk assessment** in an **interconnected and interdependent perspective**.

This culture obviously starts within each organisation, involving proactively all actors. The contribution from **ATRISC** – our partner expert in organizational reliability and crisis management – about Resilience-enhancing services: the organizational dimension examines some of the strategies able to improve **resilience at the organisational level**.

To fully create a culture of security we need an active and **interested community**, and therefore – as InfraStress has marked its first year of activity – we are having an **enrolment campaign**, which means you (as an expert, stakeholder or simply someone interested in security and resilience) can join our community! The campaign is presented by Prof. Denis Čaleta from the Institute for Corporate Security Studies.

Finally we have an overview of recent and upcoming events where InfraStress is involved.

I sincerely hope you will find this newsletter interesting and stimulating, and be sure to follow us on the project's official social channels in order to keep up to date with project developments and updates.

InfraStress in a Nutshell

- ▶ **Project name:** Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system
- ▶ **Project reference:** 833088 - Project type: Innovation Action
- ▶ **Call:** SU-INFRA01-2018-2019-2020 - Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe
- ▶ **Duration:** 2 years (1 June 2019 - 31 May 2021)
- ▶ **EU funding:** 8 M€
- ▶ **Consortium:** 27 partners of excellence from 11 countries with very cross-cutting and complementary competences and excellent track records, including 5 Sensitive Industrial Plants and Sites operators
- ▶ **Objectives:** InfraStress will develop TRL7 level methods and solutions. Addressing the current fragmentation of available security solutions and technology, InfraStress will provide 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
- ▶ **Expected impact:**
 - Assessing and modelling SIPS assets, vulnerabilities, combined cyber-physical-social risks and threats, thus generating a state-of-the-art knowledge for SIPS CIP
 - Driving business innovations in critical and sensitive industry and security sector by setting up and coordinating a Sensitive Industry Protection Stakeholder Group (SIP-SG)
 - Accelerating the growth of European security companies in the rapidly growing industrial C/P security markets
 - Creating a culture of security and training on our novel approaches to SIPS CIP in MSc and free Massive Open Online Course (MOOC) course.



InfraStress demonstrations in operational environments

Page 1/2

*by Eleni Psychia,
Motor Oil Hellas*

The time of the piloting and demonstration activities in the InfraStress project has come! Motor Oil Hellas will coordinate the detailed planning of tasks and activities, technical solutions, management of persons responsible for specific actions, and control of results.

It's a crucial period for the InfraStress Project. It brings pretty much most of InfraStress partners together and represents bridges between generating knowledge about Sensitive Industrial Plants Sites (SIPS) and or Critical Infrastructures (CI) and technological breakthroughs on the one hand, and industrial detection applications on the other.

The highlights of these activities are the learning processes taking place at and around Critical Infrastructures around Europe and how they contribute to reducing physical, cyber, and natural threats.

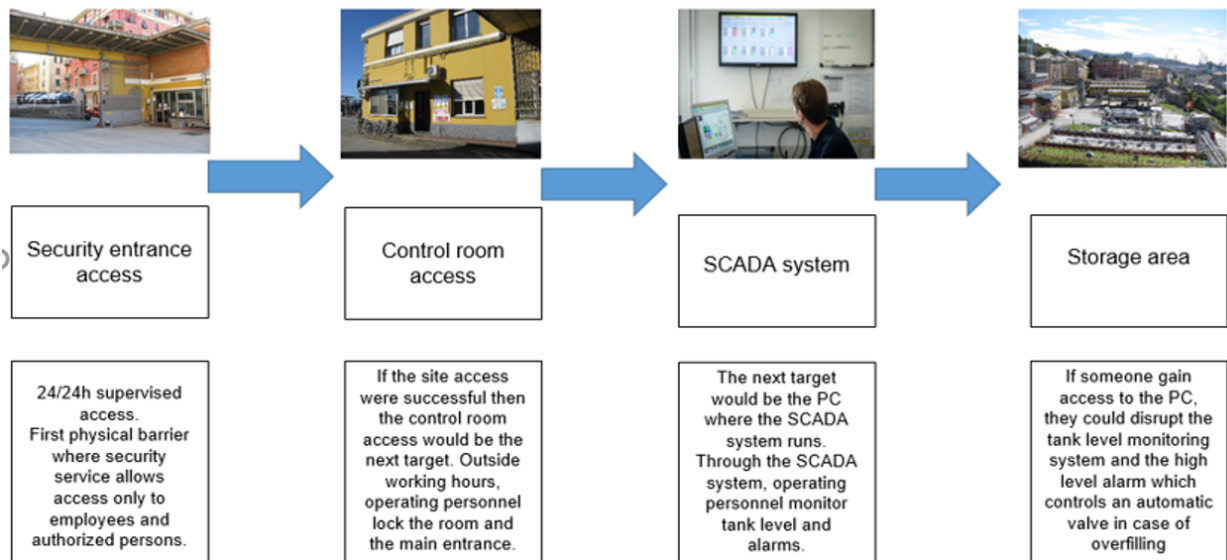
It also elaborates on the importance of actor facilities preconditions and on how tools and components provided by technical partners of InfraStress can improve SIPS and CI resilience and protection capabilities.

