Identification and Evaluation of Cyber-Physical Threats on Interdependent Critical Infrastructures

Sandra König
Austrian Institute of Technology
Vienna, Austria
Sandra.Koenig@ait.ac.at

Abdelkader Magdy Shaaban
Austrian Institute of Technology
Vienna, Austria
Abdelkader.Shaaban@ait.ac.at

Tamara Hadjina
Končar - Digital
Zagreb, Croatia
tamara.hadjina@koncar.hr

Klemen G. Gregorc
KABEG
Klagenfurt, Austria
klemen.gregorc@kabeg.at

Albert Kutej
KABEG
Klagenfurt, Austria
albert.kutej@kabeg.at

ABSTRACT

Increasing interdependencies between critical infrastructures and digitization increase the vulnerability to cyber-attacks and cyber-physical attacks. Incidents have multiple direct and indirect consequences, including cascading effects, and a formal analysis is strongly recommended to understand these effects. This paper shows how threat identification and impact evaluation for interdependent critical infrastructures can be supported by two existing tools. The approach is illustrated with an example based on a running EU project.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

threat identification, risk modelling, cascading effects, impact estimation, simulation

ACM Reference Format:
Sandra König, Abdelkader Magdy Shaaban, Tamara Hadjina, Klemen G. Gregorc, and Albert Kutej. 2023. Identification and Evaluation of Cyber-Physical Threats on Interdependent Critical Infrastructures. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3600160.3605026

1 INTRODUCTION

Protection of Critical Infrastructures (CIs) is challenging for many reasons. A CI consists of numerous cyber and physical components that influence each other. CIs depend on one another and exchanges goods and data [22]. Recent incidents [4, 15, 21] rose the awareness of cyber-attacks and their impacts in both cyber and physical domain [12].

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605026

The analysis of threats to interconnected critical infrastructures contains two major steps: identification of threats and evaluation of these threats. Both can be supported by existing tools. ThreatGet is a tool that allows a static threat identification [1]. Threat Propagation Engine (TPE) [2] is a simulation framework that mimics how a threat can propagate through interdependent CIs.

In this paper we show how these two tools can be combined to identify and analyse threats in interconnected CIs. The approach is illustrated through an example inspired by a pilot case in the EU funded project PRAETORIAN [20].

2 RELATED WORK

Recent incidents increased the awareness of CI operators to cyber-attacks and advanced attacks such as Advanced Persistent Threats (APTs) [26]. Such incidents demonstrated the need for robust approaches for identifying, assessing, and mitigating cyber risks [7]. Currently, these tasks are often treated domain-specific [9]. The ThreatGet tool can be utilized to identify cyber threats across various scientific fields, including automotive, railways, Cyber-Physical Systems (CPS), Internet-of-Things (IoT), and other domains [24]. In the course of PRAETORIAN it has been extended to also detect physical threats.

Cyber and physical threats to critical infrastructures are discussed in multiple scientific contributions. Various attributes of cyber attacks in CI are summarized in [17] and an applicable set of protection mechanisms for mitigating these risks is provided. In addition, an analysis of the cyber vulnerabilities of Critical Energy Infrastructures systems is presented in [19]. The authors highlighted the different cyber vulnerabilities in critical energy infrastructures where cyber-attacks occur.

Recent incidents have also demonstrated far-reaching consequences of physical incidents [18], but also of cyber attacks such as the Wannacry ransomware [5] and the NotPetya malware [8] or targeted attacks [6]. The TPE allows estimation of impacts of a cyber, physical or cyber-physical threat [23]. The simulation is based on a probabilistic model of threat propagation [11] that combines information from various operators and experts about the local situation to get a holistic view. It is a generalization of a model of malware spreading through a heterogeneous network [13].

3 THREAT IDENTIFICATION

Due to the high complexity of interdependent CIs and the increasing cyber threats, a formal threat identification process is crucial. In this work, we use ThreatGet because it provides an innovative rule-based approach for identifying cyber threats in system models. ThreatGet is a threat modeling tool developed by the Austrian Institute of Technology [1]. The tool uses a system model and formal rules to identify security vulnerabilities that may result in unforeseen negative consequences. It has been developed in the context of automotive security.

