

# *CYBERSANE*

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

## Contents

Editorial .....	2
CyberSANE Pilots .....	3
Final Event - CyberSANE 2022 workshop in ARES conference .....	5
Press & Other Content .....	6
Publications .....	7
News & Events .....	7
CyberSANE Partners .....	8



## Editorial

The CyberSANE project has reached its end. We are proud to have brought together such an amazing group of partners during the project development.

The project ran for three years co-funded under European Union's Horizon 2020 Research and Innovation programme, creating a security incident handling, warning and response dynamic system to protect Critical Information Infrastructures (CIIs) against different types of cyberattacks and intrusions which is also based on knowledge and collaboration while allowing continuous learning during the whole lifecycle of an incident.

On this issue you will see the description of our pilots and some details of our final event in the ARES

conference. After so many virtual events it was a real pleasure to have a real-life event! Do not worry if you could not be there as the final workshop has been recorded and is now available in our website.

We are more than thankful that you followed our progress along the last years even in the difficult times of COVID-19. We hope you enjoyed the experience and that our five CyberSANE components and results will continue to be a valuable contribution in the field of cybersecurity and critical infrastructures protection.

Best regards,

The CyberSANE Consortium!

# CyberSANE Pilots

## First pilot - Transportation

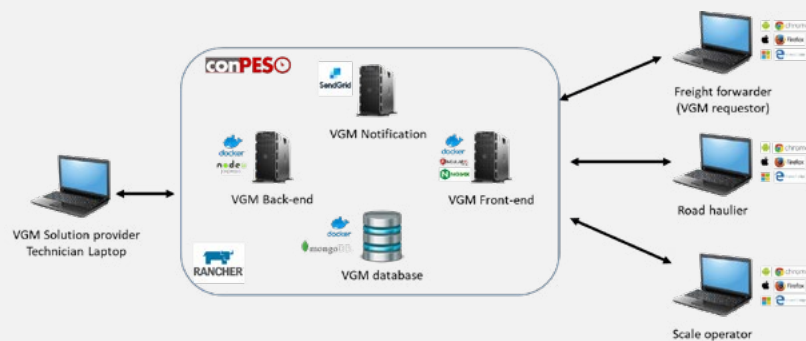


First pilot regarding container cargo transportation was conducted on 2nd February 2022. The scenario defined for this pilot is based on an electronic tool used for exchanging information among companies in the port of Valencia. Due to the travelling restrictions because Covid-19, the initially plan of having a face-to-face meeting had to be changed to a virtual event.

In order to comply with the international regulation for loading full container in vessels, Fundacion Valenciaport developed conPESO. It is an electronic platform that facilitates the compliance of SOLAS regulations on weighing containers for the port logistics community. The platform offers users an effective solution

to allow containers to arrive at the port with Verified Gross Mass (VGM), reducing last minute incidents or delays at container terminals or the appearance of congestion situations. The data can be automatically shared among all the involved actors.

The pilot covered two scenarios of fraudulent modification of container weight and disruption of port services. The interaction of integrated components on the CyberSANE platforms such as L-ADS, Gloria, ShareNet, PrivacyNet, MEDUSA for Dark Web Intelligence and Event Registry showed how to identify and eliminate a malware as well as to create a lesson learned based of taken course of actions and inform partners about potential threats.



## Second Pilot- Solar Energy



The second CyberSANE pilot took place on 5th April 2022. The CyberSANE Energy pilot focused on the assessment, detection and elimination of potential threats issued against an Energy-Management system product developed by Lightsource Labs Ltd called "Tribe".

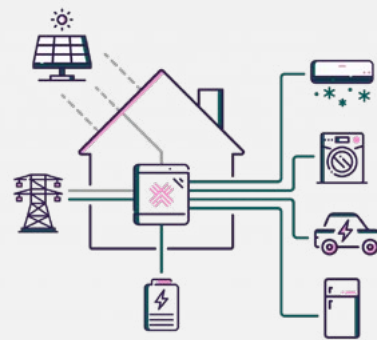
The Tribe Hub is an advanced, intelligent, IoT gateway designed to monitor, control, optimize and automate energy flows within a

building; effectively turning it into a smart home.

The Tribe Hub sits in between energy sources (like the power grid, PV solar panels and a hybrid battery storage system) and household appliances. Domestic appliances can be connected to Tribe via IoT smart devices such as wireless, energy metered power plugs. The data collected by the IoT Gateway is also transmitted to and stored in a cloud-based infrastructure

called “the Broker” using an encrypted communication protocol.

