A survey on cross domain threats of the NIS directive sectors: the transportation sector case study

Andreas Menegatos[1] [0000−0002−2469−5535], Konstantinos Maliatsos[2] [0000−0002−8823−018X],

[1] Department of Digital Systems, University of Piraeus, Greece
amenegatos@unipi.gr

[2] Department of Information and Communication Systems Engineering, University of the Aegean, Greece
kmaliat@aegean.gr

Abstract. The Network and Information Systems (NIS) Directive is designed to enhance the security and resilience of critical infrastructure systems, such as energy, water, and transportation networks, by mandating organizations to implement appropriate security measures and report certain security incidents. Threat modeling plays a pivotal role in the context of the NIS Directive, as it provides a structured approach of identifying and assessing potential security risks and vulnerabilities in systems, facilitating compliance with the Directive. Threat modeling is a valuable tool for organizations to gain a comprehensive understanding of the potential threats they face, the probability of their occurrence, and the potential impact of such threats on their systems. This information can then be leveraged to develop and implement suitable security measures to mitigate those risks. This research initially explores the transportation sector, identifying and describing its four subdomains. Afterwards, it identifies the assets involved in the transportation sector that need protection and it presents a taxonomy useful to model every Cyber Physical System (CPS) used in the NIS directive sectors. Then, a detailed overview of the threats against the transportation sector is provided along with the assets that may be affected by these threats. As a result, it is highlighted that a vast amount of those threats emerges in more than one of the NIS domains, demonstrating the need to develop an holistic security framework for the protection of both the tangible and intangible assets of a CPS.

Keywords:threat modeling, transportation sector, cross-domain threats, tangible assets.

1. Introduction

The transportation sector consists of four (4) subdomains namely the air transportation (aviation), the railway, the maritime transportation and the road transportation. The aviation refers to an air transport which holds a valid license or equivalent. In this context, airline and airport management companies and operators of ancillary facilities located within airports are considered the most significant type of entities. The aviation sector is vulnerable to a multitude of threats, with data-related risks emerging as the most prominent of them. Alongside ransomware and malware, those threats specifically target customer data held by airlines and proprietary information belonging to original equipment manufacturers (OEMs). In this context, there has been a notable increase in ransomware attacks impacting airports in 2022, as well as proliferation of fraudulent websites impersonating airlines [1]**.**

As far as the railway transport subdomain is concerned, the most important type of entities is considered to be the railway infrastructure operators along with the railway operators. The railway infrastructure operator refers to any organization or company responsible for the operation, maintenance, upgrade and renovation of railway infrastructure on a network, as well as the responsibility for participating in its development, in accordance with the rules laid down by the member state. Similarly, a railway operator is any licensed public or private entity whose principal activity is the carriage of goods and/or passengers by rail, provided that such undertaking also provides traction. Concerning the threats, ransomware and data-related threats primarily target CPS of the railway sector, like passenger services, ticketing systems, and mobile applications, leading to service disruptions. In this regard, a recent study from ENISA [1] showed that in 2022, there has been a growing frequency of Distributed Denial of Service (DDoS) attacks carried out by hacktivist groups against railway companies. These attacks have been attributed primarily to Russia's invasion of Ukraine.

In terms of sea transportation, the following type of entities are recognized: (i) Maritime transport companies, (ii) port management, (iii) Vessel Traffic Service (VTS) operators, (iv) VTS operators for inland waterway, (v) sea and coastal passenger and freight transport companies (as defined by the EU regulation for maritime transport, excluding individual ships used by these companies), and (vi) port management bodies and companies that exploit port facilities or perform works/projects within ports, or use equipment located within ports. Within the maritime sector, there is a prevalence of ransomware, malware, and phishing attacks specifically aimed at port authorities, port operators, and manufacturers. In this context, state-sponsored attackers frequently engage in politically motivated attacks that result in operational disruptions at both ports and vessels.

