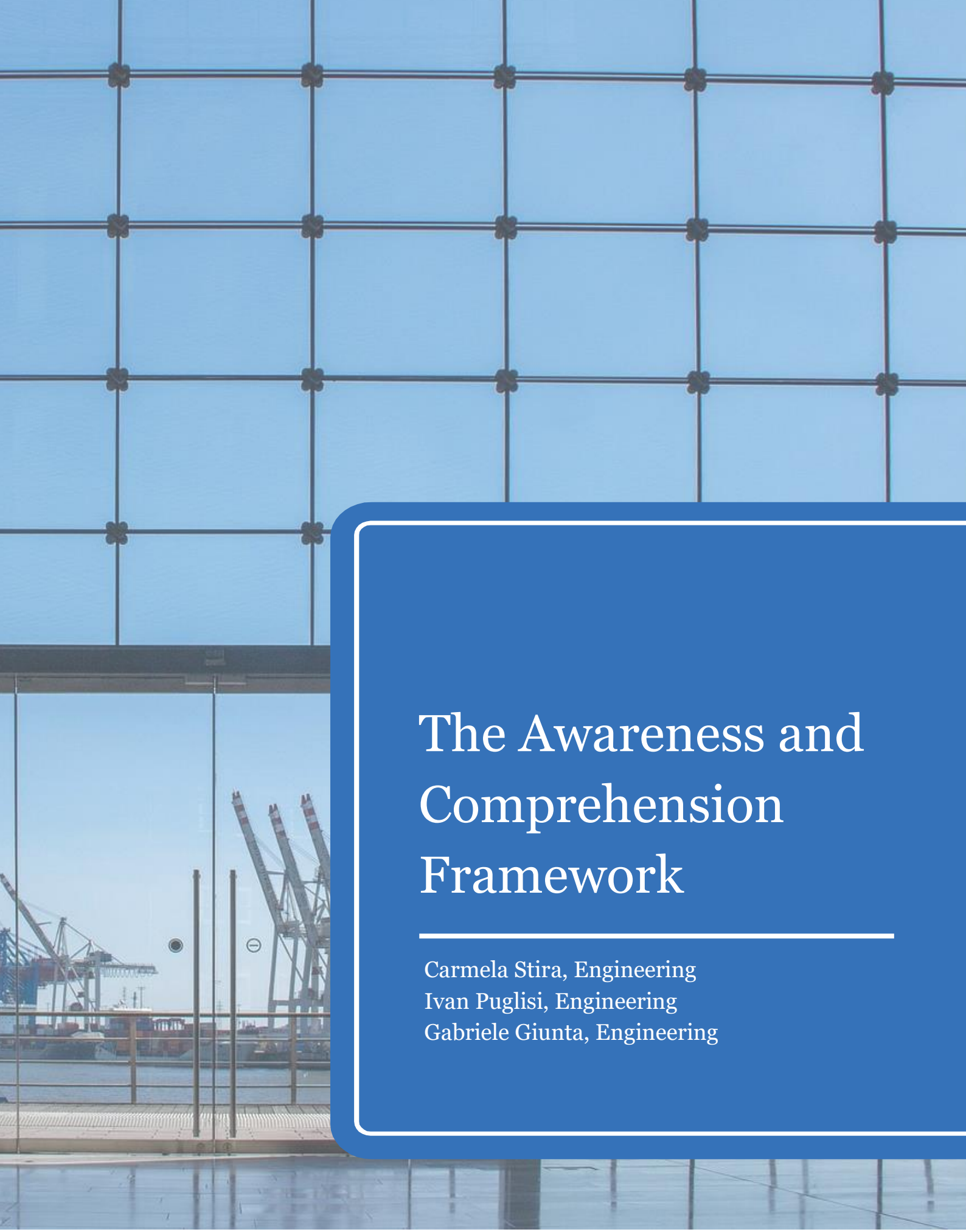

The Awareness and Comprehension Framework

Carmela Stira, Engineering
Ivan Puglisi, Engineering
Gabriele Giunta, Engineering

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 Awareness and Comprehension Framework

Carmela Stira, Ivan Puglisi, and Gabriele Giunta (Engineering)

The construction of distributed Situation Awareness is crucial for optimized incident management in critical infrastructures, aiming to support the decision-making phase and enable a prompt response from the relevant stakeholders. The Awareness and Comprehension Framework adopted within the ATLANTIS project utilizes correlation rules and AI models to create a comprehensive representation of the situation based on information derived from the heterogenous sources.

