A Cyber Security Digital Twin for Critical Infrastructure Protection: The Intelligent Transport System Use Case

Giovanni Paolo Sellitto, Massimiliano Masi, Tanja Pavleska, Helder Aranha

A Cyber Security Digital Twin for Critical Infrastructure Protection: The Intelligent Transport System Use Case

Giovanni Paolo Sellitto[1][0000−0002−8497−8748],
Massimiliano Masi[2][0000−0003−4737−7107],
Tanja Pavleska[3], and
Helder Aranha[4][0000−0002−9502−1597]

[1] Independent Scholar
[2] Autostrade Per L'Italia SpA mmasi@autostrade.it
http://www.autostrade.it
[3] Jozef Stefan Institute, Ljubliana
[4] Independent Scholar hmspider@gmail.com

Abstract. The problem of performing cybersecurity tests over existing industrial control systems is well-known. Once it is deployed, a critical system cannot be made unavailable for the purpose of simulating a cyber attack and thus it is hard to introduce corrective measures based on actual test outcomes. On the other hand, a high security posture is required for critical infrastructure and security by design is mandatory for new projects. Such requirements call for an architectural approach to introduce security straight from the early development phases. However, the adoption of a systematic design approach does not guarantee the cost-effectiveness of security countermeasures analysis, which is an extremely cumbersome task as the creation of a physical model is often costly or impossible.
To address these issues, we propose the introduction of a specific view in the system's architectural blueprint, called the Cybersecurity Digital Twin. It is an Enterprise Architecture model of the system specifically targeted at providing a sound base for simulations in order to devise proper countermeasures without any outage of the physical infrastructure. To provide a proof of concept and demonstrate the practical viability of the proposed solution, we apply the methodology to a Cooperative Intelligent Transport System use case, evaluating the system security of the obtained solution.

Keywords: Cyber Security · Digital Twin · Threat Modeling · C-ITS.

1 Introduction

Model-based approaches have been widely used for system design and testing (e.g. in digital circuits design, aviation, space technology, housing) and for governance purposes in socio-technical systems, since the availability of digital models

facilitates the use of simulations to forecast the system behavior under conditions and stresses that cannot be achieved on the real system without detrimental consequences.

One field of application for model based engineering is the design and testing of *industrial control systems* (ICS), which is a challenging task, since old ICS are usually based on the *Supervisory Control And Data Acquisition* (SCADA) architecture, where each plant (water pipes, intelligent electronic devices, or tunnels in motorways) is a complex system on its own. Moreover, ICS are usually custom-built and their blueprints do not follow an enterprise architecture approach. The simulation of Business Continuity Plans in ICS (required by international best practices such as in ISO 22301 and national regulations) and their assessment is usually restricted to the design / construction phases because halting a critical system to perform tests is not an option.

To mitigate this problem, recently the concept of *digital twin* (DT) emerged as a tool to perform analysis, testing, and simulation of aspects such as service interruption, lack of availability, or continuity in an ICS [2]. A Digital Twin is a digital representation (a model) of the real system that contains enough information to control specific operational parameters or aspects of the physical infrastructure. Digital twins are common in civil engineering industry, where the Building Information Model (BIM) is the de-facto standard to design and operate buildings. In the field of ICS, digital models could offer a viable solution to replace destructive tests and to simulate the effect of events like earthquakes and flooding, which would be impossible to test on the real infrastructure [23].

While in the EA field some authors have tackled the challenge of deriving a Digital Twin from an Enterprise Architecture (EA) model of the system, in the case of ICS the derivation of a digital twin aimed at performing simulations is usually considered as an infrastructure maintenance task instead of being part of the architectural design phases. This is due to the relative novelty of the concept of digital twin, the rapid development of commercial tools to perform visual simulations and also to the frequent lack of an EA model in the case of SCADA systems. The situation is even worse when we consider the specific application of a digital twin for a security assessment of an ICS as, firstly, the modeling languages used to describe a cyber security digital twin have little in common with usual EA modeling languages, like Archimate or UML and, secondly, the models used in Visual Threat Modeling have little resemblance with the Reference Architectures used in the field of IoT or Industry 4.0.