Finally, for the road transport, road authorities or bodies that use Intelligent Transport Systems (ITS) technologies as well as operators of ITS are recognized as the basic type of entities. A road authority is any public authority responsible for the design, control or management of the road network which falls within its territorial jurisdiction, whereas a road operator is any public or private entity responsible for maintaining and managing the road network. In the road transport sector, ransomware attacks are the most prevalent, followed by data-related threats and malware. The automotive industry, particularly original equipment manufacturers (OEMs) and tier-X suppliers, has been specifically targeted by ransomware attacks, resulting in disruptions to production processes. Data-related threats primarily focus on IT systems to gain access to customer and employee data, as well as proprietary information. While most cyber incidents can be categorized within specific subsectors, there is a limited number of cases that defy classification. These incidents involve broader campaigns that target the entire transportation sector in specific countries. Those campaigns are often attributed to hacktivist groups and state-sponsored actors, and their occurrence is closely linked to geopolitical tensions [1].

In the following section, a generic asset taxonomy for cyber physical systems of the NIS directive sectors is presented. This work was conducted in the course of the City-level Cyber-Secure Multimodal Transport Ecosystem (CitySCAPE[1]) Horizon 2020 project.

2. Main asset categories of Cyber Physical Systems

Assets are generally classified into two (2) basic categories based on their physical presence or lack thereof: (i) tangible assets and (ii) intangible assets. Tangible assets exist in a physical form and possess a determinable monetary value. They are typically capable of being exchanged for a monetary value, although the level of liquidity may differ across various markets. Tangible assets stand in opposition to intangible assets, which possess a conceptual value rather than an exchange value based on transactions. In particular, an intangible asset is a non-monetary asset that, although it lacks physical substance, can be identified provided that the asset is separable or arises from contractual or legal rights. Separable assets may be subject to sale, transfer, licensing, and other similar transactions. Examples of intangible assets include licenses, trademarks, patents, films, copyrights, and import quotas.

In the context of the CitySCAPE research project, a set of generic tangible assets was defined as part of the risk analysis procedure. The main concept behind the definition of those basic assets was that all assets involved in a Cyber-Physical System can be decomposed into basic assets which share a large number of common features, threats and vulnerabilities.

In the following sections, the threats are correlated with basic assets to form common threat patterns that are identified at several or all domains. The adopted asset taxonomy is presented in the following table:

[1] https://www.cityscape-project.eu/

Table 1: *CitySCAPE's project asset taxonomy*

Asset Group ID	Asset Group	Asset ID	Basic Asset Type	Reference
AS-HW	Hardware	AS-HW-01	Sensors/Actuators Hardware	[2]
		AS-HW-02	Power supply	[2]
		AS-HW-03	Computational Device	[3]
		AS-HW-04	HW Interface	–
		AS-HW-05	I/O Devices	–
		AS-HW-06	Storage	[3]
AS-DA	Data	AS-DA-01	Backup Data	[2]
		AS-DA-02	Configuration Data	[3]
		AS-DA-03	Operation Data / Application Data	[3]
		AS-DA-04	System Data	[3]
		AS-DA-05	Test Data	[3]
		AS-DA-06	Audit Data	[3]
AS-SS	System Software	AS-OS-01	Embedded Systems Firmware	[2]
		AS-OS-02	Native API	–
		AS-OS-03	Hypervisor	[4]
		AS-OS-04	Operating System	[3]
		AS-OS-05	Containers / VMs	[3]
AS-SO	Application Software	AS-SO-01	Web-Based Services	[2] [3]
		AS-SO-02	Application Software	[3]
		AS-SO-03	Database Management Systems	[3]
AS-US	Users	AS-US-01	System Users	[3]
		AS-US-02	End Users	[3]
		AS-US-03	Contractors/Sub-contractors	[3]
AS-NE	Communication Network	AS-NE-01	Communication Protocol	[2]
		AS-NE-02	Network Interfaces	–
		AS-NE-03	Network Controller (HW)	–
		AS-NE-04	Network Stack (SW)	–

3. Threat Landscape for the transportation sector

In this chapter, a detailed taxonomy of the cyber-security threats that affect the transportation sector is presented [5] [6] [7]. The threats are aggregated into five (5) supergroups based on their potential source. Subsequently, a concise description is provided for each threat within the respective supergroups, and then these threats are appropriately mapped to the assets directly impacted by them.