The pilot showed the handling of attacks on a solar energy production storage, and distribution. An unprivileged access to a tribe hub following by prevention and detection of suspicious signatures or inaccurate readings from a compromised or cloned energy metering devices were presented a proof of concept using the CyberSANE platform. The integrated components on the CyberSANE platform such as XL-SIEM, Suricata, Encrypted Traffic Analysis, L-ADS, MEDUSA, ShareNet and PrivacyNet were used for demonstration.



### Third Pilot- Healthcare

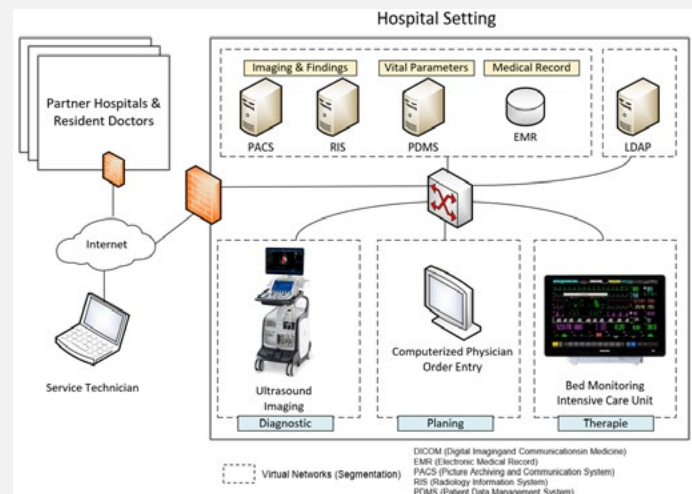


Third pilot took place on the 1st of July 2022 and focused on the detection and communication of cyber-threats within hospitals.

In a regular healthcare environment there are numerous medical devices, such as ultrasound imaging, magnetic resonance imaging or computer tomography devices. Those devices produce medical data linked to individual patients during diagnostic processes. The whole system of medical devices and their data is protected with firewalls; nevertheless, medical devices own a relatively large attack potential as the focus during the development of those devices was not on IT security. Medical technology is furthermore increasingly connected to network functionalities; medical technology used to be built for closed subsystems, but nowadays it gets more closely related to the hospitals' information technology.

Service technicians regularly provide support for medical devices and thus access potentially critical medical IT networks. This is a weak point for hospital IT security.

For the CyberSANE pilot, we focused on simulated attacks against an ultrasound device. The pilot demonstrated the cyber-threat identification in a simulated hospital environment due to an external attack and communication of lessons learned



to partners using the CyberSANE platform.

Subcomponents such as SiVi, a part of the LiveNet, and L-ADS, a part of HybridNet, were used to localize the attack flow. Furthermore, an analysis of potential cyber-attacks in the media by using EventRegistry and knowledge exchanged with partner using ShareNet were presented.

All three pilots were successfully carried out with participation of dozens interested parties per pilot and showed interest in the CyberSANE platform and an interaction of its components.



## Final Event - CyberSANE 2022 workshop in ARES conference

The International Workshop on Cybersecurity on Critical Infrastructures Management (CyberSANE 2022) has been the official event to present the result of the pilots and the conclusion of our project after three years of work.

This workshop was held in Vienna on 23rd August 2022 in conjunction with the 17th International Conference on Availability, Reliability and Security (ARES Conference). Since 2005, ARES, organized by SBA research, brings together researchers and practitioners in the field of IT security & privacy and serves as an important platform to exchange, discuss and transfer knowledge.

ARES 2022 came back to real life again with the possibility to interact personally after two virtual editions due to the pandemics. This edition had a total of 330 participants from more than 32 countries presenting 180 papers and included 25 workshops - 11 of them in the EU Projects Symposium.

CyberSANE workshop was presented early in the morning with the other eleven EU project workshops in a short pitch meeting (one minute/one slide) and started in the afternoon. The workshop opened with Luis Ribeiro's talk called "From Zero to Hero" about the recent history of cybersecurity and the need for solutions such as CyberSANE nowadays. The next CyberSANE2022 presentation was done by our technical coordinator, Thanos Karantjias from Gruppo Maggioli. Thanos explained the CyberSANE Architecture and performed a live demo of the CyberSANE Platform. The following presentation was performed by Armend Duzha, from Gruppo Maggioli and described the business models and the strategies employed during the CyberSANE Project.

