The CCI-SAAM Framework

Artemis Voulkidis, Synelixis

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.

The CCI-SAAM Framework

Artemis Voulkidis (Synelixis)

In this paper, the ATLANTIS approach towards a coordinated, cross-CI, cross-border, cross-domain knowledge sharing, risk assessment, threat analysis and countermeasures mitigation is presented, under the framework of the CCI-SAAM platform. The aim of the latter is to establish a trusted and traceable framework for standardized and automated exchanges of cyber- physical threat information, so that emerging risks, threats, and attacks can be detected and mitigated more quickly, effectively ameliorating the security and safety of the European CI.

1. Introduction

The European Council defined, in Directive 2008/114/EC [1], the European Critical Infrastructure (CI) as "*an asset, system or part thereof located on EU territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or well-being of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions*" and highlighted the need for their protection. Encompassing just two CI domains (energy and transport) at the time, the importance of CI security for the EU was strategically elevated in December 2022, when the European Parliament and the Council published the Directive (EU) 2022/2557 [2], addressing eleven critical sectors and stressing that "*any disruption of essential services, even one which is initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in a far-reaching and long-term negative impact on the delivery of services across the internal market*". However, challenges remain in adapting regulatory frameworks to evolve with emerging threats and fostering a culture of cross-CI resilience. In this context and considering the importance of connected information in uncovering the cascading systemic risk that spans the status of interconnection among the various CIs, it is necessary to enable cross-sectoral collaboration towards resiliency planning and towards ensuring the generation of advanced analytics and CI interdependency modelling. Indeed, a connected information approach allowing CIs to exchange risk information controllably and securely among them can help towards alleviating the adverse cascading effects of relevant risk manifestations. However, a concrete framework allowing for handling cyber-physical security as well as systemic risk information is yet to be proposed.

ATLANTIS employs the *Cross-CI (CCI) Sharing Assessment Analysis Mitigation* (CCI-SAAM) platform that covers the compete CCI ecosystem, uncovering systemic risk and enabling risk assessment, state awareness, collaborative incidents mitigation and countermeasures enforcement over multiple cross-connected CI. This document presents the ATLANTIS approach towards defining such a platform, focusing on the technologies that enable the connected information principle.

2. The Current State of Affairs in VVI Information Exchange

Currently, there is no definite, official European approach or platform addressing the need for a connected information infrastructure towards handling systemic CCI risk management. The closest attempt towards such a modality being the NIS2 directive [3], which addresses the exchange of security information among various actors by establishing several mechanisms designed to bolster cooperation and information sharing. Effectively addressing the need for communication among the various actors of the NIS2 directive (the European Computer Security Incident Response Teams -CSIRTs- in particular), the EC has opted for the adoption of the EC-funded open source framework, MeliCERTeS [4], that acts as a collection of relevant open source tools and frameworks in an attempt to meet the operational requirements for cooperation in the CSIRTs Network (see [5] for details and discussion). However, the focus of MeliCERTeS and its ecosystem of applications mostly targets cybersecurity and does not assist the disclosure of hidden interconnections among the European CCI. In any case, ATLANTIS is fully compliant with MeliCERTeS, actually planning on maintaining a MeliCERTeS node in the context of the core of CCI-SAAM.

3. The Role of CCI-SAAM

The ATLANTIS CCI-SAAM, building on top of and substantially extending the developments of EC-funded projects such as H2020 DEFENDER [6] and PHOENIX [7] projects, aims at filling the gap that lies among the CI stakeholders, offering a way of securely exchanging physical and cyber threat intelligence (PCTI) data and uncovering hidden interconnections among them, effectively giving rise to an interconnected Pan-European CCI.

Indeed, CCI-SAAM provides a coordinated framework that enables critical infrastructure operators and stakeholders to collaboratively assess risks, share information, and implement mitigation strategies. In addition, it integrates capabilities for systemic risk analysis, threat intelligence, explainable AI, and cooperative response to strengthen resilience against cascading failures. Lastly, the CCI-SAAM platform facilitates seamless communication and coordinated action across CI domains and national borders.