3.1.1. Natural and social phenomena

This group consists of various threats that represent natural disasters and social phenomena like (i) earthquakes, (ii) fires, (iii) extreme weather, (iv) solar flare, (v) volcano explosion, (vi) nuclear incidents, (vii) dangerous chemical incidents, (viii) pandemic, (ix) social disruptions, (x) shortage of fuels. Large scale natural disasters and rare social phenomena are infrequent but could impact the systems supporting critical business functions (e.g., destruction of an airport). Also, other sectors could be affected if transport infrastructure is not working properly due to calamities: (e.g., goods are not delivered in time or quality is altered) threat probability is low, but the impact might be huge. Regarding the affected assets, any asset category (directly or indirectly) may be affected by this type of threats.

3.1.2. Supply chain failure

The transport sector is heavily reliant on third-party services, and any failure in this regard has significant implications for service provision. This dependency is driven by various factors, including safety considerations, operational and financial responsibilities, adherence to safety, cybersecurity, and technical standards, cost considerations, and contractual obligations. Collaboration among stakeholders is essential, as a failure of a third party can have a negative impact on the entire system. For instance, in July 2016, a third-party failure, specifically an internet service provider outage at Rome's Fiumicino airport, resulted in a two-hour delay in passenger check-in operations.

In the railway sector [6], cloud services are leveraged to enhance rail signaling capabilities. With an increasing number of users, railway operators must carefully assess investments to improve their services. However, without adequate measures such as access controls, redundancy, and fallback computers in data centers, security can be compromised, posing risks to both users and passengers. For example, self-driving vehicles that are unable to maintain a safe distance from each other due to compromised security measures can endanger passengers and pedestrians.

This group of threats encompasses malicious acts originating from various entities including Internet Service Providers (ISPs), Cloud Service Providers (CSPs), and remote maintenance providers. Additionally, it includes all types of failures such as power supply failures, hardware failures, and network failures. Evidently, these threats have the potential to impact all asset groups of the proposed asset taxonomy.

3.1.3. Human errors

This group entails the following threats:

(i) **Unauthorized access control- Unauthorized data access**: To ensure availability, integrity and confidentiality, access control procedures should be in place: e.g., there is a high need for protection of the radio block centers (RBC) (railway sector) which in case of unauthorized access and also manipulation, can lead to the inoperability of trains or worst could produce consequence to the operational safety [6]. This threat potentially affects all assets of the presented asset taxonomy.

(ii) **Non-compliance (BYOD)**: The absence of adequate control over Bring Your Own Device (BYOD) poses significant risks to the infrastructure. It is imperative to be ensured that these devices are kept separate from the perimeter of critical servers and services. Access to the network of the infrastructure should be carefully regulated and secured through the use of individual credentials associated with each device, such as digital certificates. Whenever feasible, these devices should operate within a policy-based infrastructure when joining the IT domain of airports or railway stations [5] [6]. This approach creates a more restricted environment, allowing for the enforcement of policies such as limitations on peripheral usage through group policy settings. This threat affects hardware assets such as computational devices and I/O devices, software assets like application software and database management systems as well as all types of data (backup data, configuration data, operation data and log data) that are used by the CPS.

(iii) **Configuration errors - Operator/user error**: Configuration errors or errors made by operators/users can have detrimental consequences to the proper functionality of the CPS that are used in the context of the transportation sector. For instance, system downtime and flight cancellations at smart airports can be attributed to either failures or the total absence of secure password settings on devices prior to deployment [5]. Such impacts can introduce significant security vulnerabilities, and in the worst-case scenario, may result in serious incidents involving users' safety, such as those related to self-driving vehicles [7]. Additionally, the loss of hardware, such as laptops containing sensitive data or authentication details (such as passwords or VPN certificates), can introduce vulnerabilities and pave the way for subsequent attacks.

