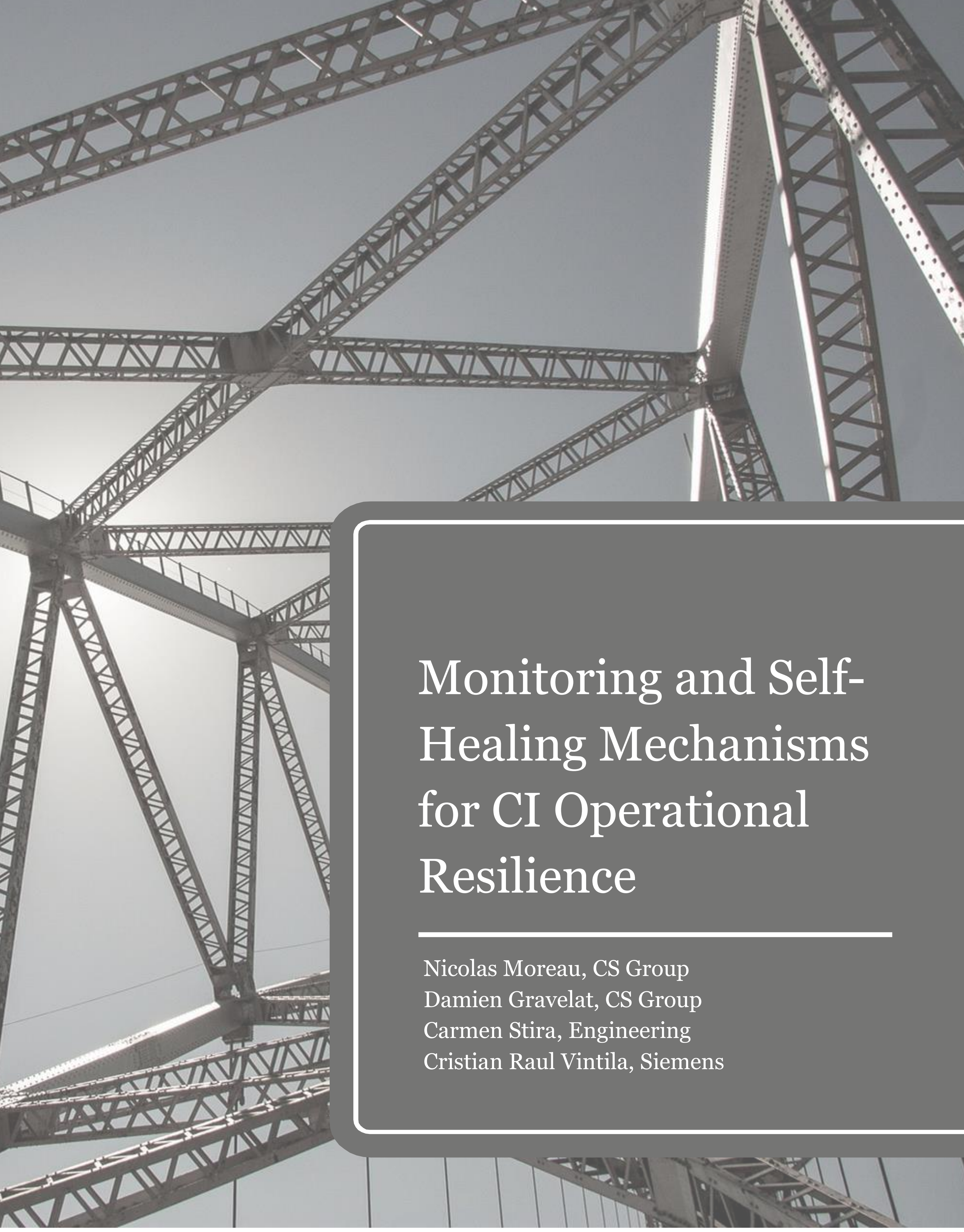

Monitoring and Self-Healing Mechanisms for CI Operational Resilience

Nicolas Moreau, CS Group
Damien Gravelat, CS Group
Carmen Stira, Engineering
Cristian Raul Vintila, Siemens

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under the Grant Agreement No. 101073909.
The contents of this document represent the views of the authors only and remain their sole responsibility. The European Research Executive Agency and the European Commission are not responsible for any use of the included information.