4. The Research and Development Path in ATLANTIS

A high-level depiction of the CCI-SAAM framework architecture is provided in Figure 1, where the cylinders indicate data stores and squares represent processes. The CCI-SAAM is provided with information from the various ATLANTIS-enabled CI, by employing a secure communications channel, backed up by 5G technologies. This information flow mostly comprises two different types of information, namely:

1. **Selected risk-evaluation-related data** chosen by the CIs to be shared to the Pan-European CCI-SAAM infrastructure with a scope to generate an accurate view of the European Critical Infrastructure risk state (awareness), and
2. **Federated Learning (FL) models** from the various CIs, essentially offering model aggregation services to the CIs.

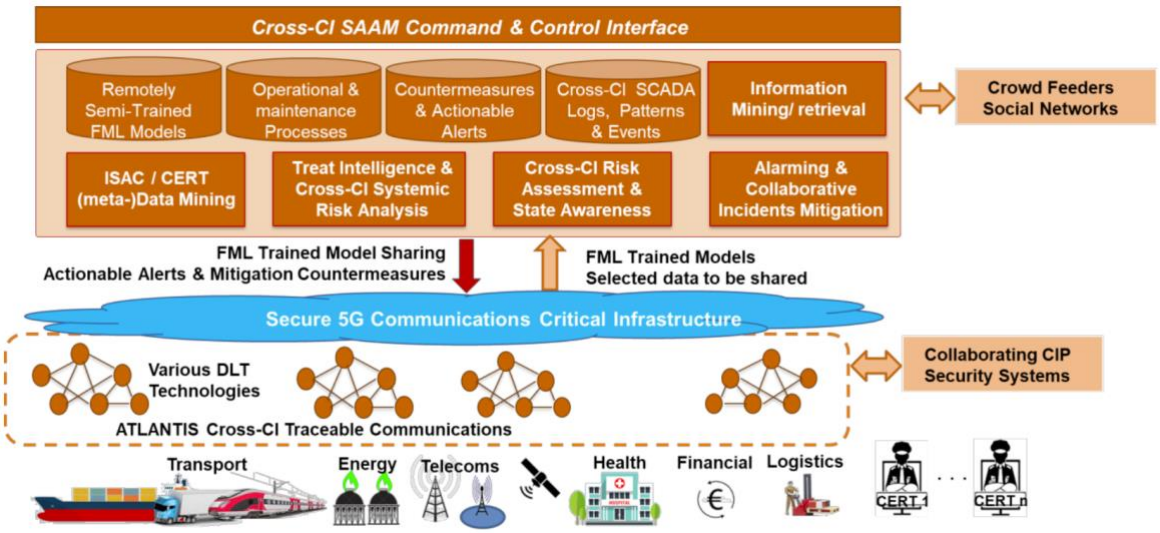

Figure 1. High-level architecture of the CCI-SAAM framework.

The support for the two types of information communicated in CCI-SAAM serves entirely different purposes and objectives. The risk evaluation data from the ATLANTIS-enabled CIs contain information regarding identified risks[1] at the local level, effectively allowing CCI-SAAM to combine information from multiple CIs, elaborate on the generated insights and come up with actionable alerts and risk mitigation/alleviation strategies so that the residual risk of the identified risk may be minimized. These data (could be related to reports on both physical and cyber threat intelligence – PCTI – data) may contain information on CI-related identified risks, threats, vulnerabilities, attacks, attack campaigns as well as identified courses of action (mitigation strategies) that were taken at local CI level. This information gets stored to a "Cross-CI SCADA Logs, Patterns and Events" data store and then, gets consumed by a Threat Intelligence & Cross-CI Systemic Risk Analysis process which, in turn, will trigger a procedure of identifying the security risk state of the pan-European CI, as a whole. At the same time, an "ISAC/CERT (meta-)Data Mining" process may receive information from multiple (federated) ISACs/CERTs/CSIRTs (Information Sharing and Analysis Centres / Computer Emergency Response Teams / Computer Security Incident Response Teams), in an attempt to get a clearer view of the security status non-ATLANTIS-enabled CIs, again at pan-European level. Similarly, an "Information Mining/retrieval" process has been foreseen, that gets information from crowd feeders and social networks, so that the cross-domain risk analysis data processing may be further assisted. The outcome of the risk analysis process should, next, be fed to an "Alarming & Collaborative Incidents Mitigation" process which will attempt to generate actionable alerts at local, regional, or pan-European level and communicate them to the ATLANTIS-enabled CIs as well as the federated ISACs/CERTs/CSIRTs.