(iv) **Malware injection attacks** (i.e.virus, ransomware, worms): Malware has the potential to significantly impact the entire infrastructure, as it operates maliciously within the host machine and often spreads to interconnected systems. Its dissemination can occur through various means, including social engineering, direct exploitation of software vulnerabilities, or tampering with devices. The recent surge in ransomware attacks has affected numerous stakeholders within the transportation sector. For instance, in 2020, Adif, the Spanish Administrator of Railway Infrastructures, fell victim to a ransomware attack, resulting in the exposure of personal and business data [6]. Similarly, the Airbus Group experiences an average of up to twelve cyber-attacks annually, with a majority of them being ransomware incidents [5]. Typically, these attacks are facilitated by unpatched vulnerabilities that have not been addressed in a timely manner. This type of threats necessitates proactive measures to mitigate their potential impact that lies primarily on intangible assets like safety and security, airline/airside operations, IT communications passenger management.

3.1.4 Malicious actions

In this group the following threats are included:

(i) **Denial of Service (DoS), Amplification / Reflection Flooding Jamming:** The main impact of a Denial of Service (DoS) attack is the disruption of services. In a distributed environment, this type of threat, known as Distributed Denial of Service (DDoS), can result in the unavailability of certain cloud-based services. The repercussions may include a slowdown in security checks, delays for passengers, flight cancellations, diminished confidence, harm to the company's reputation, and potential financial losses. An example of a DDOS attack occurred in 2018, targeting the DSB ticketing systems in Denmark [6]. This incident affected approximately 15,000 customers who were unable to purchase tickets from ticket machines. As far as the affected assets are concerned, the following asset categories are susceptible to this type of threat: (i) software assets (application software, database management systems), (ii) operating system assets (hypervisor, containers/VMs), and (iii) network assets (communication protocol, network interface, network H/W, network S/W).

(ii) **Social engineering attacks (Phishing Pretexting, Untrusted links, Baiting Reverse social engineering Impersonation, Identity Theft):** Social engineering involves the manipulation of individuals to disclose information or carry out actions on behalf of the attacker. These types of attacks are particularly effective as they can bypass technical and physical security controls. In general, employees who lack sufficient awareness of security protocols or have not received adequate training in these matters can pose a considerable risk to the cybersecurity of the infrastructure. This is because attackers can potentially gain complete access to victims' accounts, identities, and authorizations. Successful social engineering attacks could lead to data breaches, data leakage, or data theft. The asset groups that are vulnerable to those type of attack are in principal all types of data (backup data, operation data, system data, audit data), the software (web-based services, application software and database management systems), the operating system (native API, hypervisor, operating system and containers), and the users (system users, end users).

(iii) **Exploitation of software vulnerabilities:** Potential vulnerabilities may be present in smart airport systems, railway systems, and other types of systems within various sectors. Additionally, there may be unidentified security issues pertaining to IT and smart assets, or issues for which patches have been developed but not yet implemented. In this regard, it is imperative for the vendors of these assets and the managers that are responsible for transport infrastructure to diligently assess whether their systems are operating with the most up-to-date security patches. Failure to do so may render them susceptible to sophisticated attacks. Assets that may be entailed in this type of threat are computational devices as well as certain types of data (backup data, configuration data, operation data and log data).

(iv) **Transport device tampering:** Manipulating self-serving e-ticketing systems is a task that can be easily accomplished, primarily due to their typical placement in publicly accessible areas. If such attacks are successful, the attacker can gain unauthorized entry into the system and potentially modify its intended functionality. Furthermore, they may also illicitly obtain users' personal information. The asset categories that may be targeted in this case include mainly hardware assets like computational devices, H/W interfaces, I/O devices, and storage as well as the network interface.

(v) **Exploitation of insecure interfaces and APIs:** A potentially existing cloud computing environment in CPS of any sector, provides user interfaces and APIs for device interconnectivity and interaction with the Cloud service. However, if these interfaces are inadequately designed and lack essential security measures such as encryption and access control, they become entry points for malicious attackers. Compromised or exploited APIs can lead to significant data breaches. From the presented taxonomy, all types of interfaces (H/W interface, network interface) in conjunction with the Native API are vulnerable to this type of threat.