Monitoring and Self-Healing Mechanisms for CI Operational Resilience

Nicolas Moreau and Damien Gravelat (CS Group),
Carmen Stira (Engineering), Cristian Raul Vintila (Siemens)

The ATLANTIS project aims to enhance resilience of European Critical Infrastructures (ECI) against cyber-physical threats. It stresses the use of self-healing mechanisms and monitoring tools for system continuity. Utilizing microservices, orchestration, and redundancy, ATLANTIS addresses challenges in scaling these mechanisms to a system-of-systems level. Implementation of an orchestrator and microservices ensures high availability and resilience, bolstering security against cyber threats.

1. Introduction

The ATLANTIS project goal is to enhance the resilience and protective capacities of interconnected European Critical Infrastructures (ECI) in light of the ever-evolving landscape of cyber-physical threats. With the growing interdependency of critical infrastructure sectors and the increasing sophistication of malicious actors, there is a pressing need to strengthen the defences of these infrastructures. ATLANTIS recognizes the pivotal role played by IT infrastructure in ensuring the seamless functioning of critical systems, and thus, aims to address the vulnerabilities inherent in these systems. By leveraging advanced technologies and innovative approaches, ATLANTIS seeks to mitigate risks posed by both existing and emerging large-scale combined threats, thereby safeguarding the continuity of operations and minimizing the potential for cascading disruptions across interconnected infrastructures. Through a multifaceted strategy encompassing self-healing mechanisms, robust monitoring frameworks, and collaborative efforts across stakeholders, ATLANTIS endeavours to fortify the resilience of European Critical Infrastructures against a wide array of cyber, physical and hybrid threats.

2. The Current State of Affairs in Monitoring and Self-Healing Mechanisms

The **self-healing** is the ability of a system to automatically recover or repair failing parts. In the context of ATLANTIS, the concept must be understood at two different levels. The first one is at the level of a given Critical Infrastructure where mechanisms shall be implemented to ensure the self-healing of all the IT systems used to perform its functions and to supervise it. The second one, that is more related to the ATLANTIS project, operates at a pan-European level where a toolbox will be set in place to ensure the cross-sector and cross-border threat prediction and incident mitigation. As this toolbox must be available at all times, it is therefore highly recommended to set in place all self-healing mechanisms that will allow us to reach this goal.

The self-healing concept cannot be separated from the monitoring of the system. Indeed, diagnostic always comes before the cure. It is therefore necessary to set in place monitoring tools on the system (or system of systems) that will provide information to the self-healing tools to determine which actions to perform and when to keep the system up and running.

Self-healing and monitoring mechanisms are already in place in advanced IT systems. Here is a list of such mechanisms:

- **Microservices**: They enable self-healing by isolating services, allowing for autonomous deployment and scaling based on demand. Each microservice operates independently, so failures are contained, and the system can continue functioning. Service discovery and load balancing mechanisms redistribute traffic to healthy instances, maintaining system stability. Their modular nature facilitates quick recovery from failures, as failed services can be restarted or replaced without affecting the entire system.
- **Orchestration**: This mechanism allows the automation of software deployment. It works with containers, and it is suitable for running and managing large cloud-native workloads. It automatically manages service discovery, incorporates load balancing, tracks resource allocation, and scales based on compute resource utilization. It also performs individual resource integrity and enables applications to self-heal by automatically restarting or replicating containers.
- **Redundancy**: It is defined as the state of exceeding what is necessary to function properly, to prevent the failure of an entire system due to a single component failure [1]. In this context, network redundancy is the process where additional instances of devices or equipment are installed within the network infrastructure. The additional instances serve as a backup mechanism to automatically swap the networks operations in the event of a network failure.
- **The event-driven architecture (EDA)**: It enables reliable and asynchronous interaction between components and services in a system. It operates by exchanging messages that represent significant events and changes in the system's state. This communication is supported by a messaging broker that handles the flow of events among the components.
- **The service mesh**: This is now an integral part of the cloud-native stack. It boosts applications with augmented observability, security, and reliability, operating at the platform rather than the application layer.
- **The monitoring**: This is a key part of self-healing. All mechanisms set in place must be able to provide status so that tools can cope with potential problems.