Therefore, as part of our research activities in the PRAETORIAN project [20], we have developed a catalog of components for the CIs that encompasses a wide range of system components. These components can be utilized to model different CI models. Each component within the catalog is accompanied by a set of security properties, which are defined as a collection of protection mechanisms designed to address various cyber incidents.

The tool manipulates a threat database comprising a wide range of cyber threats described in a dedicated language developed to imitate the behavior of cyber incidents within the connected system components. The threats are described as rules, which can be utilized by ThreatGet's rule engine to identify existing security vulnerabilities in the system models. ThreatGet was mainly focused on cyber threat investigation, but in the PRAETORIAN project, we extended the capabilities of ThreatGet to include physical threat investigations as well. Furthermore, we update and enhance this database to ensure its relevance in addressing cyber and physical threats related to CI.

The rule engine of ThreatGet plays an essential role in the process of identifying and analyzing threats. It applies all the rules defined in its threat database to the given system model in order to identify any potential cyber and physical threats that could propagate through the system network. These rules assist in determining whether any of the applied security properties for each system component or connection could be violated as a result of cyber incidents.

In addition, ThreatGet automatically determines the severity level of each identified threat and estimates the overall risk within the model. The overall risk estimation highlights all security issues that require more security concerns [24].

3.1 Model for Threat Identification

A model of a CI system using the ThreatGet catalog describes the cyber and physical components, as well as the interconnections between them. This paper uses a running example that describes in detail a power plant and a hospital and some first responders on a higher level, i.e., as a single element, as shown in Figure 1.

The model describes the interconnections between physical and cyber components in the power plant (upper part) and the hospital (lower part). Physical components include an entrance *Gate*, the *Flood Gate* that controls the water stream before passing the *Dam* at the power plant and a *Water Sensor* at the hospital that detects a possible rise of the water level. Cyber components include components that manage and control the information flows between the interconnected system parts within these premises. For example, the IT System manages the patient records and stores any related medical data. This component includes an asset called *Sensitive Data*

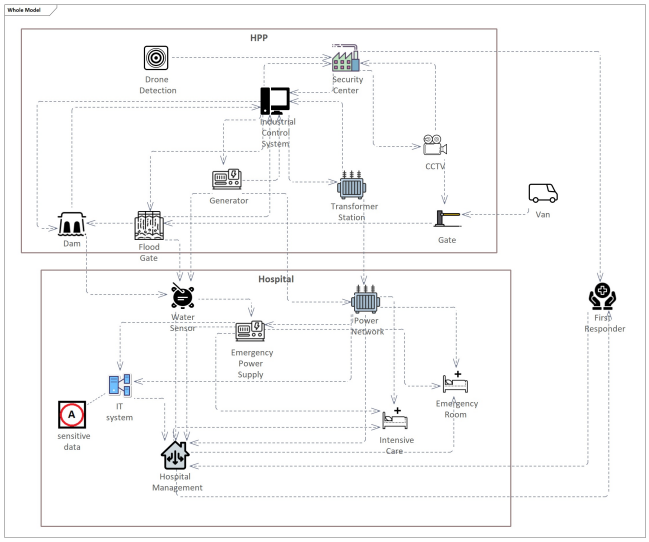

Figure 1: ThreatGet model for power plant and hospital

(illustrated by the letter "A"). This asset represents a critical element within our system model that requires more security attention. It indicates that the *IT System* has classified data that could be prone to any potential cyber risks. The next section shows the potential cyber-physical threats identified by ThreatGet due to violation of security properties.

3.2 Identified Threats

ThreatGet facilitates threat investigation to identify potential cyber and physical threats within the system model that may target specific component or assets. Each component and asset contains a wide range of security properties describing protection mechanisms for addressing cyber-physical incidents. ThreatGet determines potential cyber-physical threats that violate any of these properties and lead to any successful cyber-physical attacks. According to the previously discussed CI network model, shown in Figure 1, the tool identifies a set of cyber and physical threats. Table 1, shows a selection of threats identified by ThreatGet.