In this paper, we propose a methodology to derive a digital twin of a critical infrastructure, aimed at performing simulations for cyber security and visual threat modeling, starting from an architectural blueprint of the system. Following a common approach in architectural design, we refactor the system architecture[5] to derive a specific architectural view, which is used to produce a digital twin. In turn, the results of the simulations performed on the digital twin will can be fed back into the EA, guiding the designers in the inclusion of the countermeasures foreseen by simulations. Given that usually there is no

[5] Following IEC 62443-3-3

EA blueprint readily available for ICS systems based on SCADA, we propose a methodology that leverages a Reference Architecture (RAMI 4.0, in the specific case of this paper) to take stock of the assets that are relevant to build the digital twin (DT). This methodology takes an existing EA model or a blueprint as an input and categorizes the assets, bridging the gap towards their description in the specific architectural language used to describe the DT.

Our method builds upon the notions of architectural viewpoints and views [14]. The digital twin is obtained through a specific cybersecurity viewpoint of an ICS that can lead to multiple views, since cybersecurity is a cross-cutting concern.

To illustrate the application of the theory, we present a real world Use Case in the domain of *Cooperative Intelligent Transport System* (C-ITS), deriving the DT and performing simulations for a simple transport infrastructure. C-ITS is a networked system of devices aiming at increasing safety and sustainability levels through the application of the Internet of Things (IoT) in the sector of road transportation [11,30,16].

The availability of a DT enables the application of probabilistic risk analysis, reasoning on possible threats represented as attack trees. Based on the results, countermeasures are derived and the process is repeated until the overall risk of an attack that can compromise the critical infrastructure is lowered to an acceptable level. When a satisfactory solution is thus reached, the results are fed back into the architecture leading to an improved blueprint [27].

The product used to perform the visual threat analysis (SecuriCAD [24][6]) requires that the System Under Testing (SUT) is modeled using a specific Meta Attack Language (MAL). This is quite a common situation when dealing with digital models targeted at performing simulations or used to control SCADA infrastructures. To cater with this scenario we propose a separate step that translates the DT into MAL, making the procedure parametric with respect to the target language used to model the DT.

The rest of this paper is structured as follows: Section 2 presents some preliminary concepts. Section 3 describes the methodology, deriving a cybersecurity view and distilling a Digital Twin. Section 4 presents the application of the methodology to the C-ITS use case. In Section 5 we present related works, and, finally, in Section 6 we touch upon future work and conclude.

2 Theoretical Background

This section introduces some concepts that will be exploited throughout the rest of the paper. In Section 2.1, we introduce the concept of EA and show how the constellation of concepts introduced here are relevant for the design of digital twin, which is described in Section 2.2.

[6] SecuriCAD is a a tool that adopts a probabilistic approach to *threat modeling*, based on the definition of Attack Trees, which are the set of steps that the attacker is likely to perform in order to reach our assets

2.1 Enterprise Architecture, Viewpoints, Views

An architectural approach to system analysis and design defines rules for building a blueprint. Usually, it relies on some *Reference Architecture (RA)*, which is a generic conceptual model that provides a template to design an *Enterprise Architecture* in a particular domain.

Viewpoints define abstractions on the set of models representing the enterprise architecture, each aimed at a particular type of stakeholder and addressing a particular set of concerns. Viewpoints can be used to address specific concerns in isolation or to relate several concerns.

A Reference Architecture usually exploits some domain knowledge to define a set of architectural viewpoints, targeted to specific purposes and categories of stakeholders. In the case of the Internet of Things, a number of Reference Architecture models have emerged: the Reference Architecture for Industries 4.0 (RAMI 4.0) defines some viewpoints which are typical for the industrial automation, while the Internet of Things Reference Architecture (IoT RA) presents an integrated architectural model for IoT, whereas the Industrial Internet Reference Architecture (IIRA) is specially devised for industrial control systems. Some authors have pointed out the similarities between these reference architectures [29] with respect to the viewpoints, as shown in Table 1.

IoT RA	**IIRA**	**RAMI 4.0**
	Business	Business
Usage	Usage	
Functional	Functional	Functional
Information		Information
Communication		Communication
System	Implementation	Integration
		Asset

Table 1: Comparison between viewpoints in EAs

For the purpose of explaining our approach, we choose RAMI 4.0 as it can describe any IoT system and provides a built-in dimension to describe the system life cycle. However, the whole approach does not depend on the underlying Reference Architecture model.