3. Monitoring and Self-Healing Mechanisms at Scale

Mechanisms and technologies described above are already in use in software infrastructure requiring high level of scalability and availability. The main challenge we are tackling in ATLANTIS is to scale up all these mechanisms from CI level (and their dedicated IT) to system of systems level as described in Figure 1.

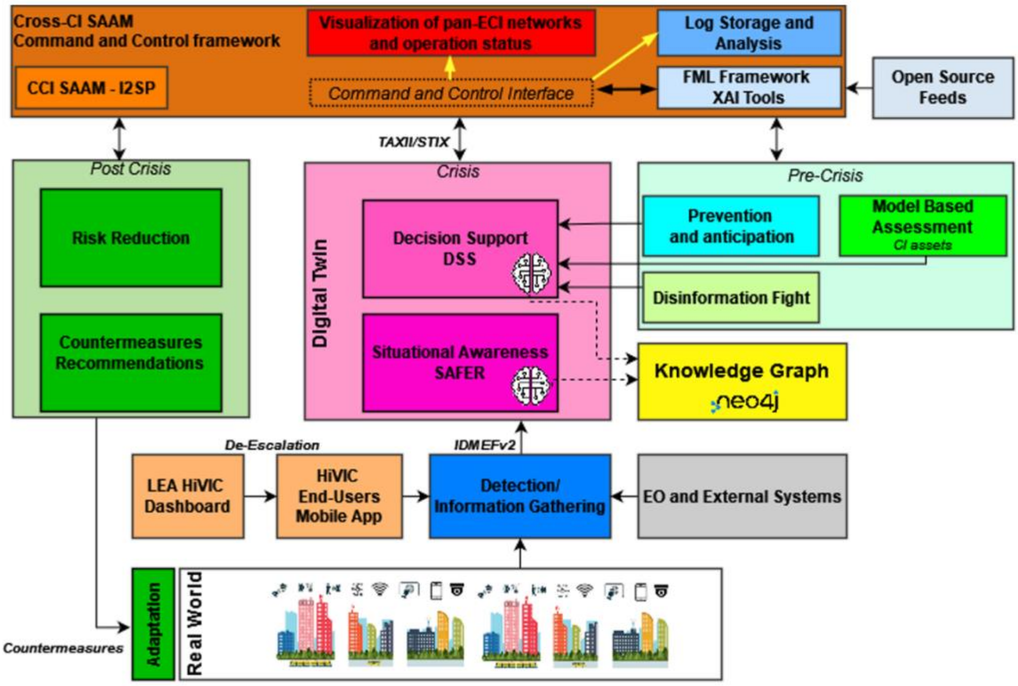

Figure 1. ATLANTIS components.

It gives a global overview of all the components but, according to the developments that have been already done, each component will be composed of several sub-components that will have their own architecture.

Coming back to the roots of ATLANTIS, the main goal of the project is to set a toolbox dedicated to CI operators, to LEAs, to government agencies and to any stakeholder that would have to be involved in a pan-European crisis due to a CI breakdown. Therefore, it is for us an obligation to use all the tools at our disposal to make sure that the ATLANTIS toolbox has the highest availability as possible as possible regardless of the complexity of its architecture. And furthermore, using all the monitoring tools set in place, our goal is to be able to provide a real-time synthetic view of the state of the system of systems to help end-users in their decision making.

4. The Research and Development Path in ATLANTIS

As described in Section 2, one of the mandatory steps is to make sure that all ATLANTIS components will be compatible with an orchestrator that can handle the redundancy and the scalability of the whole system. Taking this obligation into account, we are using Kubernetes.

Kubernetes uses four main components:

1. First, the **containers** are the unit of software that packages code and its dependencies.
2. Then, the **application components** or Pods consist of one or more containers sharing storage and network resources.
3. Next, **worker machines** or Nodes represent a virtual or physical machine where the Pods run.

4. Finally, the **Cluster** is a set of Nodes. Redundancy is supported on Kubernetes using parameter configurations such as the number of replicas in the application components or Pods, allowing resiliency and self-healing.