1. Introduction

Situation Awareness (SA) in risk management systems is crucial for obtaining a comprehensive and global understanding of 'what is happening' in the examined system, especially in the case of incidents. It helps operators gain a complete overall picture of the current situation and supports them in making timely and effective decisions in response to unforeseen events or emerging threats. Additionally, it enables efficient resource management by providing detailed information about the critical aspects of the situation and the incident management priorities. Of particular interest in the context of risk management in critical infrastructures (CIs) is the *system-level* SA, which is derived by aggregating and correlating the *individual* SA coming from the different actors involved in the CI protection. Distributed or system-level SA indeed promotes coordination among CI operators involved in risk management, enhancing their communication, collaboration, and synchronization through the exchange of meaningful information.

Therefore, the Awareness and Comprehension Framework (ACF) has a crucial role within the ATLANTIS security system as it can provide a distributed situational picture through the adoption of automated processes analyse real-time data, overlaying information collected during risk assessment, and applying optimized models derived from the study of significant historical events and the experience of domain operators.

Building upon research outcomes obtained in previous projects related to critical infrastructures protection (i.e., H2020 INFRASTRESS[1], H2020 7SHIELD[2], H2020 PRECINCT[3]), within the ATLANTIS project an innovative approach is being adopted. This approach is based on the use of optimized AI models and the adoption of a Digital Twin methodology, which creates a virtualized image of the system/systems to be monitored and protected.

[1] https://cordis.europa.eu/project/id/833088
[2] https://cordis.europa.eu/project/id/883284
[3] https://cordis.europa.eu/project/id/101021668

2. The Current State of Affairs in Awareness and Comprehension Frameworks

The literature on the application of situational awareness frameworks to risk management is quite limited and lacks studies with generalized solutions [1]. The lack of material and research on the practical implementation of SA in the context of risk assessment, compared to theoretical and methodological research (highlighted in Section 0), is related to the fact that organizations and companies are unwilling to share sensitive information regarding their systems, given the sensitive nature of the topic [2][3].

However, existing studies have highlighted how physical and cyber or hybrid security risks are generally estimated with little reference to the situational awareness of the system relative to the organization in which it is contextualized, and that the assessment of security risk data is not carried out continuously and especially not historically [4][5].

Within the ATLANTIS project, ACF will be based on theoretical studies and models, but it is oriented towards a practical approach useful for continuously monitoring and managing risks in order to minimize its impact and share the acquired knowledge to optimize present and future processes.

3. The Role of Awareness and Comprehension Framework

An effective emergency response to any type of physical, cyber, or cyber-physical threat relies on the ability to understand '*what is happening*' in the system under consideration. Effective risk management, therefore, depends on understanding what is happening and, consequently, on the representation of situational awareness, which, in turn, relies on the ability to quickly organize, understand, and assimilate vast amounts of data from various elements composing the system under consideration.

In a study evaluating information security practices, it emerged that the majority of security incidents were indirectly caused by a lack of situational awareness [6]. Adequate situational awareness provides a comprehensive understanding of the situation related to the critical infrastructure element under examination and the environment it interacts with. It also involves a correct interpretation of information from the system, enabling those involved in risk management to operate effectively in their context and take the necessary actions to address current issues and prevent future ones.

Furthermore, to provide the most efficient response to a crisis, it is essential for operators from different organizations to communicate effectively and share information to achieve situational awareness. Studies on distributed cognition indicate that, during collaborative problem-solving, a shared cognitive understanding within the group facilitates the discovery of solutions.

Accurate situational awareness relies on the observer's ability to organize and analyse data from various information sources to understand what is happening in the process. Making timely and correct decisions depends on the ability to build a good understanding of the current situation and, consequently, on the ability to transform heterogeneous data from

different sources into structured and useful information for situation management (Figure 1 below).

The available contextual data must be transformed into useful information to achieve the goal and must be processed and interpreted based on experience and the specific environmental context. Achieving this goal depends on understanding how people process and use information in their decision-making activities.