RAMI 4.0: RAMI 4.0 model represents a consolidated architectural framework for the Industry 4.0 domain [21]. The conceptual space, depicted in Figure 1, is structured along three axes. The first axis presents the six RAMI architectural layers. From top down, the *business layer* addresses the economic and regulatory aspects, the *functional layer* describes the functionality implemented by the various architectural assets and their run-time environment; the *information layer* describes data and it is used to support the semantic interoperability aspects.

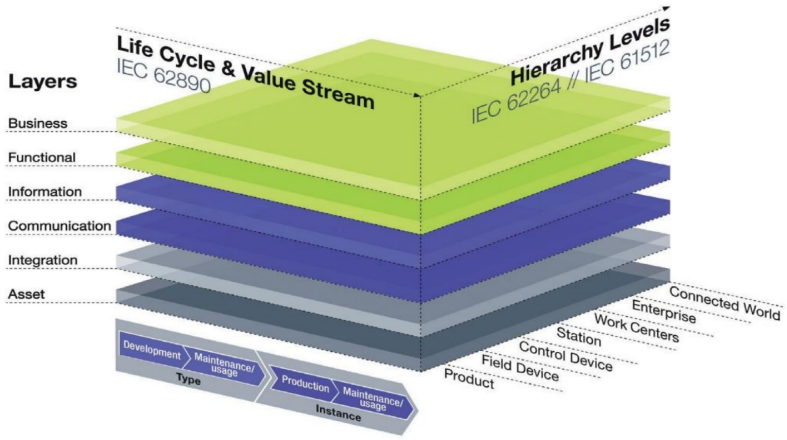

Fig. 1: The reference architectural model for Industrie 4.0

The *communication layer* describes the access to information and the functions of a connected asset (e.g., REST, SOAP, DSRC, 5G). The *integration layer* represents the transition from physical to information world (e.g.man-machine interfaces) and finally the *asset layer* represents the assets that exist in the physical world (sensors, actuators, SCADA).

The second axis follows the*Life cycle* and *Value stream* and they represents the distinction between the instance and the type: the type represents the concept, while the instance, the object, represents the physical object in the system memory.

The third axis, the *Hierarchy*, consists of: the *Product*, describing the unit produced by a system/machine; the *Field Devices* and the *Control Devices*, i.e. the physical unit coordinating the other devices; *Stations* - systems grouped together into a *Work Center*; the *Enterprise*, which is the organization and the *Connected World*, the interface with external systems.

2.2 Digital Twin

There are multiple definitions of *digital twin*: we borrowed one that defines it as a "virtual description of a physical product that is accurate to both micro and macro level" [13]. Digital twins are expected to exhibit *fidelity*, i.e., a high number of parameters transferred between the physical and virtual entity, high accuracy and a satisfying level of abstraction [19]. In [7], digital twins are used to perform simulation of the security aspects of cyber and physical systems to enable security by design, whereas in [3] they are defined as "an evolving digital profile of the historical and current behaviour of a physical object or process". Following the reasoning of [7], the cybersecurity digital twin is defined as a "virtual replica of the system that accompanies its physical counterpart during

its lifecycle, consumes real-time data if required, and has the sufficient fidelity to allow the implementation, testing, and simulation of desired security measures and business continuity plans".

However, these representations alone cannot show whether the system is secure or if a recovery plan is effective. Therefore, a cost-effectiveness analysis is usually performed to find the balance between security and usability, safety, functionality and financial impact. By creating a specific cybersecurity digital twin and applying a security by design approach, the verification of the desired security properties and the cost-effectiveness analyses have a measurable impact.

3 Methodology

In our work, we will introduce a *cybersecurity viewpoint* in the enterprise architecture, from which the *cybersecurity digital twin* is derived as a separate set of *views* in the EA blueprint. In new projects, it can facilitate architectural design, while for existing systems, it facilitates the evaluation of new countermeasures and the elimination of obsolete ones. In this section we show how to build the digital twin of an ICS from its architectural representation while ensuring fidelity, as depicted in Figure 2. For a new ICS following the *security by design* approach, the starting point is the System Architecture, the *high level system blueprint*. For existing systems, a *reverse engineering from existing ICS* step is required, to derive the architecture by introspecting the system and mapping it onto a target EA conceptual space.