To adequately validate the benefits and full set of features of the CyberSANE



system, a set of pilot scenarios were defined. Although CyberSANE will be applicable to various scenarios in a CII's context, these three pilots, covering three sectors (energy, transportation and health) are the basis of the project.

After the coffee break, Guillermo Yuste from Atos introduced the role of the five CyberSANE components in each one of the pilot use cases. Then, Pablo Giménez Salazar from Fundación Valenciaport presented the challenges and lessons learnt during the deployment of the Container Cargo Transportation pilot. He talked about protection of IT, OT and port community systems of one of the sixth largest ports in Europe in terms of volume of traffic against complex threat scenarios disrupting port operations or facilitating illegal activities, unauthorised access to corporate network of SCADA, interference with the authorisation processes for vessels, among others.

The Solar Energy production, storage and distribution pilot was presented by Robert Bordianu from Lightsource Labs. The pilot was related to the protection of their smartly integrated distributed energy platform and its components against threats to the back-end through unauthenticated remote access to IoT components or other entities to disrupt or change services and data and to the IoT and communication systems processing and transmitting sensitive data.

The pilot related to cyberthreat identification and communication in healthcare was presented by Andrius Patapovas from Klinikum Nürnberg. The health pilot focused on the detection and communication of cyber-threats within hospital in order to prevent patients from physical damage and to protect electronic patient data.

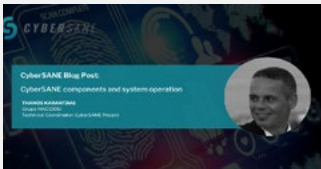
The event concluded with a presentation by Manos Athanatos from FORTH who talked about the various





## CyberSANE final official video

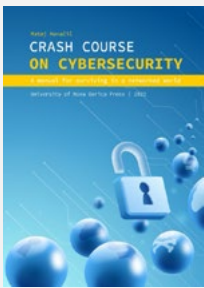
A new video including a short description of the pilots have been produced. The project and its importance has been summarized in around 5 minutes.



## Blog Post: CyberSANE components data-flow and system operation

This post by Thanos Karantjias from Maggioli contains the description of the CyberSANE core and components and its functions

# Publications



## Crash Course on CyberSecurity – A manual for surviving in a networked world, Matej Kovačič, University of Nova Gorica Press

The aim of this handbook is to provide a clear overview of the various aspects of cybersecurity that are relevant for business entities and to provide technologically neutral advice for the implementation of protection against cyber-attacks within companies.

This handbook is intended for managers who are primarily responsible for the implementation of information security solutions in their business environment and for users of information technology. The provision of information security requires both technology and appropriate organisational rules (security policies). An important part of the provision of information security in an organisation is also the education of users (employees). Employees who are not aware of the security risks for the organisation represent a major hazard and poor information security can ultimately jeopardise the very existence of the organisation.



Matej Kovačič

# News & Events



## CyberSANE Healthcare Pilot Case Study

1 July 2022, Virtual

CyberSANE held the third Pilot Case Study, organised by Klinikum Nürnberg. This pilot tested and validated the CyberSANE System in the scope of a cyber-attack scenario on a simulated infrastructure of a healthcare provider.



## CyberSANE 2022– International Workshop on Cybersecurity on Critical Infrastructures Management

23 August 2022, Vienna (Austria) + streaming

On the 23rd August 2022, CyberSANE held the International Workshop on Cybersecurity on Critical Infrastructures Management (CyberSANE 2022). The objectives of this workshop were to present the CyberSANE project and its architecture to participants. Furthermore, we presented the three use cases as well as the results of their respective studies. We also talked about the various standardisation activities partaken during the project as well as various business models. It was held in conjunction with the 17th International Conference on Availability, Reliability and Security (ARES 2022), in Vienna, Austria.

## CyberSANE Partners

### Valenciaport Foundation (VPF)



The Valenciaport Foundation for Research, Promotion and Commercial Studies of the Valencia region (Valenciaport Foundation) is a private non-profit research created in 2004 through an agreement between the most representative associations and companies of the Valencia logistics-ports community and various institutions of the Valencia region, all of which are involved in logistics and maritime transport.