In the first steps, Motor Oil, as Lead Partner of the validation and demonstration of InfraStress in operational environments, gathered all the potential physical and cyber-attack scenarios emphasizing to specific vulnerable point(s) and the existing preventive countermeasures of each SIPS and CI participating in the project, based on the following demonstration case scenarios:

- Big Refinery (Motor Oil - Greece),
- Medical devices manufacturing Cyber/Physical protection (DePuy Synthes – Johnson & Johnson – Ireland),
- Chemical storage C/P protection (Attilio Carmagnani «AC» SpA - Italy),
- Cyber/Physical Protection and cascading effects and interdependency among CIs (Petrol, Luka Koper - Slovenia),
- User engagement in SIPS protection (Fisipe, Municip. of Barreiro - Portugal).

During the activities of defining the cyber scenarios, CI end users decided to be subject of a cyber-attack due to existing airgap measures. The attack scenario is unauthorized physical access to control rooms where the PLC/ESD/SCADA cabinets are located to take over the control from the operators to either block the operations in general or operate the plant out of the safe operational boundaries.





On the other hand, physical security countermeasures at the CI sites include many different layers of protection to simulate and test (site fence, entry control, guards, video surveillance etc.).

All these types of attack scenarios are real, but fortunately, the first versions of the Cyber and Physical threats detection tools are ready. Every device that will be available for demonstration can cover and identify real attack scenarios defined by SIPS & CIs, even natural threats via simulation systems. Based on the pilot scenarios, supporting partners of each SIPS & CI (SATWAYS, NOA, UTRC, STAM, ICSS, JSI, INOV) identified which tools are more appropriate for each pilot scenario.

Key Results up to now



Initial pilot scenarios defined



Components to Pilots Mapping



Working Groups Pilot-Component



T8.2

Preparation and execution plan of InfraStress pilots

To sum up, speaking on behalf of every pilot team, we are excited about this period of the project. This is not only because we have already seen the promising added value to our infrastructure but additionally, because our method of running the tasks was through relationships of trust. We saw the individual commitment to a group effort. This makes us firmly believe that InfraStress will complete the mission of identifying gaps in knowledge on threats to the critical infrastructure as well as improving the risk-assessment procedures. We are employing new knowledge on security procedures and systems, exploiting innovative solutions to enhance infrastructure protection, exchanging experiences between project partners & enhancing security awareness.

InfraStress develops the following tools and services up to TRL 7 for validation and demonstration on the five pilot sites described in the previous article.

DFSL brings several sensors and components:

- Perimeter Laser Fence Sensor for intrusion detection,
- Laser Fence Sensor for detection of objects thrown above a wall,
- 2- dimensional mini drone detector (for detection of intruding drone,
- 3- dimensional mini drone detector for detection of intruding drone,
- Flying Hunter Type B for neutralization of the intruding drone,
- Flying Watcher for aerial surveillance of intrusion on ground,
- Non-authorised people detector in a gathering of people.

