Status of the R²D²

The R²D² Project completed its first year of life during which the technical and scientific foundations were laid for the development of its four products. In these first twelve months, several activities have advanced the development of the project, in the field of the resiliency, reliability, cyber-, physical and operational security. The use cases, requirements and architecture have been defined, the software design and functional descriptions of the four products have been completed, and the development phase of the four products has finally begun. The project will be validated in four pilot sites

(including TSOs and DSOs), which have completed a monitoring and survey of the available IT and OT infrastructure, and of the applicable regulation and legislation relating to the (cyber) resiliency of electrical systems. Finally, in this first year, R²D² has been active in confirming its presence in the various forums and initiatives at European level to communicate and disseminate its objectives, and the innovations proposed by the project.

R²D²: A new member of the EU Cluster for Securing Critical Infrastructures

R²D² is set to make significant contributions to the European Cluster for Securing Critical Infrastructures (ECSCI) by focusing on strengthening the security and resiliency of power systems. ECSCI, which comprises a cluster of European projects, serves as a platform for sharing advancements in security and resilience within critical infrastructure.

R²D² project coordinator, Ugo Stecchi, emphasizes the significance of this involvement, stating, *"It will be available opportunity to share our accumulated knowledge not only with stakeholders in the energy sector but also with experts from various critical infrastructure domains. We can exchange best practices and procedures, thus contributing to the ongoing*

discourse on the state-of-the-art of critical infrastructure security."

The objective of this engagement is to facilitate the exchange of findings related to the prevention and mitigation of cascading events, cyber-threat intelligence, and other factors influencing the resiliency and security of electrical systems with fellow cluster participants.

EMMA-SURVEILLANCE:Enhancing Substation Security with AI-Powered Visual Detection

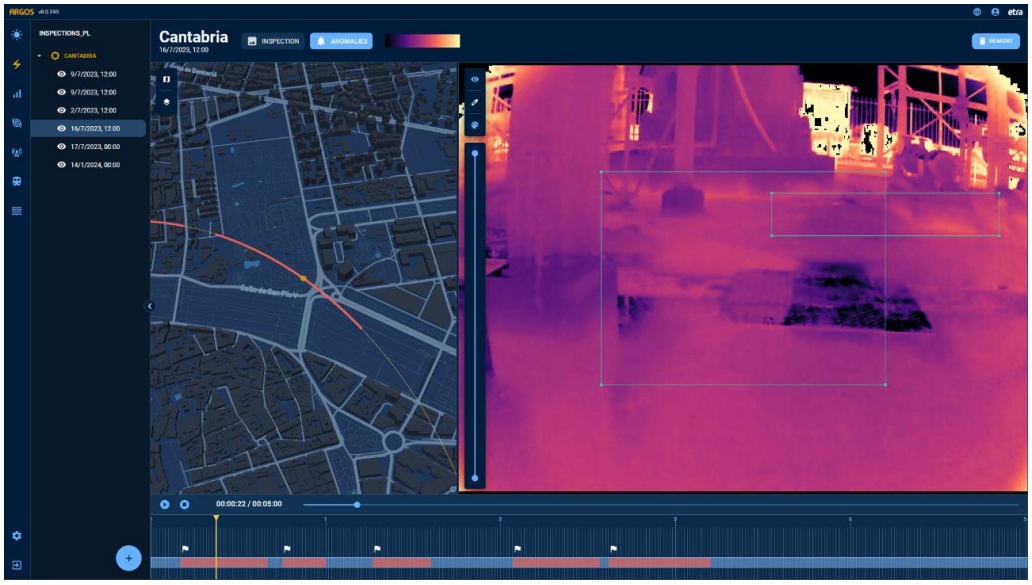
As part of the ongoing R^2D^2 project, partners are actively developing an innovative tool named EMMA-SURVEILLANCE to enhance the security of critical facilities situated within electrical substation transformer centers. This solution incorporates an artificial vision algorithm, refined through the retraining of the renowned YOLO (You Only Look Once) model.

EMMA-SURVEILLANCE's algorithm is designed to proficiently identify fires, smoke, and the presence of animals in the proximity of the substation. The primary objective is to provide timely alerts

to personnel in case of potential emergencies, ensuring a prompt and effective response. Additionally, the system is equipped to recognize animals, a crucial feature considering their tendency to interact with substation structures. This capability mitigates the risk of electrocution and prevents significant disruptions to the electrical system.

The deployment of this model involves installing it in a stationary camera strategically positioned within the corresponding pilot substation. This implementation aims to offer comprehensive surveillance and early detection capabilities to bolster the overall security measures in place.

Read more here.



Unlocking the Power of Threat Hunting in OT Environments

In today's dynamic digital landscape, the R^2D^2 project stands out as a vital initiative addressing the escalating cyberthreats facing industrial systems and critical infrastructures. The convergence of Information Technologies and Operational Technologies (IT and OT) under the industry 4.0 paradigm has opened vulnerabilities exploited by APT groups and cybercriminals, posing risks to both industrial infrastructures and society.

As threat hunting is a complex process, cybersecurity experts utilise advanced tools like CARMEN, developed by S2 Grupo in collaboration with Spain's National Cryptologic Centre. CARMEN, an instrumental component of the R^2D^2 project, extends threat visibility to both IT and OT traffic, facilitating early detection of vulnerabilities and anomalies in industrial control systems. This proactive approach enhances security, improves incident response, and minimizes operational disruptions.

As part of the R^2D^2 project, S2 Grupo has elevated CARMEN's capabilities for analysing OT traffic.
Read more here.