Part of Valenciaport Foundation team consists of researchers specialised in transport economics, logistics and intermodality coming from the Institute of International Economics (IEI) of the universities of Valencia, Alicante and Jaume I of Castellón. The other part is composed of R&D&I specialists in the field of maritime and intermodal transport coming from the Foundation of the Port Institute for Research and Cooperation, this being an entity with renowned prestige in this domain. Finally, in the professional domain, the research team also includes staff from the Port Authority of Valencia itself and other companies of Valenciaport's ports-logistics community. As such the Valenciaport Foundation manifests an R&D&I centre of excellence that not only undertakes its own academic research but also serves as a tool at the service of all agents involved in the transport and logistics chain and particularly within the maritime and port domains. On top of the activities linked to research and training the Valenciaport Foundation also carries out international cooperation projects focused on the optimal and integrated development of transport, logistics and ports located in third countries.

Valenciaport Foundation contributes to CyberSANE with the preparation and implementation of the pilots and participation in most stages of the project. Valenciaport Foundation leads WP9 related with coordination and pilots' demonstration. Valenciaport Foundation also contributes to WP2, WP10 and WP11 related with the whole development phases of the project.

In this context, Valenciaport Foundation lead the Stakeholders' Requirements specifications (T2.3) and the scenarios and test cases definitions (T2.4) and participates on pilot activities engaging Port Security Operators and/or Port Facility Operators in the customization (e.g., on the basis of the terminals, assets, zones etc. of the port) (WP9) and the use of the CyberSANE system involving drills of simulation scenarios and security assurance models (WP10).

The premises of Valenciaport Foundation are located in the Port of Valencia, next to the offices for the Port Authority. For the purpose of the project, the Foundation has at its disposal the global facilities of Valenciaport.



Dr. Pablo Gimenez



Angel Laguna  
Argente



Valenciaport Foundation provided access to some of the systems in the port of Valencia such as the Port Community System (PCS), the SCADA system or the Emergency Control Centre (CCE).

The flow of information in the port of Valencia is highly complex and involves a great many agents. Each movement of a TEU requires multiple communications amongst members of our Port Community, creating a highly complex information network. The Port Community System is an open, neutral electronic platform that enables smart and secure exchanges to be made between public and private

agents with the aim of improving the competitive position of our port community.

SCADA (Supervisory Control and Data Acquisition) is a system for remote monitoring and control that operates with coded signals over communication. The control system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording. SCADA is responsible for managing all the sensors deployed in the port, the building consumption or the gates access information.

## Lightsource Labs (LSE)



Lightsource Labs (LSE) established in 2016 in Dublin as the innovations arm of Lightsource Renewable Energy. Lightsource Renewable Energy, founded in 2010 is a global leader in the funding, development and long-term operation

of solar PV projects. Lightsource's revenue model is focused on capturing value throughout the life of the asset, integrating in-house development, operational management and contracted income (25-30 years+) and deep asset financing expertise to optimise competitiveness.

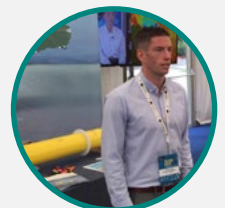
LSE scheme is formulated around the development and delivery of disruptive, transformational and intelligent energy management solutions for the enormously untapped market of Smart Energy. These solutions are comprised by cutting edge technologies combined by innovative financing models which are able to create "NoBrainer" propositions for specific sectors.

LSE mission is to deliver a comprehensive, integrated platform and a number of digital services on top, helping energy "procumers", utilities and grid operators to optimize power flows, secure the electricity grid (without additional investments) and finally reduce the cost of electricity.

LSE first innovative product is SIDE - Smartly Integrated Distributed Energy, a smart software-hardware solution optimised for Grid 2 Home / Home 2 Grid optimization of a distributed generation system consisted by a solar array, a home battery and controls of large appliances, like washing machines, dishwashers, fridges etc. The orchestration of the power flows is performed by SIDE Gateway, located in the home. The gateway has been designed to allow for new functionality and connectivity to be added as requirements evolve.

The SIDE Cloud Platform is fully hardware agnostic - available to adapt the offering to individual markets and keep up with the fast-changing components market. The SIDE Gateway relays data back to the cloud while all actions are controlled locally to allow the Smart Home to ride-through grid or data connection outages. LSE has also developed an automated CRM system, designed to manage the customer journey for "prosumer" and streamline customer acquisition.

Today SIDE is generating electricity behind the meter, by controlling solar & storage and continuously optimizing power flows to maximise the benefit of locally generated solar power. There is a clear roadmap of new features including even smarter optimisation through machine learning of the consumers' profiles and improved weather forecasting predictive analysis which will allow improved efficiency, economics, reliability, and energy conservation for the household. In parallel to these features SIDE develops localised grid support services,



Diarmuid O'Connor



Robert Bordianu

facilitating electric vehicle penetration, creating value to the homeowner through light-touch interactions.