The process of monitorization uses two different probes:

1. On the one hand, the liveness probe where Kubernetes checks if the Pod is running.
2. On the other hand, the readiness probes let Kubernetes know when the Pod can serve traffic.

The self-healing process uses the information provided by those probes and the number of replicas for the Pods to monitor the components. Kubernetes replaces a Pod if something is wrong and initializes a process to terminate the old Pod [2], always maintaining the expected number of "healthy" replicas, as shown in Figure 2.

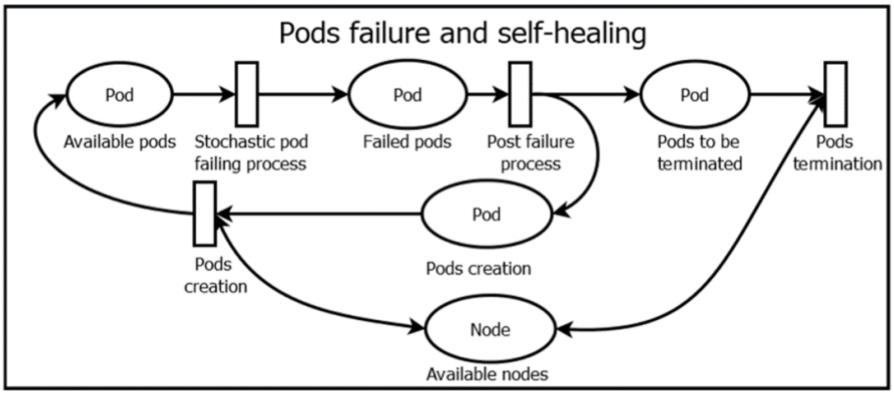

Figure 2. Pod self-healing process.

In addition to orchestration, we are also implementing a microservice oriented architecture both at component and toolbox level (as proposed as an example in Figure 3).

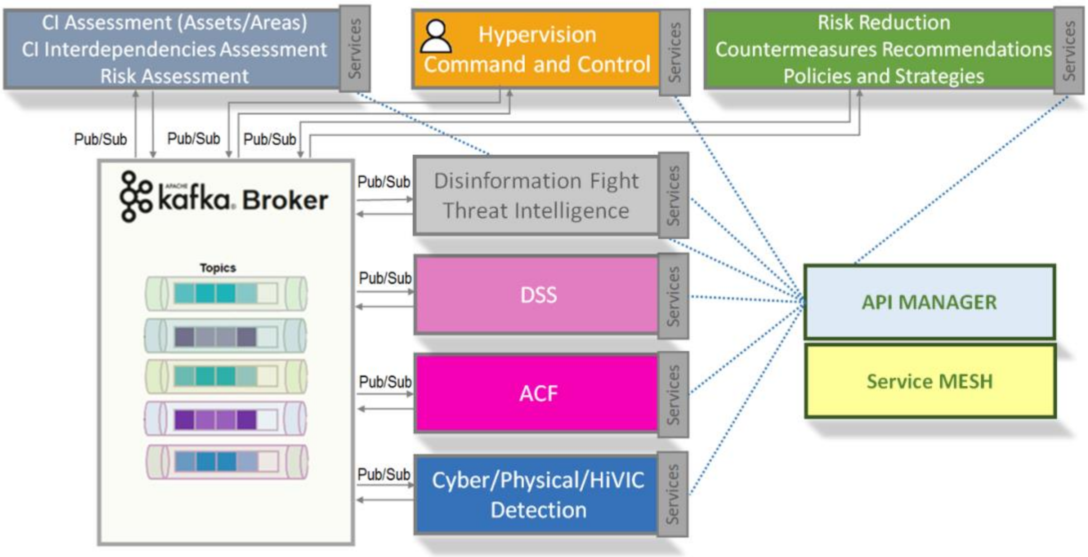

Figure 3. Pod self-healing process.

After covering these steps, our ambition to set a place an upper monitoring layer using Linkerd [3] or Istio [4] to feed the system of systems digital twin what we identify as double virtualization. The representation of this digital twin is yet to be decided (either using Green Twin solution [5] from ATLANTIS partner's SNEP or Grafana, the data visualization and monitoring platform [6]).