(vi) **Insider threats:** The insider threats, which encompass malevolent activities such as information theft, data manipulation, sales of critical data to competitors, and information leakage, involve individuals who possess insider access within an organization. These individuals can be current or former employees, contractors, or trusted partners. Their authorized access allows them to potentially compromise a Cloud service which could ultimately result in a data breach. The asset categories from the abovementioned asset taxonomy that are primarily susceptible to this type of threats include data (backup data, configuration data, operation data and log data) along with the system and end users.

(vii) **Data interception during transit (Man-In-The-Middle Attack):** Within a potentially existing cloud architecture model, data undergoes transfer from the cloud customer to the cloud service provider. However, during this transitional phase, there is a risk of interception by malicious actors, leading to the potential compromise of data and subsequent data breach. Evidently, the asset category that becomes the target of such attacks, as outlined in the presented taxonomy, is the data category, encompassing backup data, operational data, and system data.

3.1.5 System Failure

System failure threats refer to potential risks that can lead to the malfunction or breakdown of computer systems or networks. These threats may arise from various sources, including hardware failures, software bugs, power outages, natural disasters, or human errors. When system failures occur, they can result in the loss of data, disruption of services, or even complete system shutdown. Organizations must implement robust backup and recovery mechanisms, redundancy measures, and disaster recovery plans to mitigate the impact of system failures and ensure business continuity. Regular system maintenance, monitoring, and testing are also essential to identify and address vulnerabilities that could lead to system failures.

The following threats can be classified into this group:

(i) **Software failure:** This threat refers to security events such as failures in device components, devices or systems, communication link disruptions, disruptions in main supply, disruptions in service providers, disruptions in power supply, hardware failures, and software bugs. System failure can have significant implications for the security posture and operational capacity of an infrastructure. Consequently, infrastructure system managers must ensure that critical functions are maintained at a minimum level or establish a defined recovery protocol to mitigate the impact. It is imperative to prioritize the continuity of operations and implement appropriate measures to address software failures promptly and effectively. From the presented asset taxonomy, this threat impacts the assets of both the operating system (embedded firmware, Native API, hypervisor, containers) and the software asset categories (web-based services, application software, database management systems) as well as computational devices from the hardware asset category.

(ii) **Network-related technical failures or attacks:** Inadequately configured filtering devices, such as firewalls, or generally weak network security measures, can frequently provide opportunities for attackers to establish backdoors and exploit vulnerabilities. As a consequence, these attackers can gain unauthorized access to sensitive data and functionalities, potentially uploading malicious software or executing malicious commands. The asset categories affected by this type of threat encompass the operating system, including embedded firmware, hypervisor, and containers, as well as the network, comprising network interfaces, network hardware, and network software. Additionally, computational devices within the hardware supergroup are also susceptible to these threats.

(iii) **Outdated firmware:** In certain subsectors, such as railways, specific components and systems have been initially developed with state-of-the-art security measures in place. The primary challenge lies in the ongoing task of ensuring that these systems remain up-to-date, as a failure to do so inevitably leads to their eventual obsolescence. Moreover, these systems are typically distributed across a network, encompassing various locations such as stations and tracks. This distributed nature poses challenges in achieving comprehensive cybersecurity control and oversight. From the presented asset taxonomy, the main asset category that is subject to this type of threat is the data category (backup data, configuration data, operation data and log data) along with the embedded system's firmware asset from the operating system asset category and the computational devices from the hardware asset category.

4. Discussion and Cascading effects

Considering the proposed asset taxonomy's generic applicability to any cyber-physical system within the NIS sectors, it is evident that the threats described thoroughly in the preceding section are not exclusive to the transportation sector. Rather, they constitute a common set that affects all other NIS sectors as well. Nonetheless, each sector also faces its own context-specific threats – nevertheless, similar threats occure in all domains, if we accordingly substitute application-specific functions or objects.