LSE is conducting the first in-the-field trial of the SIDE integrated with a solar and storage product. The trial names Sunplug ([www.gosunplug.com](http://www.gosunplug.com)) is being conducted in the UK in mid 2016 as part of a non-exclusive partnership with EDF.

LSE and EDF have jointly marketed a new Smart Home package to UK consumers. Co-brand "Sunplug", the purpose of the trial has been to gain high quality real-world data, test marketing strategies and give SIDE an in-the-field trial in Lightsource's home market. The trial has been open to both EDF customers and customers currently using another supplier for their grid power. Users interact with their system via the Sunplug app or web portal. LSE Labs controls

the battery operation locally and retains high quality anonymised power-flow data.

Taking a strong stand in fighting electronic crime, the company aims at being a pioneer of its sector in managing its corporate systems security. Given the extent and the criticality of the Supply Chain that LSE is a member of, the interest in CyberSANE scope is self-apparent. LSE participates in the project as end-user and contributes in most of the WPs, initially through the provision of input for the system requirements and specifications, and regulation framework in WP2, and later during the CyberSANE system testing and validation, techno-economic assessment, dissemination of results in WPs 9, 10, and 11.

---

## Klinikum Nürnberg (KN)

---

### Klinikum Nürnberg

*Wir sind für Sie da!*

Klinikum Nürnberg (KN) is a maximum care hospital, full medical service provider and one of the largest municipal hospitals in Europe. With its 2,370 beds, two main locations in Middle Franconia and with its staff of about 7.000, KN is one of the most diversified health service providers in Germany to almost 100,000 inpatients and of approximately 105,000 outpatients each year. KN encompasses over 42 specialty departments, centers and institutes, which are distributed on 9 main facilities, namely Klinikum Nürnberg North and South; 3 midsize hospitals in the greater region of Middle Franconia; a series of outpatient medical service centers; the research unit Paracelsus Medical University (PMU); a center for outpatient rehabilitation and finally a center to provide outpatient palliative care. Klinikum Nürnberg contributes to CyberSANE as piloting partner. That encompasses the definition and selection of a pilot area, collaboration in creating a pilot plan (WP9), conducting the pilot and collaboration in assessing pilot results (leader of WP10). Furthermore, KN gathered requirements from its ICT business unit, its executive staff and users (WP2). KN also tested the propagated R&D solutions to contribute concerning validation of objectives of the proposal. KN provided a representative set of use case scenarios in IT-security and privacy protection resting on and dealing with outpatient and clinical information

systems and high performance computing in hospitals.

So far KN leads and executes regional and national R&D projects mainly in the domain of medical and clinical engineering and technology. To that effect, fundamental experiences about management and implementation of R&D projects exist.

KN has a sound experience of how to manage, secure and protect ICT infrastructures in hospitals and other organisations with the core business of providing healthcare in daily operations. Furthermore, KN has expertise to manage and support information and communication scenarios between required professional connectivity and coherence with its corresponding and accompanying risks like socio-technical threats and vulnerabilities in cyber-security and privacy protection of an infrastructure supporting clinical processes.

In technical perspective, the departments, business units and locations of KN were connected by a WAN infrastructure, including a series of LANs and VLANs, two data centers and around 4000 connected, stationary devices. The ICT department maintains and aims to secure 2 computing centers, servicing around 5800+ workstations, laptops and printers as well as monitoring 480 medical workstations and 500+ medical devices. Not to mention approximate 680 different software applications (510 on client, 170 server-side), more than 6 different operating systems each with its versions and variants (server, client, embedded) and remote maintenance access by 100+ manufacturers of hard- and software products.



**Manfred Criegee-Rieck**



**Andrius Patapovas**



**Lena Griebel**

**PDM**

**Atos**



*Inria*



**UBITECH**  
UBIQUITOUS SOLUTIONS



**FORTH**  
FOUNDATION FOR RESEARCH AND TECHNOLOGY - PELLE

**Sphynx**  
Technology  
Solutions

**KU LEUVEN**




 **University of Brighton**

 **SIDROCO**

  
FUNDACIÓN  
VALENCIAPORT

lightsource**Labs** ©

**Klinikum Nürnberg**  
*versand für Sie da!*

**in** cybersane-h2020  
 CyberSANEH2020  
 cybersane-project  
 cybersane-project.eu



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833683