As shown in Table 1, each threat has an impact on a specific cyber or physical component within the system model by compromising one or more of its security properties. For instance, the first threat, "Illegal processing of data," violates the authorization mechanism of the hospital's IT system, which could potentially jeopardize the confidentiality of sensitive patient records stored within that component. The sensitive data is considered a critical asset; therefore, it is defined in Table 1 as an affected asset that requires additional protection.

The threat "Vulnerability due to absence of backup for sensitive data" is another cyber threat that can impact the IT system in the hospital. This threat could be triggered if no defined data backup for a hospital's sensitive information, such as patient medical records. Furthermore, a potential cyber attack on the hospital's IT system could lead to the loss of sensitive information and potentially to the demand of a ransom.

Table 1: Selected cyber and physical threats according to ThreatGet's outcomes

Cyber Threats				
#	Threat Title	Affected Components	Affected Assets	Violated Properties
1	Illegal processing of data		sensitive data	Authorization
2	Vulnerability Due to Absence of Backup for Sensitive Data	IT System hospital	————	Data Backup
Physical Threats				
1	Unauthorized access to critical premises	Power Plant gate	————	Physical Access Control
2	Damage Dam risk	Dam	————	Physical Access Control

ThreatGet also identifies threats related to malicious physical actions. The first threat in the Physical Threats category, "Unauthorized access to critical premises", occurs when there is a violation of the physical access control security property at the power plant gate. That could lead to multiple consequences because an unauthorized person can enter a critical location like the power plant. Another physical threat identified by ThreatGet is the "Damage Dam risk," which compromises the physical access security control of the dam.

4 THREAT EVALUATION

In this section we investigate the consequences of some of the detected threats. For this we use a probabilistic model that estimates the impact of an incident in a network, which is described in the next section. While the threat identification requires qualitative knowledge, i.e., a formal model of the infrastructure and rules describing dangerous configurations, the simulation of effects is based on a probabilistic model since precise predictions are hardly possible in such a complex environment. Parametrization of the model (i.e., estimation of the probabilities) is time-consuming because expert knowledge is needed, but involving domain experts is crucial to build a model that is close to reality (and therefore useful).

4.1 Probabilistic Impact Estimation

At the core of the impact estimation is a graph model that describes the interdependnecies between the CIs, called *interdependency graph*. It models the different CIs, or relevant components of CIs, as nodes and the dependencies as directed edges. The direction of the edge corresponds to the direction in which the problem propagates, i.e., an edge $X \longrightarrow Y$ means that a problem in X may affect Y. Interdependencies can be physical, e.g., all CIs need power to operate smoothly, but also include exchange of information, e.g., if a control system is used to supervise physical processes.

The interdependency graph of the considered example that is shown in Figure 2. It differs from the ThreatGet model in Figure 1 since it describes how a problem propagates in a network rather than understanding how problems can occur. In particular, the interdependency graph does not have assets (as the TheratGet model). Instead, other elements like humans or logical objects can be included in the model, if it is relevant for the scenario (e.g., in case of a social engineering attack).

How much a node is affected by an incident is described through a *state*. The state represents the functionality or availability of a

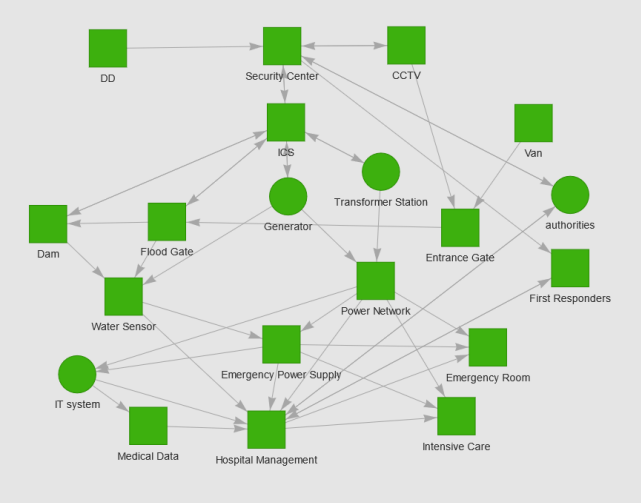

Figure 2: Simulation Model for Threat Analysis

node (depending on the nature of the node) and is described through an integer between 1 (best) and 5 (worst), where intermediate states correspond to different degrees of impact.