Regarding the flow related to the FL Trained Models, this includes model weights from the local ATLANTIS-enabled CIs to the CCI-SAAM, so that a model aggregation strategy may be applied, effectively enabling FL on (P)CTI data across the ATLANTIS-enabled CI federation.

[1] The risk reports may contain information related to non-systemic identified risks.

Last, a "Command and Control Interface" is foreseen, that enables a visual representation of the European CI security risk awareness, catering for easier decision-making from the side of the operators of the CCI-SAAM.

At the time of writing this report, the interconnections, data flows and standardized communication data models and protocols (e.g. based on STIX/TAXII [8][9] as well as MISP core format [10]) among the various components have been identified and base technologies implementing the expected features have been worked upon.

5. The Challenges and Barriers

At their core, the challenges and barriers of CCI-SAAM are mostly related to paving the necessary policy-making path so that the concept of secure information exchange in the context of CCI becomes part of the culture of the both the CI operators and the regulatory/legislator bodies of the EC. To this end, it is of fundamental importance to define and agree upon a comprehensive set of terms and rules of engagement of the CCIs and publish them at the form of a manifest to be communicated to the relevant competent regulatory/legislative bodies.

From a technological perspective, the challenges mostly lie on the determination of the process that could lead to uncovering the hidden interconnections among the various CIs, in an attempt to identify cascading effects, particularly considering the limited modelling and, in general, data availability.

6. The Benefits and Impact

The benefits of CCI-SAAM mostly lie on the employment of data in the discovery and timely communication of systemic risks and proposed courses of action among various, interconnected CCIs. This information exchange, when properly handled, has the potential of significantly enhancing the security, safety, quality of service and stability of the European CCI. This may be achieved by identifying coordinated/cascading systemic risks and offering actionable recommendations to CI operators on how to alleviate their effects.

7. Future Outlook

The design of CCI-SAAM is flexible, yet concrete, building upon state-of-the-art concepts, approaches, and technologies, designed with scalability and survivability in mind. To this end, a performance-oriented, cloud-native approach towards its design and deployment has been sought, ensuring its relevance for the years to come.

The architecture of CCI-SAAM is modular, based on the concept of microservices, allowing for the employment of new technologies and solutions and facilitating the upgrade path of the various composing entities. Further, the use of standardized protocols ensures the relevance of the design and the ease of integration with third-party services and platforms.

8. Conclusions

In this report, the concept and initial design principles of ATLANTIS proposal towards establishing a pan-European, CCI risk-awareness/management framework, CCI-SAAM, has been presented. Effectively enabling intelligent CCI interconnection, the CCI-SAAM has the potential of significantly enhancing the security and robustness of the European CCI landscape, by leveraging on intensive data analysis towards uncovering hidden interconnections between the various CIs at pan-European level.

References

[1] Council of the European Union, "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," 08 Dec. 2008. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114. [Accessed 25/1/2024].

[2] European Parliament and the Council, "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC," 27 Dec. 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj. [Accessed 25/1/2024].

[3] European Parliament, Council of the European Union , "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 06 Jul. 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016L1148.

[4] "MeliCERTes Project - knowledge base," [Online]. Available: https://melicertes.github.io/docs/. [Accessed 20/2/2024].

[5] European Cybersecurity Competence Centre, "MeliCERTes project presented at the FIRST Annual Conference," 06 Jul. 2022. [Online]. Available: https://ec.europa.eu/newsroom/ECCC/items/752680/. [Accessed 20/2/2024].

[6] EU research results - CORDIS, "Defending the European Energy Infrastructures," [Online]. Available: https://cordis.europa.eu/project/id/740898.

[7] "Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks," [Online]. Available: https://cordis.europa.eu/project/id/832989.

[8] Introduction to STIX. [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro. [Accessed 28/2/2024]

[9] Introduction to TAXII. [Online]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro. [Accessed 28/2/2024]

[10] A. Iklody and A. Dulaunoy, "MISP core format," 1998. [Online]. Available: https://tools.ietf.org/html/draft-dulaunoy-misp-core-format-00. [Accessed 23/2/2024].

Front cover image by Gerd Altmann via Pixabay.
https://pixabay.com/users/geralt-9301