United Technologies Research Centre Ireland (UTRC) provides tools for AI-based Physical Security Information Management that detects and diagnoses physical security events. On the one hand, this tool will allow detecting anomalies in real-time environmental sensor measurements (temperature, humidity, light, etc.) and generate spatial-temporal events describing those anomalies. On the other, this component will provide Access Control Management capabilities. In particular, this tool allows detecting anomalous access rights of employees to some areas of a building based on a static access policy database. This tool also allows identifying tailgating events in real-time based on streaming access logs collected by the card reader network.

National Observatory of Athens (NOA) addresses environmental monitoring at SIPS, in which earthquake monitoring and air quality monitoring are involved. For earthquake monitoring, NOA will exploit and make available the National Earthquake Detection Network and the National Atmospheric Monitoring Network data, in real-time, to complement Motor Oil Hellas local environmental monitoring systems. For air quality monitoring, gas emission, flow and concentration of oxygen, nitrogen oxides, sulfuric dioxide, and particulate matter will be detected, analysed and presented.

Ethniko Kentro Erevnas Kai Technologikist Anaptyxisa (CERTH) brings capabilities of events detection, anomaly detection, and object and concept detection. In event detection, both high-level and primitive semantic events of interest are identified. In anomaly detection, occurrences of interest that significantly vary from the usual/expected patterns are identified. In object and concept detection, a wide range of real-world objects or high-level semantic entities are detected.



CERTH is also responsible for providing metrics regarding the observed humans' behaviour and actions, in terms of:

- Human action recognition,
- Person re-identification to identify/track the presence of a human subject in different, sources that may potentially cause alerting event triggering,
- People counting.

Several working prototypes developed and evaluated by CERTH in relevant environments within several EU projects are appropriately extended and adapted to the particular domain of SIPS.

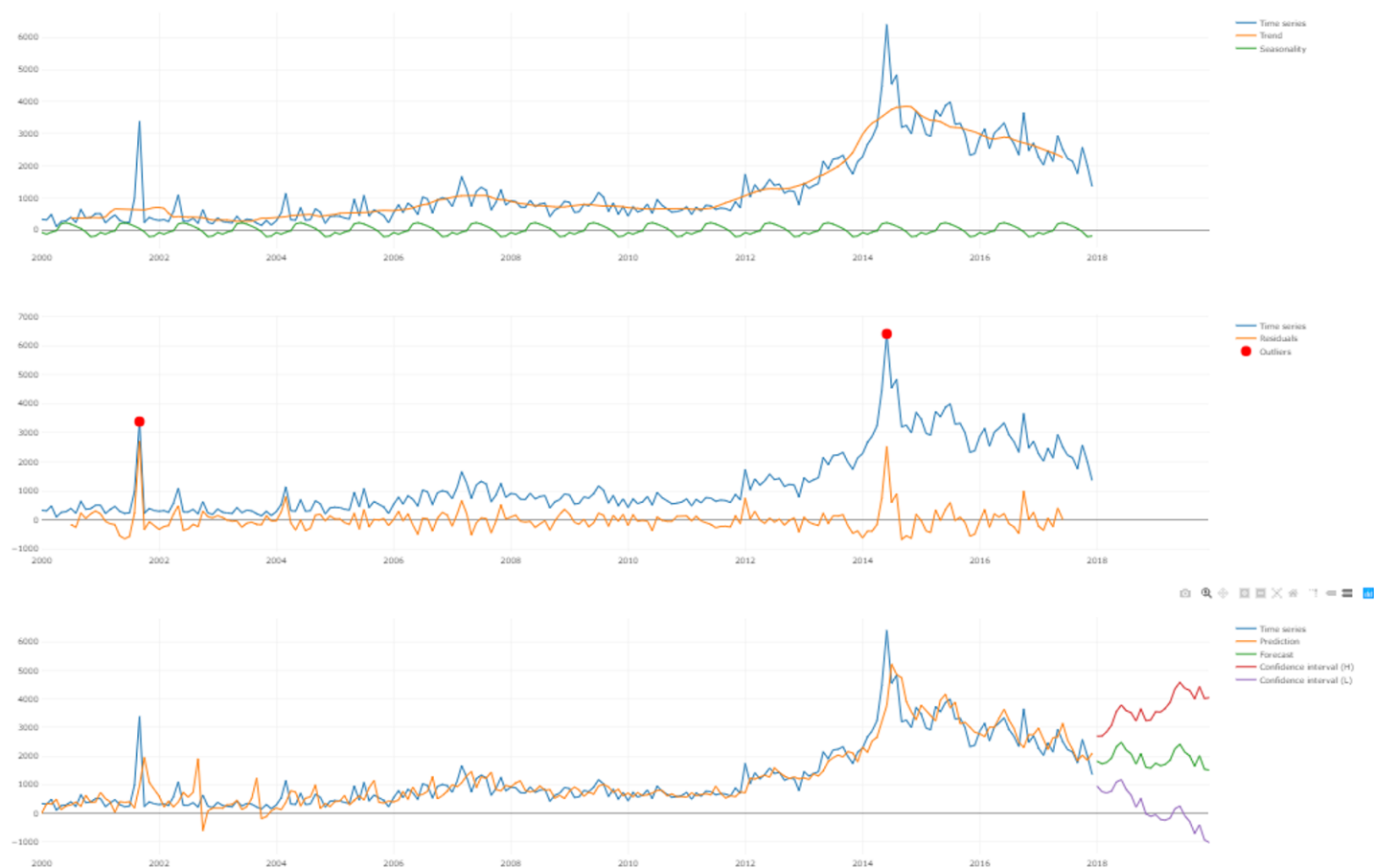
Consorzio Interuniversitario Nazionale per l'Informatica (CINI) provides a tool that monitors the compliance of implemented cybersecurity processes concerning behaviours prescribed by SIPS business processes. CINI also brings a tool that analyses the traffic in Industrial Internet of Things (IIoT) and Supervisory Control and Data Acquisition (SCADA) networks to detect ongoing attacks or even anomalous behaviours. The device also handles protocols and systems specific of ICS installations and deal with new advanced threats such as Permanent Denial of Service (PDoS) or routing attacks to ad-hoc networks. In addition, CINI also integrates existing and novel cyber-physical detection systems and sensors. In this, a data model and API for the integration is to be provided. It enables efficient integration of new data sources and detection systems, by providing the framework with flexible and efficient data acquisition and pre-processing capabilities, for a broad set of data collectors.