The state of a node can change due to an incident. In the propagation model [11] these changes are assumed to be probabilistic since precise predictions are practically impossible in such a complex network with a huge number of influencing factors (such as weather, time of attack etc.). Formally, for each possible threat a transition matrix describes the reaction of the node to this threat, e.g., T_{ICS} shown below for 3 states.

$$T_{ICS} = \begin{pmatrix} 0 & 2/3 & 1/3 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}.$$

The i−th row gives the distribution of the next state if the node is currently in state i, i.e., t_{ij} is the probability that the node switches from i to j due to the incident.

There are multiple ways to estimate the transition probabilities, depending on the amount of data that is available [14].

This reaction of a node to the considered threats is called *local dynamics*, since it describes the local reaction. The simulation triggers one node by sending a threat message to it, If the node reacts by changing its state, it sends a notification to all neighbours and these may in term react to the problem of this node. With this it is

possible to understand the global dynamics, including cascading effects.

In the next section, we apply this simulation model to the considered example to analyse some of the identified threats.

4.2 Impact Estimation for Selected Threats

The threats identified in Table 1 are analysed in this section with the simulation model described in the previous section. For our analysis we use an implementation done by the Austrian Institute of Technology [2] in course of the PRAETORIAN project. The current implementation allows visualization of the graph on a map by adding coordinates to the nodes. We refrain from doing so here because such data is sensitive and the benefit of the tool can be shown without coordinates.

For each threat, 100 simulations were run to estimate the impact. The timeline of one example run is shown to demonstrate how the network changes over time, and the consequences are described. We also give some context to illustrate how such attacks could happen. These descriptions are either based on existing reports and on our imagination, so they do not necessarily represent any real threats.

4.2.1 Manipulation of Control System. Attacks on Control Systems occur these days in many sectors, including the energy sector [3, 16]. A simulation run for an attack on the power plant's Industrial Control System (ICS) is shown in Figure 3. If the ICS of the power plant

Time	Entity Name	Event	New State	Because Of
0	ICS	Manipulation of Control	3	
1	Security Center	Manipulation of Control	3	ICS
1	Generator	Manipulation of Control	2	ICS
1	Transformer Station	Manipulation of Control	2	ICS
2	Power Network	generator limited	2	Generator
2	Power Network	transformer station limited	3	Transformer Station

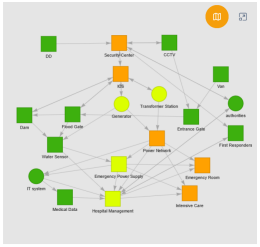

Figure 3: Simulation of manipulation of ICS

is manipulated, then it is possible that generator and transformer station have problems due to the lack of control. In that case, power generation might be limited, which may cause problems at the hospital, in particular in the intensive care unit.

4.2.2 Unauthorized Drone. A drone is detected by a drone detection system (DD). A simulation run for this event is shown in Figure 4. Employees check if this drone is allowed (e.g., for inspection [25]) or not. If it is considered malicious, the security center is informed and potentially also the authorities because other CIs in the area might also be target to an attack. Even though this event does not spread very far in the interdependency graph, it marks the security center of the power plant and the authorities alerted (yellow to orange, depending on the level) and more attention is given to possible subsequent events like an attempt to get access to the power plant.

Time	Entity Name	Event	New State	Because Of
0	DD	drone detection	4	
1	Security Center	malicious drone	3	DD
2	authorities	malicious drone	2	Security Center

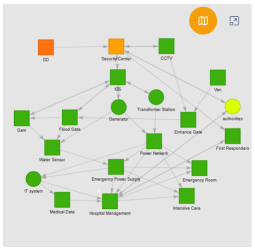

Figure 4: Simulation of detection of a drone

4.2.3 Unauthorized Vehicle. A vehicle is checked at the entrance gate. If it were unauthorized and still gets access to the power plant, attackers could damage the dam. A simulation run of this attack is shown in Figure 5. If the van is unauthorised and successfully passes