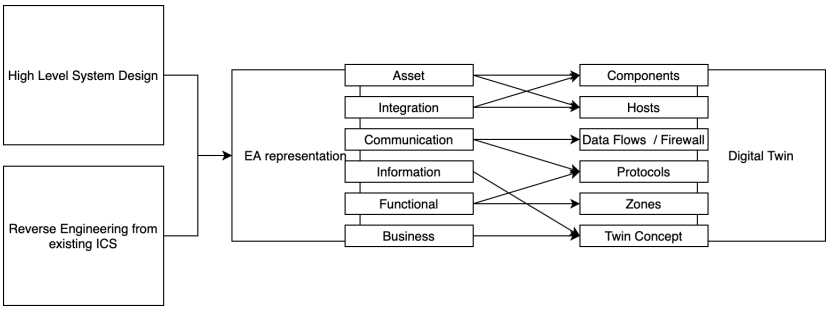

Fig. 2: Digital Twin design process

In the first phase, we derive a cybersecurity view from an existing EA blueprint and in the second phase we distill a digital twin to support cybersecurity simulations. We will include all of the relevant assets in a specific view that will pave the way for distilling a digital twin purposefully designed to perform cybersecurity simulations.

3.1 Phase 1: Derive a Cybersecurity View

The first step is to choose a reference EA model. In this paper, the methodology is explained referring to the RAMI 4.0 architectural model. Based on the reference architecture, a cybersecurity view is derived. The cybersecurity view contains all the assets that are relevant for security purposes. Some guidelines exist that can be adopted to perform this step. For ICS, it is recommended to define and map data flows[7]. To do that, the components of the system can be categorized as different views (e.g. architecture layers).

The assets to protect are selected and included in a specific view **dissecting** the EA blueprint over the RAMI 4.0 reference model. The **dissection** is an analytical process which maps each component of the EA onto a specific element of the RAMI 4.0 2.1. Fig. 3 depicts a generic example of applying this process over a single layer.

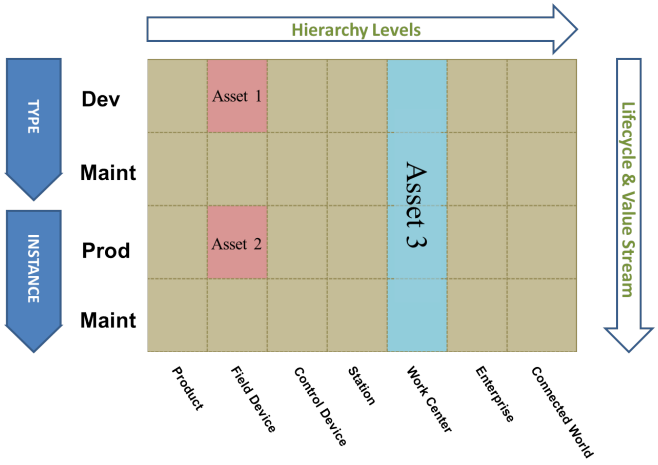

Fig. 3: Dissection over a RAMI 4.0 architecture layer: an example

The procedure is sketched in algorithm 1.

3.2 Phase 2: Derive the Cyber Security Digital Twin from the Cybersecurity View

Different formal languages exist to represent the digital twin of a physical system [19,5,22]. For our purpose, the relevant architectural assets and its relation-

[7] See, e.g., NIST cybersecurity framework for the protection of critical infrastructure [25] that has a specific control (ID.AM-3) requiring that *organizational communication and data flows are mapped* in order to segment and segregate network traffic, and identify firewall rules (the *zone and conduit* principle of IEC 62443)

Algorithm 1: From EA to Cybersecurity View

an EA blueprint (new systems) or a blueprint (for a legacy system) **Result:** A View containing $\mathcal{A}$, the assets to protect
Let $p = \emptyset$ be the set of assets to protect;
Let i = *Business* layer in RAMI 4.0 model;
foreach *layer i in RAMI 4.0 model* **do**
    dissect blueprint over layer i
    identify assets to protect p using guidelines
    $\mathcal{A}$= $\mathcal{A}$ U (i,p)
end

ships are represented using the Meta Attack Language MAL [18], which is suited for security application and, more specifically, for attack simulation and threat modeling. To do that, MAL provides structures (graphs) to model the domain. To translate the Cybersecurity View into the cybersecurity Digital Twin, we can simply describe the relevant Architectural Assets and their relationships using the Meta Attack Language mentioned above. For this paper, we defined the target model using SecuriCAD, the visual editor for MAL. SecuriCAD comes with a set of pre-defined objects that can be used for the creation of a model of the ICS system:

- *components*, such as clients (ssh clients, generic in house-build, GPL, or COTS components);
- *keystore* to hold secrets;
- *access control systems*;
- *hosts*, grasping the peculiarities of Windows or Linux. Hosts can be considered patched and hardened, or unsupervised and unpatched. Typical unpatched hosts are CCTV cameras, while hardened systems could be workstations in a control room;
- *data flows*, *firewalls*, and *protocols* representing the details around the system communications. Data flows also represent *zones* and *conduits* or *protection rings* à la ISO 27002, that can be either physical or logical.

The graph represents the digital twin where the reasoning can start by applying business concepts. As part of the mapping, all assets and integration parts can be either components or hosts. This depends on their maturity model or their inherent characteristics: a device that has an off-the-shelf operating system is a host, while a PLC is a component. The communication entries are data flows and protocols, while the information components become part of the cyber security digital twin concept (since the information has to be protected). Functionalities are then related both to protocols and to zones according to IEC 62443, while business considerations tell us "what to model" and what goes into the digital twin.

4 The Cooperative-Intelligent Traffic Systems Use Case

This Section will introduce the C-ITS use case. Section 4.1 will set the context of C-ITS, and its architecture will be defined in Section 4.2. Section 4.3 will then use these definitions to build the C-ITS Cyber Security Digital Twin.

4.1 C-ITS Overview

Road transportation systems are one of the key factors for a thriving economy and sustainable development. Thus, their full functioning is critical for any community. However, the traffic volume in the roads is increasing, demanding deployment of specific equipment to enhance the travel experience of the road user, while increasing the safety of the road itself, lowering the carbon consumption and other factors. Similarly, vehicles are increasingly endowed with smart technology to increase the safety of the car's driver and passengers, by using sensors (e.g. tyre pressure, RADAR and Ultrasonic), and communications (e.g. infotainment, GPS, and Telematics). Those two aspects, the vehicle and the road infrastructure, and the messages exchanged between them, either from the vehicle to the road or vice versa, are part of a bigger ecosystem named Cooperative Intelligent Transport system, C-ITS.

Data in C-ITS is used by actuators (the Road Side Units) exchanging messages with the vehicles and, indirectly, with the rest of the C-ITS system. Hence, the application context we are accounting for is not one of a closed system, as data is not only exchanged within a single road transportation environment, but with other road operators and even other different critical infrastructures. Smart Cities, hospitals and fire brigades all consume traffic data, e.g., to define alternative traffic routes or other paths to be followed by the ambulances for carrying patients, or to arrive to a site in case of accidents. In that sense, the methodology presented here is also applicable for a setting where the inter-dependencies between the various critical infrastructures may lead to cascading effects, since the consequences from malfunctions or from a cyber-physical attack on one critical infrastructure have impact on all inter-connected ones.

4.2 Enterprise Architectures for C-ITS

The C-ITS architecture is mainly based on the hub-and-spoke paradigm [15,30], where a central system carries the messages to the RSUs located on the motorway. The communication between the vehicle On Board Unit (OBU) and a Road Side Unit (RSU) is usually performed via radio waves [10]. A traffic control center (TCC) collects the events from the road that, in turn, are forwarded to an agent who knows for which specific subset of Road Side Units the event is relevant: an event about road works in 500 km will not be relevant. This agent, named *proxy*, plays the role of Central ITS-Station, while the RSU are named ITS-Stations. The high level architecture is shown in Figure 4. Road Operators notify the TCC about the event (e.g., road works, slippery road) or a Radio Operator is notified by other sources (e.g., other road owners or infrastructure).

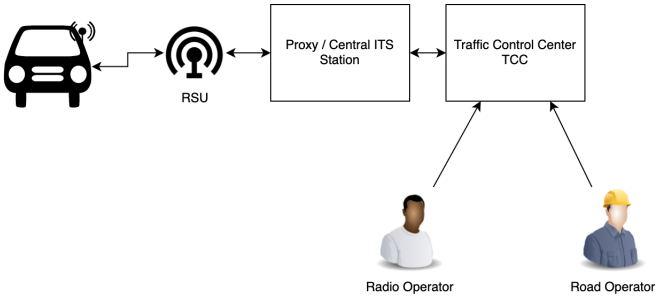

Fig. 4: C-ITS System Architecture for a road operator

Tt also notifies the TCC, who decides the relevance of the event and prepares the message to be propagated to the RSU network. The OBU and the vehicle cooperate with the ITS by acting upon the information received, via DENM[8] messages and by sending their sensed data back to the TCC.