For instance, the energy sector confronts challenges such as (i) the interfering radiation threat, which involves unauthorized interception of private communication, (ii) the control input spoofing threat, wherein attackers send control input to a process, masquerading it as originating from a legitimate source, with the intention of causing the grid's controlling process to behave maliciously, and (iii) the smart meter-based DDoS attack on AMI server, where attackers compromise numerous smart meters and subsequently utilize them to render the AMI server unresponsive [8] [9] [10] [11]. When comparing this type of threats across domains, we can identify threats in fleet control and automated vehicle control systems vs. (ii), and telemetry/remote control DDoS attacks vs. (iii).

The fact that a large number of identified threats is shared among the various domains despite that the scope of operation of the Operator of Essential Services (OES) in the NIS directive domains or Digital Service Providers (DSP) may be vastly different, is explained due to:

- The functional areas of the Operators remain the same regardless of the domain/sector of the OES.
- All functional areas of the Operators rely on an information and communication platform – a digital infrastructure possibly provided, operated, or implemented by a DSP.
- All essential services are interconnected with each other in modern society, and therefore cascading risks and threats are highly possible.

For all Operators, regardless of the domain, the functional areas of their operation are the following: *Administrative task; production tasks; distribution tasks; sales tasks, customer service tasks, financing task; marketing tasks; human resources tasks; R&D tasks; and Information and Communication platform operation.*

The latter monitors, controls all the aforementioned tasks, which means that it has become the heart of the system. Depending on the domain, the scope and type of each set of tasks may vary – especially for tasks like Production, Distribution, and R&D, where the majority of the performed functions are domain-specific. However, regardless of the functional procedures, all tasks are monitored, controlled or carried out through a network of computing devices. Maintaining the resources (physical or virtual), installing new software and/or additional hardware, updating all components are crucial ICT functions that ensure the smooth and reliable OES operation. On the other hand, a failure or an attack on the ICT system may be catastrophic since it may affect all possible functional areas of the OES.

This practically means that:

- All OES components -from data to sensors-actuators, websites, and mobile applications-controlling all aspects - from production to marketing – of the OES operation constitute the ICT platform.
- All conventional threats that concern an ICT platform or a digital infrastructure are relevant for all OESs regardless of the sector.
- The main differences per sector are located in the impact and criticality of an attack depending on the functionality of the compromised asset.

In [12], ENISA emphasizes the fact that the threat landscape reveals several emerging interdependencies between OESs and DSPs at system and service levels. In fact, there is an increasing number of cybersecurity incidents that, due to these interdependencies, either propagated across organizations, often across borders or had a cascading effect at the level of essential services.

Generally, interdependencies and cascading effects propagate through the following modes [13]:

- *Physical:* if the state of a service depends on the material/physical output of another service/infrastructure.
- *Cyb*er: if the state of a service depends on information and data exchanged through the information service and communication links.
- *Geographic*: The spatial proximity between services/infrastructures makes them geographically dependent in case of a local (e.g., environmental) event/incident.
- *Logical*: Logical interdependency is a connection between states of operations between services/infrastructures that are not physical, cyber, or geographic and are the result of human decisions and actions (e.g., failure of infrastructure will increase demand for substitute services).

Cascading effects can be investigated in four different levels:

- Propagation of threats between assets of the same entity (e.g., from a cloud service to an automation system of a railway service provider).
- Propagation of threats between entities of the same ecosystem (e.g., railway service provider to railway infrastructure operators).
- Propagation of threats between different ecosystems (e.g., from railways to road transportation).
- Propagation of threats between different NIS directive domains.

The latter is of utmost importance since an incident may affect multiple dimensions of the societal structure.

Focusing on the Cyber aspect of cascading effects, in order to be able to identify the potential of a cascading threat, the following mechanism has been developed in the context of the CitySCAPE risk analysis methodology.

