Situational Awareness for CPS

Cristina Alcaraz
Computer Science Department,, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
alcaraz@lcc.uma.es,

1 Synonyms

Anomaly detection; prevention; response; attack traceability; visualization.

2 Definitions

The ability of the system to collect data from multiple heterogeneous sources and understand the current state of a system over a period of time and space. This information can come from the cyber world and the physical world, including the interconnection of both worlds and human interactions. In critical scenarios, this process can even require proactive traceability mechanisms and reliable visualization for better decision making and business continuity.

3 Background

Situational awareness is a research field that has been widely considered for various types of applications (e.g., emergency management, (cyber-)defense, etc.) during the last three decades, and especially for the field of Industrial Control Systems (ICSs). The capabilities of the situational awareness allow the system to address the life cycle of an attack, from its prediction or detection to its mitigation. This aspect even becomes more relevant for complex and critical infrastructures, such as ICSs composed of Cyber-Physical Systems (CPSs), with high human interaction.

Multiple risks may arise not only in the cyber part but also in the physical part where both worlds converge thanks to the new communication systems, leading to serious interruptions in the final services. This is largely due to the fact that these three domains (cyber, physical and networking) are actually three areas that are highly susceptible to multiple kinds of threats. These threats may come from typical deviations caused by human errors, misinterpretations of the situation and malfunctions, to diverse cyber kill chains (e.g., advanced persistent threats) led by advanced attackers with resources and skills to exploit 0-days vulnerabilities ([4]). In these circumstances, it is clear to understand the importance of enhancing situational awareness and improving decision making for a suitable (automatic, semi-automatic or manual) response. Any defensive action can certainly be beneficial for business continuity, in which the provision of minimal services and their distribution to the end-users are, certainly, critical.

To understand the main functionality of a situational awareness-based system, it is first necessary to go to the original concept coined by Mica [2]. The concept comprises "*the perception of the elements of the environment within a volume of time and space, the understanding of their meaning and the projection of their state in the near future*". These three levels (perception, comprehension and projection) are still applicable with the exception that their integration depends on the type of application scenario, its restrictions, interactions and complexities as stated by [4]. In the case of critical infrastructures, [1] address this issue by additionally including recovery and self-learning approaches in the situational awareness process. The goal here is to guarantee protection 24/7 in large and extended environments, and therefore resilience.

4 Application

So far, there are available several guides (e.g., [5, 4]) and methodologies (e.g, [1]) to apply situational awareness in critical scenarios, identifying the main software components and technologies for awareness automation. In this case, various techniques would have to be considered to normalize, clean, process and correlate large volumes of data from various heterogeneous sources. But apart from this, it is also necessary to respond accordingly, trace threats or anomalies, and feed back all awareness for self-learning through machine learning and artificial intelligence with support for risk management and attack analysis. This also means that the integration of situational awareness mechanisms into CPS-based systems becomes an extremely complex task.

A good practice would be to design systems that are decoupled from the control processes with guarantees for a rapid automation and autonomy for protection. This protection should not only cover anomaly detection and event monitoring in the physical and logical world, but also the implication of measures that help anticipate a clearer and accurate decision-making. A misinterpretation of the situation may trigger a devastating effect on a critical system. For this reason, [3] underline the relevance of the Game Theory to improve the effectiveness of the situational awareness and its integrated components, together with training programs combined with cyber-defense exercises and command and control exercises.

This way of verifying the primary functions of the situational awareness can even benefit the feedback from the entire awareness process. For example, cyber range models could not only guarantee human operators' training, but also update awareness mechanisms with new attack techniques, strategies and potential risks.

CPS-based critical infrastructures can also share or notify situations, configurations and threats between them so as to expand functionalities and skills. Therefore, situational awareness is a research area with great possibilities to be merged with other application fields such as cyber threat intelligence, cyber intelligence for defense, cybercrime or risk management.

5 Open problems and future directions

Although situational awareness is nowadays a very considered research area in the literature and especially for the cyber part, its current application in critical applications is not so trivial as expected. Cyber-physical systems have strict control requirements in which security is vital to reduce risks but its implication should not impact on the primary functions required for control. Therefore, one of the pending issues for the future is to find lightweight solutions that address not only the cyber and networking part but also the physical part and the diverse interactions.

Other questions that remain open would be how to apply the new technologies of Industry 4.0 and its paradigms to accelerate the computational logic of situational awareness processes; decouple functionalities with control systems; and ensure adequate awareness of the situation and better performance in the field. In this sense, situational awareness can be supported by diverse technologies. For example, computing paradigms (edge, fog, cloud) could allow to centralize or distribute the main computing functions; virtualization paradigms, such as digital twins, could aid to pre-compute, simulate, and anticipate malicious scenarios; Big Data and artificial intelligence can provide the system with greater intelligence and autonomy against potential threats; distributed ledger technologies can make sure the immutability of events registered or their sharing with other entities; or consensus techniques for real-time traceability of a threat, diagnostic and health management.

Related to Big Data, it is also necessary to protect access to private data produced in a critical environment and from the misuse of machine-learning techniques that can corrupt the privacy of an organization or organizations. Likewise, the use of the new Industry 4.0 technologies to enhance the situational awareness should not infringe the intellectual property of an organization, especially when digital twins are part of the logical of the situational awareness. Any threat in the digital twin may not only affect the good performance of the awareness process but also put the 'physical' world and the intellectual property at risk. For this reason, security measures, around the situational awareness, are essential to guarantee a low rate of false positives or negatives, as well as the integrity and availability of resources and data.

Apart from this, there is still a significant dependence on human interactions, where decision making must be objective according to the decisions made by human being. Therefore, this issue still remains open and it is required creating trustworthy systems, the responses of which have to be suitable to spread full trust in the system and delegate automatic actions. There are no specific standards of situational awareness either, and especially for cyber-physical systems and critical infrastructures. There are only some guides on how to apply the concept, considering some security nuances for access control, good use of resources and data accessibility.

References

[1] Cristina Alcaraz and Javier Lopez. Wide-area situational awareness for critical infrastructure protection. *IEEE Computer*, 46(4):30–37, 2013 2013.

[2] Mica R Endsley. Toward a theory of situation awareness in dynamic systems. *Human factors*, 37(1):32–64, 1995.

[3] Ulrik Franke and Joel Brynielsson. Cyber situational awareness–a systematic review of the literature. *Computers & security*, 46:18–31, 2014.

[4] Blaine Hoffman, Norbou Buchler, Bharat Doshi, and Hasan Cam. *Situational Awareness in Industrial Control Systems*, pages 187–208. Springer International Publishing, Cham, 2016.

[5] McCarthy James J., Alexander Otis, Edwards Sallie, Faatz Don, Peloquin Chris, Symington Susan, Thibault Andre, Wiltberger John, and Viani Karen. Situational Awareness for Electric Utilities. National Institute of Standards and Technology, Special Publication (NIST SP) - 1800-7, 2019.