Uniwersytet Technologiczno Przyrodniczy (UTP) brings a tool that performs effective anomaly-based intrusion detection in the application layer, providing scalability and specifically tailored for SIPS scenarios. It integrates Extreme Learning, Lifelong Learning, Evolutionary Algorithms, and other strategies combining both novel and time-proven approaches.

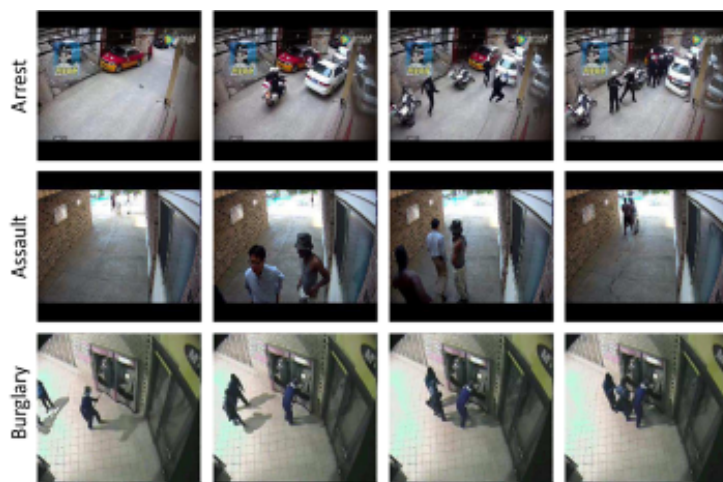
Instituto de NOVAS Tecnologias (INOV) develops apps that detect and report possible suspicious or concrete threats directly from users working inside the industrial plant or in its vicinity based on gamification techniques to foster user participation and based on crowd-sensing works on smart parking and transportation. The gamification approach increases participation from the population. INOV also brings a tool that monitors and detects the population's response to the information being published and can identify the dominant emotion occurring in social networks.