- The implementation of a threat at a given asset or entity may have one of the following impacts (that can also be considered as high-level threats):
    - Loss of transmitted information/data.
    - Loss of stored information/data.
    - Disclosure of transmitted information/data.
    - Disclosure of stored information/data.
    - Modification of transmitted information.
    - Modification of stored information/data.
    - Interruption of service.
- If the asset or entity is interconnected with other assets or entities, then a cascading threat is implemented towards a secondary asset or entity, if the impact from the implementation of the initial threat:
    - concerns transmitted information/data (loss, disclosure, modification) towards the secondary asset/entity.
    - concerns stored data in a shared (with the secondary asset/entity) database or repository.
    - Concerns disruption of a service provided by the initial asset/entity to the secondary.
- The propagated impact is manifested as a propagating threat and should be taken into account when calculating risk or impact at the secondary asset/entity.

The described mechanism is applicable at all four levels of cascading effect cases. Thus, if the interconnected assets/entities are part of different ecosystems or domains, large scale cascading effects may occur. A simple example is the following: modification of data in the banking system may propagate to a public transportation system, through information/data exchange with its ticketing subsystem.

Extended analysis of the threat landscape per NIS directive domain can be found in [14].

5. Conclusions

This paper presented a taxonomy for the assets that can be applicable to all CPSs used in all NIS directive sectors. Then, a survey of the transportation sector is performed with an overview of possible threats in conjunction with the asset categories that are affected by these threats. The survey comes to the conclusion that the vast amount of the identified threats is applicable to most (if not all) NIS directive domains. This is resulted by the fact that all OESs rely on information and communication systems in order to provide services. Finally, the mechanism of cascading effects through threat propagation among assets or entities is described. The method is applicable for cascading effects between entities, ecosystems, or even sectors/domains.

Acknowledgment

This work is a part of the CitySCAPE project. CitySCAPE has received funding from the European Union’s Horizon 2020 research & innovation programme under grant agreement no 883321. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

References

[1] ENISA, "ENISA Transport Threat Landscape," 21 March 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape.

[2] ENISA, "Baseline Security Recommendations for IoT," 20 November 2017. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[3] ENISA, "Good practices for IoT and Smart Infrastructures Tool," 2019. [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool.

[4] ENISA, "Cloud Computing Risk Assessment," 20 November 2009. [Online]. Available: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

[5] ENISA, "Securing Smart Airports," 16 December 2016. [Online]. Available: https://www.enisa.europa.eu/publications/securing-smart-airports.

[6] ENISA, "Railway Cybersecurity," 13 November 2020. [Online]. Available: https://www.enisa.europa.eu/publications/railway-cybersecurity.

[7] ENISA, "Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations," 12 January 2016. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-recommendations.

[8] J. Slowik, "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE," DRAGOS Inc., 4 October 2018. [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf.

[9] J. Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack," DRAGOS Inc., 15 August 2019. [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

[10] J. Staggs, D. Ferlemann and S. Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection,* vol. 17, pp. 3-14, June 2017.

[11] N. Falliere, L. Murchu and E. Chien, "W32. Stuxnet Dossier," *Security Response,* vol. 5, no. 6, p. 29, 2011.

[12] ENISA, "Good practices on interdependencies between OES and DSPs," 30 November 2018. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps.

[13] S. Rinaldi, J. Peerenboom and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine,* vol. 21, no. 6, pp. 11-25, December 2001.

[14] K. Maliatsos, C. Lambrinoudakis, A. Menegatos, C. Lyvas, A. Kanatas, C. Kalloniatis, R. Mancilia, P. De Vito and A. Giannakoulias, "CitySCAPE D2.2: Analysis NIS directive Cross domain threats and proof of concepts," 31 May 2022. [Online]. Available: https://www.cityscape-project.eu/wp-content/uploads/2022/07/D2.2-Analysis-NIS-directive-Cross-domain-threats-1.pdf.

[15] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker and C. Glyer, "Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure," MANDIANT, 28 November 2022. [Online]. Available: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton.

[16] CISA, "Cyber-Attack Against Ukrainian Critical Infrastructure," 20 July 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.