Time	Entity Name	Event	New State	Because Of
0	Entrance Gate	vehicle detection	4	
1	Flood Gate	unauthorised vehicle	4	Entrance Gate
2	Dam	flood gate damaged	2	Flood Gate
2	Water Sensor	flood gate damaged	3	Flood Gate
3	Hospital Management	water level high	2	Water Sensor
3	Emergency Power Supply	water level high	2	Water Sensor

Figure 5: Simulation of detection of a vehicle

the gate, it could damage the flood gate. This would cause a flooding in the surrounding area. In the considered scenario, such a flooding might affect a hospital (which is discovered by the water sensor in the basement). Due to the high water level in the basement, the emergency power supply might be disrupted. If the water sensor notices a high water level, the hospital management is informed.

4.2.4 Ransomware Attack. In a situation like a flooding, attackers may use the stressful situation to start a ransomware attack on the IT system of the hospital. A simulation run is shown in Figure 6. If

Time	Entity Name	Event	New State	Because Of
0	IT system	Ransomware	3	
1	Medical Data	Ransomware	4	IT system
1	Hospital Management	Ransomware	3	IT system
2	authorities	Ransomware	2	Hospital Management

Figure 6: Simulation of ransomware attack on IT System

the ransomware attack is successful, attackers get access to sensitive data (such as medical data from patients). Such an attack affects the hospital management as working without access to patient data is challenging. The management will have to inform authorities.

Besides the concrete descriptions of individual simulations (as shown in Figures 3 to Figure 6) it is also possible to learn from the statistics of all simulation runs of the same scenario. The relative frequency of the states, i.e., how often a node is affected how badly, provides information on which nodes might need better protection. It is also possible to combine such an impact assessment with resilience frameworks [10].

5 CONCLUSION AND FUTURE WORK

This paper proposes the combination of two existing tools to identify cyber and physical threats in CI networks and to estimate the impact of these threats. The threat identification uses a database of rules that describe possible threat scenarios and checks if these rules apply for the current system. This enables a systematic threat identification. The impact of the identified threats is assessed based on a stochastic model that describes the possible direct and indirect effects. Simulation of such effects allows identification of cascading effects and provides estimates of the impact for each component. In course of the PRAETORIAN project it became clear that especially information about intra-CI effects is of interest to CI operators. During demonstration activities, partner emphasized that early warnings about potential threats due to cascading effects is crucial to respond and reduce the impact on dependent CIs. A holistic overview on the consequences of an incident are also relevant for decision makers on a municipality or regional level when preparing against considered threats or attacks.

Future work includes the creation of new rules to detect cyber-physical threats, as well as the analysis of larger networks. A description of how the ThreatGet and the TPE support the general risk management process is in progress. It is also intended to implement an interface between the two tools to simplify the joint use in future projects.

ACKNOWLEDGMENTS

This work was done in the context of PRAETORIAN project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021274.
We wish to thank projects partners for interesting discussions and valuable insights.