Engineering Ingegneria Informatica (ENG) brings tools for the detection of relevant security events info from Open-source intelligence and social media. The tool extracts near real-time information from public Web and social media about relevant events for SIPS and vicinity security. Prototypes developed in previous EU projects are adapted for detecting specific SIPS-related security events and relevant information.





Visualization of the TS temporal analysis results, including TS decomposition, prediction and anomaly detection



► Typical violent scenes from UCF-Crime dataset for anomaly detection



Visualization of attention maps (heatmaps) for different query positions (red points) in a non-local block on COCO object detection (In the same image, the attention maps of different query points are almost the same)

Resilience-enhancing services: the organizational dimension

by Renaud Vidal – ATRISC

A SIPS CI is a socio- technical system. As a result, its resilience does not only rely on technical devices, but depends significantly on organizational processes and especially on sense-making processes. These organizational processes enable employees to address the questions: “what is going on, what should we do about it”. They define the organizational ability to detect weak signals of unexpected events and emerging threats. In the framework of InfraStress, ATRISC has developed a robust and tractable assessment of this organizational dimension of SIPS resilience. The methodology leads to the assessment of 5 organizational traits: preoccupation with failure, reluctance to simplify, sensitivity to operations, deference to expertise, commitment to resilience.

For instance, the first resilience culture trait “preoccupation with failure” refers to the organizational ability to look at cues, pieces of information, indicators, partial available data with the underlying question: “are these the symptoms of a potential failure?” The absence of this cultural trait fosters the organizational tendency for complacency, a key contributor, for instance, to NASA’s challenger and accidents.

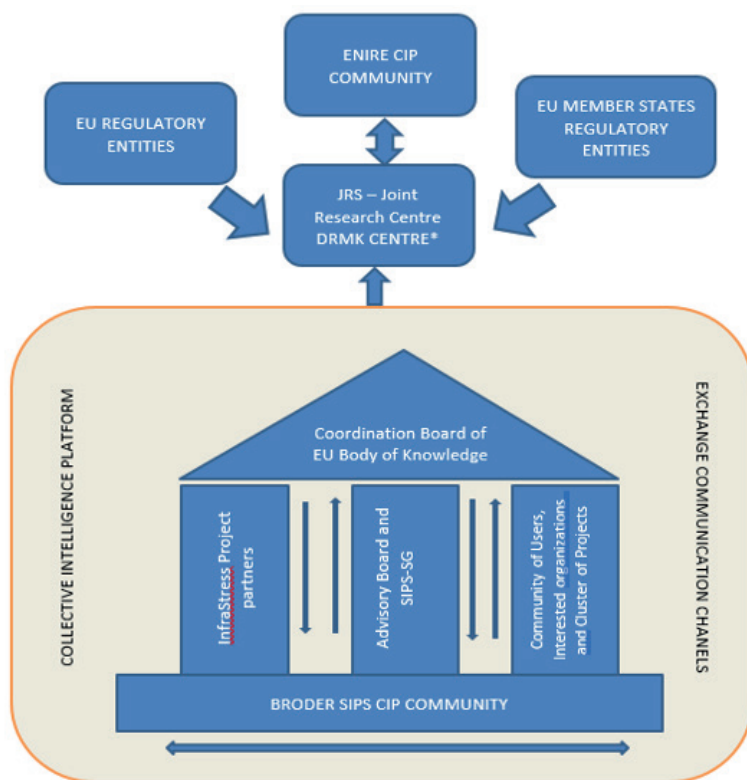
In one of the project’s use case scenarios, a SIPS has had a significant event in which an unauthorized person has entered the plant and gained access to the IT/OT facilities. Imagine that the company, to which the unauthorized person belongs, was required to address an urgent problem in the plant and that the person presented at the gate documentations that were somehow “ambiguous”. Many reasons are possible, for instance recent changes in validity statuses were not fully entered in the database but were transmitted to security personnel during the morning briefings only. The security employee under time pressure wrongly allowed the entrance of the person. He failed to remove the ambiguity of the documentation, for instance, by asking his supervisor, or by checking with a colleague. Imagine that this happened because of the degraded working relations between security agents or because of the fear of an excessive punishment by the supervisor. In this case, additional training of personnel will not solve the issue. Nor will any new technical device. This organizational issue must be addressed, and this involves looking at status changes processes, morning briefings, modes of supervision, working interactions, reward and punishment systems...