5. The Challenges and Barriers

The key challenges to tackle will be to scale up the monitoring and self-healing concepts at the level of a system of systems, the ATLANTIS toolbox, to go toward a double virtualization by providing a digital twin of the system of systems.

These challenges will come with the provision of a set of guidelines and recommendations to help the ATLANTIS partners in their path to make their components compatible with the self-healing mechanisms. This step will be highly connected with the ATLANTIS DevSecOps process described in [7].

At this level, one barrier is the complexity of the mechanisms to set in place for numerous applications and software composing the ATLANTIS toolbox. It demands a real effort of evangelisation, training, and support to make sure that all component owners respect the above-mentioned recommendations.

These steps being covered, the final challenge is to gather all the information coming from the components via the monitoring tools, Kubernetes, Kafka, etc., and to represent them in a meaningful and concise way (considering the high number of components and sub-components) for the end-users. This is an on-going work for which the envisaged tool has not been identified yet.

6. The Benefits and Impact

One key benefit will be the implementation, the testing and the usage of self-healing mechanisms in the context of a widely distributed architecture considering that most of the components will be installed on their own environments (on-premises, in the cloud, and both).

This will also allow us to put into practice the set of guidelines that will come out of the ATLANTIS project to provide the CIs owners with recommendations that has been fully tested and validated on the ATLANTIS architecture.

And finally, using the monitoring and self-healing mechanisms will ensure the high availability of all the ATLANTIS toolbox set in place to improve the resilience and the protection capabilities of the interconnected European Critical Infrastructures.

7. Future Outlook

In the current perturbed international context where cyber-attacks have become fully part of the belligerent arsenal, it is now mandatory to deploy all necessary measures that would ensure the operation continuities of Critical Infrastructures. Considering that they highly depend on their IT system, self-healing mechanisms must now be part of the package to protect them.

In the frame of ATLANTIS, we still need to apply these mechanisms to a wide variety of components, but we consider that it is an important step toward the generalization of usage of these tools into the Critical Infrastructures IT systems that are part of the consortium.

8. Conclusion

In conclusion, the ATLANTIS project represents a significant stride forward in fortifying European Critical Infrastructures (ECI) against the complex and multifaceted challenges posed by modern cyber-physical threats. By using cutting-edge technologies such as microservices, orchestration, redundancy, and event-driven architecture, ATLANTIS aims to create a robust ecosystem capable of quickly detecting, mitigating, and recovering from potential disruptions. The utilization of orchestrators and microservices, coupled with advanced monitoring and self-healing mechanisms, will allow to ensure high availability and resilience across critical infrastructure IT systems. Furthermore, the project's emphasis on collaboration, knowledge-sharing, and the dissemination of best practices underscores its holistic approach to enhancing cybersecurity resilience at a pan-European level. Reinforcing the protection capabilities of European Critical Infrastructures is our main goal but we would also like to see ATLANTIS results serving as a blueprint for future resilience initiatives in the face of evolving cyber threats.

References

[1] X. Xu, A. Chen, S. Jansuwan, K. Heaslip, & C. Yang. (2015) Modeling Transportation Network Redundancy. Transportation Research Procedia, 9, pages 283-302,

[2] R. Li, B. Decocq, A. Barros, Y. Fang and Z. Zeng, Petri Net-Based Model for 5G and Beyond Networks Resilience Evaluation, in "*2022 25th Conference on Innovation in Clouds, Internet and Networks (ICIN)*, Paris, France, 2022, pp. 131-135.

[3] https://linkerd.io/

[4] https://istio.io/

[5] https://greentwin.eu - Green Twin - 3D-4D-6D Web-Based Digital Twin With CMMS, BIM, Facility and Energy Management, OEE, and Carbon Footprint Monitoring

[6] https://grafana.com/

[7] Ioannis Oikonomidis, Dr. Georgia Dede, “ATLANTIS Integrated Framework: The DevSecOps Approach”, 2022.

Front cover image by 1388843 via Pixabay.
https://pixabay.com/users/1388843-1388843