REFERENCES

[1] AIT Austrian Institute of Technology. 2022. *THREATGET*. AIT Austrian Institute of Technology. https://www.threatget.com/
[2] AIT Austrian Institute of Technology. 2023. *Threat Propagation Engine*. AIT Austrian Institute of Technology. https://risk-mgmt.ait.ac.at/praetorian/
[3] Mohammed Alghassab. 2022. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector. *Energies* 15, 1 (2022). https://doi.org/10.3390/en15010218
[4] Guy Chazan. 2016. *Deutsche Telekom warns cyber attack hit up to 900,000 customers*. https://www.ft.com/content/58d8a27e-b56a-11e6-961e-a1acd97f622d
[5] Catalin Cimpanu. 2017. WannaCry Ransomware Infects Actual Medical Devices, Not Just Computers. https://www.bleepingcomputer.com/news/security/wannacry-ransomware-infects-actual-medical-devices-not-just-computers/
[6] Catalin Cimpanu. 2018-09-27. *Port of San Diego suffers cyber-attack, second port in a week after Barcelona*. https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/
[7] Critical Infrastructure Cybersecurity. 2018. Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP* 4162018 (2018).
[8] Department of Health. 2018. Investigation: WannaCry cyber attack and the NHS.
[9] Lucie Flynnova, Frantisek Paulus, and Jarmil Valasek. 2022. Threats and Resilience: Methodology in the Area of Railway Infrastructure. In *2022 IEEE International Carnahan Conference on Security Technology (ICCST)*. 1–5. https://doi.org/10.1109/ICCST52959.2022.9896580
[10] Sandra König, Lorcan Connolly, Stefan Schauer, Alan O'Connor, Páraic Carroll, and Daniel McCrum. 2022. Combining Cascading Effects Simulation and Resilience Management for Protecting CIs from Cyber-Physical Threats.
[11] Sandra König, Stefan Rass, Benjamin Rainer, and Stefan Schauer. 2019. Hybrid Dependencies Between Cyber and Physical Systems. In *Intelligent Computing*, Kohei Arai, Rahul Bhatia, and Supriya Kapoor (Eds.). Vol. 998. Springer International Publishing, 550–565. https://doi.org/10.1007/978-3-030-22868-2_40 Series Title: Advances in Intelligent Systems and Computing.
[12] Sandra König, Stefan Rass, and Stefan Schauer. 2019. Cyber-Attack Impact Estimation for a Port. In *Digitalization in Maritime and Sustainable Logistics - Proceedings of the Hamburg International Conference of Logistics (HICL)*. 163–183.
[13] Sandra König, Stefan Schauer, and Stefan Rass. 2016. A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks. Springer International Publishing, 67–81. https://doi.org/10.1007/978-3-319-47560-8_5
[14] Sandra König and Abdelkader Magdy Shaaban. 2022. Parametrization of Probabilistic Risk Models. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. ACM. https://doi.org/10.1145/3538969.3544454
[15] Eduard Kovacs. 2016. *IBM Reports Significant Increase in ICS Attacks*. https://www.securityweek.com/ibm-reports-significant-increase-ics-attacks
[16] Rajesh Kumar, Rohan Kela, Siddhant Singh, and Rolando Trujillo-Rasua. 2022. APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection* 37 (2022), 100521. https://doi.org/10.1016/j.ijcip.2022.100521
[17] Leandros Maglaras, Mohamed Amine Ferrag, Abdelouahid Derhab, Mithun Mukherjee, Helge Janicke, and Stylianos Rallis. 2019. Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures. arXiv:1901.03899 [cs.CR]
[18] Sebastian Moss. 2023. *Water leak at Paris Global Switch data center causes fire, leads to outages at Google*. https://www.datacenterdynamics.com/en/news/water-leak-at-paris-global-switch-data-center-causes-fire-leads-to-outages-at-google/
[19] Tomas Plėta, Manuela Tvaronavičienė, Silvia Della Casa, and Konstantin Agafonov. 2020. Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. (2020).
[20] PRAETORIAN Consortium. 2022. *PRAETORIAN*. https://praetorian-h2020.eu/
[21] Fahmida Rashid. 2013. *U.S. Banks Back Under DDoS Fire*. https://www.securityweek.com/us-banks-back-under-ddos-fire
[22] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21, 6 (2001), 11–25. https://doi.org/10.1109/37.969131
[23] Stefan Schauer, Thomas Grafenauer, Sandra König, Manuel Warum, and Stefan Rass. 2019. Estimating Cascading Effects in Cyber-Physical Critical Infrastructures. In *Critical Information Infrastructures Security. 14th International Conference, CRITIS 2019, Linköping, Sweden, September 23-25, 2019, Revised Selected Papers*. 43–56.
[24] Abdelkader Magdy Shaaban and Christoph Schmittner. 2020. ThreatGet: New approach towards automotive security-by-design. In *IDIMT-2020 Digitalized Economy, Society and Information Management* (Kutná Hora, Czech Republic, 2020-09-02). 413–419. https://idimt.org/wp-content/uploads/2020/07/IDIMT_proceedings_2020.pdf
[25] FORCE Technology. 2023. *Drone inspection of power and hydro power plants*. https://forcetechnology.com/en/services/inspection/drone-inspection-of-power-and-hydro-plants
[26] Gordon Thomson. 2011. APTs: a poorly understood challenge. *Network Security* 2011, 11 (Nov. 2011), 9–11. https://doi.org/10.1016/s1353-4858(11)70118-0