InfraStress community enrollment campaign will start soon !

By Denis Čaleta, Institute for Corporate Security Studies

The main intention of the InfraStress project is the co-creation of an EU body of knowledge on integrated cyber-physical protection of industrial sensitive sites and plants. This will be achieved by building an organizational network with related processes and procedures for creating collective intelligence in collecting, exchanging and processing new knowledge on SIPS. The InfraStress vision consists in fostering and supporting the creation of a culture of security and CIP for SIPS. This translates into the creation of study material, best practices, factsheets, guidelines related to cyber-physical protection of SIPS. The design and implementation of the content blends cyber and physical aspects in an integrated body of knowledge. The material will be available throughout a collective intelligence platform developed in the InfraStress project. Through this platform, we provide and support interactions, exchange and bottom-up co-creation of practices, and sharing of experience and knowledge. This should become a regular base for exchanging relevant information between different internal and external members of the network. To benefit from our network, don't hesitate to join our InfraStress community (www.infrastress.eu/infrastress-community)!

InfraStress community will benefit from the support of our Advisory Board, Sensitive Industry Protection Stakeholder Group (SIP-SG), and possible network connections between relevant EU initiatives and related H2020 projects or other expert communities. Alongside the InfraStress project community, these structures will have great importance for the effective exchange of expert information. The platform will be developed in coordination and synergy with the European Cluster for Securing Critical infrastructures (ECSCI) communities.



Organizational and procedural scheme of co-created EU Body of Knowledge

The European Cluster for Securing Critical infrastructures (ECSCI) workshop was held virtually 24-25 June 2020.

InfraStress is part of this first European Cluster for Securing Critical infrastructures, gathering interdisciplinary professional communities to debate on the protection of critical infrastructures in the domains of finance, healthcare, energy, air transport, communications, gas, and water. The workshop program included keynote speeches from the EC, ENISA, and ECSO, 10 H2020 projects results presentations, roundtable and panel discussions, and thematic presentations. InfraStress was extensively represented through the following interventions:

- Improving resilience of sensitive industrial plants & infrastructures by Lorenzo Sutton (Engineering),
- Could standardization break the silos approach in Critical Infrastructure Protection? Round table discussions facilitated by Denis Caleta (ICS-Institut),
- Indicators for assessing resilience of the European critical infrastructures: Wishful thinking vs. engineering challenge by Sasa Jovanovic (Risk-technologies),
- How to protect Industry 4.0 Sensitive Industrial Plants from cyber and physical attacks by Luigi Romano (University of Naples "Parthenope"),
- Legal and Ethical frameworks concerning cybersecurity of critical infrastructures by Elisabetta Biasin (KU Leuven).

European Cluster for Securing Critical Infrastructures - ECSCI



CPS4CIP'20, the first workshop dedicated to the cyber-physical security for protecting critical infrastructures to be held September 14 - 18, 2020

InfraStress supports CPS4CIP'20 which addresses the cyber-physical security of the following domains: finance, energy, health, air transport, communication, gas, and water. The conference will be entirely virtual. In addition to be part of the program committee, InfraStress members have submitted a paper entitled "Embedding situational awareness into risk and resilience management for critical infrastructures", authored by A. Jovanović, L. Sutton, B. Caillard, L. Romano and G. Giunta.

For more info, go to <https://sites.google.com/fbk.eu/cps4cip20>

InfraStress International Advisory Board Meeting

InfraStress International Advisory Board member are experts and stakeholders interested in providing advices and recommendations to InfraStress, supporting the definition of the framework and solutions. The board will convene early July. Its members are:

- Dr. Jörg Michael Bareiß, Energie Baden-Württemberg AG (EnBW AG)
- Prof. Walter Bogaerts, Catholic University of Leuven (KU Leuven), Departement of Materials Engineering (MTM)
- Mr. Rui Pestana, Rede Eléctrica Nacional (REN)
- Dr. Milan Tarman, National Security Office of Republic of Slovenia

InfraStress partners



www.infrastress.eu

Follow us