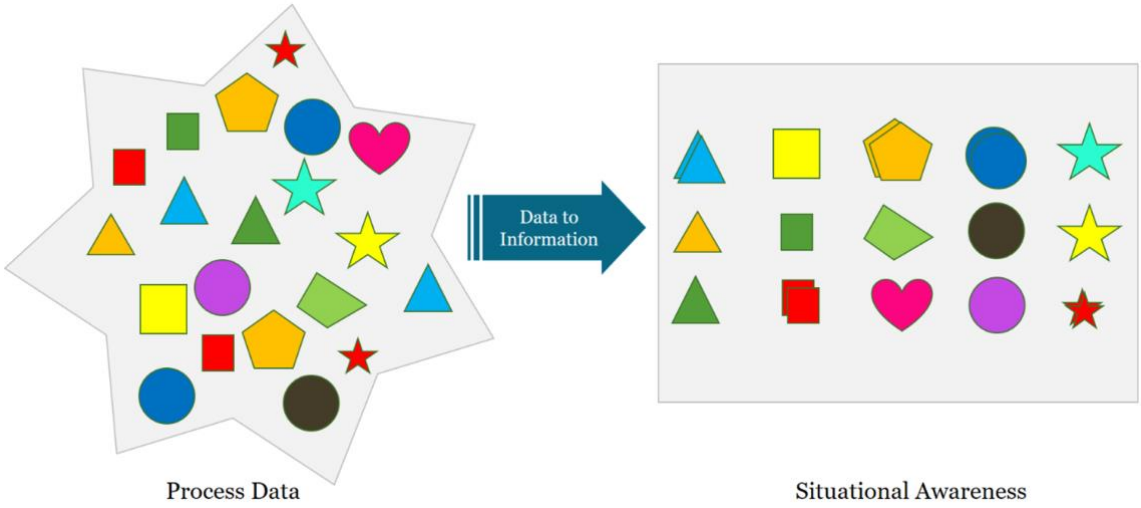

Figure 1. The informational gap.

The purpose of ACF is therefore to provide a tool capable of quickly analysing real-time data provided by the interconnected sources, so as to aggregate and correlate them even along with risk and resilient data collected during the preparedness phase, in order to construct an effective model of the current situation that highlights relevant features for swift risk management. In doing that, ACF will make use of predefined rules, models, and/or patterns derived from the analysis of historical information and interdependencies within the domain context of the system under consideration. Moreover, the framework leverages the use of AI methodologies capable of applying supervised, unsupervised, and semi-supervised machine learning models to determine the relevant features for building situational awareness.

4. The Research and Development Path in ATLANTIS

The research conducted for the development of a situation awareness component within various projects for the protection of critical infrastructures (e.g. H2020 DEFENDER, H2020 INFRASTRESS, H2020 7SHIELD, H2020 PRECINCT) focused on building a distributed situational representation obtained through the automatic processing of information collected during the pre-crisis, crisis, and post-crisis phase. The initial version of the situational awareness component developed within the aforementioned projects was focused on the information and events processing through the application of correlation rules based on the risk and resilience assessment, questionnaires proposed to critical infrastructure security experts, and the experience gained in various testing sessions.

This approach has yielded good results in terms of situational awareness. However, it heavily depends on the specific application context, even though new rules can be configured and

added based on the specific infrastructure under analysis. Achieving completeness in rule development, however, is a rather complex task. Consequently, within the ATLANTIS project, a study is being conducted to add rules and AI models to support the situational picture preparation. In particular, by utilizing training data provided by CI organizations and security experts, it is possible to effectively train ML models to support the situational picture and calculate values for those attributes characterizing the situation, effectively aiding the incident management phase.

In Figure 2, the ACF architecture, also referred as SAFER (Situational Awareness Framework for Emergency and Resilience), is depicted, thus utilizes:

- Information collected during the pre-crisis phase:
    - *Risks*: A list of taxonomically defined and agreed-upon hazards identified for the examined infrastructures.
    - *CI Elements*: Models of the elements characterizing the infrastructure in question, such as assets and areas.
    - *CI interdependencies* between infrastructures and elements within infrastructures.
- ML models trained based on historical data related to events characterizing situations of normalcy, criticality, and incidents from the examined infrastructures.
- Any additional information from other involved systems (e.g., social media) or the knowledge platform.
- Real-time information from the detection layer, i.e., from sensors monitoring the system or from humans in the vicinity (through specific apps developed for this purpose).

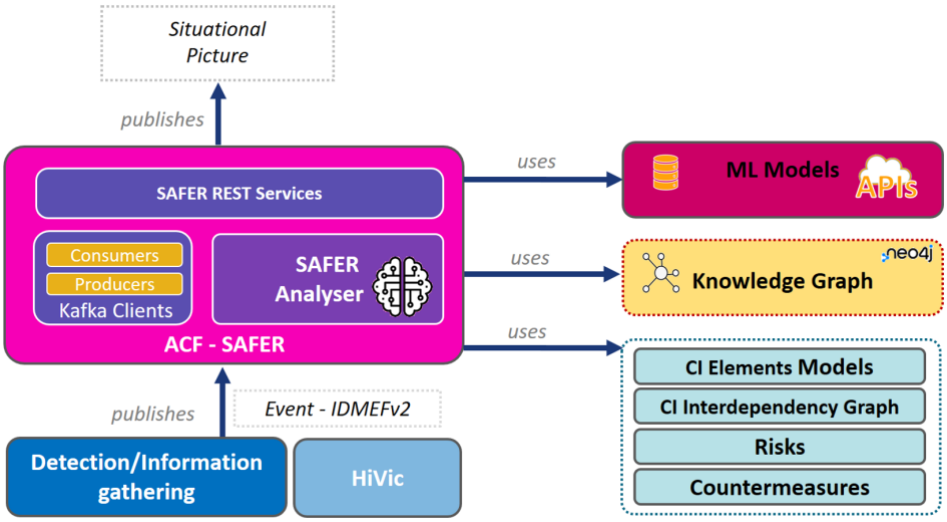

Figure 2. ACF architecture.

5. The Challenges and Barriers

The main challenge lies in selecting machine learning models suitable for the situational picture generation. These models will be generally designed starting from the risk management domain and will be customized based on the specific critical infrastructure, among those planned during the solution's experimentation phase. The model generation process involves, in a very early stage, the collection and analysis of data within the specific domain context. Within the project, the lack of training data for ML models has been highlighted as a risk, in terms of significant data and historical data availability. To manage the risk in the initial project phase, several strategies were proposed, such as reusing data from other projects operating in the same domain or similar contexts (e.g. 7SHIELD, PRECINCT, etc.) or generating synthetic training data through the adoption of generative ML algorithms. Models generated using alternative strategies can be effectively used to test the solution during the initial experimental phases, while in more advanced stages, the models can be refined by overlaying data emerging during pilot trials or data collected from previous experiments.

6. The Benefits and Impact

The main benefit of ACF is the enhancement of the incident response management processes and the assessment of the timeliness of the operational and decision-making phases, where the three elements of the situation awareness, namely perception, comprehension, and projection, play a crucial role in shaping an overall situational picture.

At the present time, main challenges are focused on developing well-trained machine learning models capable of analysing incoming data from the detection tools such as IoT sensors, automated cybersecurity tools and CCTV cameras, as quickly as possible to obtain all the information necessary for an effective incident management. The adopted model thus allows for a smooth integration of new components, as long as they adhere to the defined

interface specifications. Consequently, the proposed solution is highly scalable, flexible, adaptable, and resilient to emerging system requirements.

7. Future Outlook

New ML models will be selected and analysed in the future as well as the study of historical data from the system to be protected will be intensified. Moreover, it has been decided to implement a mechanism to externally inject machine learning models into the ACF system, making it adaptable to different application contexts and evolvable through the application of new models. In this light, the architectural choice to allow the injection of machine learning models from external sources, provide a higher level of flexibility and adaptability since it is possible to model, train, and apply specific models based on the infrastructural context in which the system operates.

8. Conclusions

Research on situation awareness has highlighted how a *system-level* understanding of the situation is crucial in supporting risk management and facilitating coordination among operators in response and mitigation activities. The situation awareness model is inspired by the descriptive model proposed by Endsley in the context of decision-making systems, based on the three phases of perception, comprehension, and projection.

The Situational Awareness and Comprehension framework is implemented through the SAFER component, a tool capable of quickly analysing relevant real-world information and generating a model of the situational picture that highlights features crucial for swift risk management. Updates to the situational model are published in the system through the use of a broker following the publish-subscribe model. Additionally, the SAFER component employs AI techniques, particularly ML models that are appropriately built and trained with data from the systems under examination, within the scope of the ATLANTIS project's experimentation. The situational model can be further enriched by the DSS (Decision Support System), thereby adding value to specific characteristics such as severity and priority, with the aim of optimizing the decision-making phase and the implementation of risk mitigation strategies by the risk reduction system.

References

[1] A. G. Kotulica, J.G. Clark (2004), Why there aren't more information security research studies, Department of Information Systems, The University of Texas at San Antonio (USA)

[2] D. B. Parker, Risks of risk-based security, Comm. ACM, 50 (3) (2007), p. 120.

[3] P. Shedden, R. Scheepers, W. Smith, A. Ahmad, Incorporating a knowledge perspective into security risk assessments, VINE J Inf Knowl. Manag. Syst., 41 (2) (2011), p. 152.

[4] D. M. Utin, M.A. Utin, J. Utin, General misconceptions about information security lead to an insecure world, Inf Secur. J A Glob Perspect., 17 (4) (2008), pp. 164-169.

[5] A. Ahmad, J. Hadgkiss, A.B. Ruighaver, Incident response teams – challenges in supporting the organizational security function, Comp. Secur., 31 (2012), pp. 643-652.

[6] Endsley, M. R. (1990), Situation awareness in dynamic human decision making: Theory and measurement (doctoral dissertation). Los Angeles, CA: University of Southern California.

Front cover image by Erich Wirz via Pixabay.
https://pixabay.com/users/ewirz-74614