The EA of the system can be represented as follows: according to the viewpoints defined for RAMI 4.0 in Table 1, the devices (RSU, Proxy, TCC) are grouped in the *asset* view, while the protocols (e.g., [10,26,1,17]) used to exchange data between those assets are logically grouped in the *communication* view. The syntax of the data exchanged (e.g., [9]) is in the *Information* view. The functionalities needed by the system and the objectives (and value assets) are then set in their respective views, *functional* and *business*.

4.3 Evaluating the C-ITS Cyber Security Properties

Here, we describe a practical application of the methodology to evaluate the Cybersecurity Digital Twin for C-ITS using MAL and the SecuriCAD tool.

The model is depicted in Figure 5 and it has three logical zones. The first one is the Traffic Control Center (attached to the Corporate Network), represented by the host TCC. The host comes from the asset layer of the system's EA, that has a client named TCCBatch, which is responsible to forward the DENM to the Central ITS Station. Attached to the network is the Laptop Maintainer, which belongs to the system administrator connected to all other hosts via `ssh`. The second zone is the Proxy / Central ITS Station, represented by its host and two streams: the downstream from the TCC ProxyBatch, which is receiving the DENMs for processing, and the upstream to the RSU, composed by a client Proxy and a service, based on Apache Kafka technology, to receive the CAMs. The third zone, the Road Side Units, are placed on the motorway (represented by its Physical zone) where the RSU host (a Linux system) runs a BXC, an in-house software that processes the CAMs and DENMs. Finally, the communication and information aspects (protocols and data flows) are represented in the data flow section. The "star" present in some of the components represents the functional

[8] Decentralized Environmental Notification Message

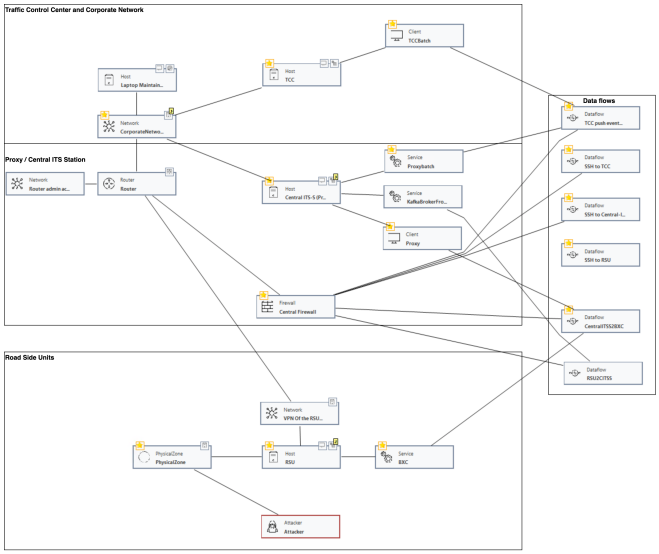

Fig. 5: The Cyber Security Digital Twin of the C-ITS

and business layers, e.g., the functionalities and the high value business objects that have to be protected. This model represents the EA as described in Section 4. The two other components shown in the Figure are the central firewall and the VPN of the RSU.

To perform the simulation, the attacker is placed in the physical zone. This is done in order to check the security of the EA by reasoning over the system representation. The countermeasures that will be used to protect the functionalities of the business objects are defined by discovering attack trees and the likelihood that a specific asset could be compromised.

In this case, the business reasoning identified three canonical attack scenarios that can be simulated (CITS1, CITS2, CITS3), in which the attacker compromises either the IT network or the RSU network or targets both the IT and the RSU services. Table 2 shows the reasoning used to lower an initial high risk ($> 60\%$) to a medium ($30\% \leq$ risk $< 59\%$) and then to low ($< 29\%$), which has previously been determined as an acceptable value. In scenario CITS1, the attacker connects to the Corporate Network as in Figure 5. Without any countermeasures (as defined in the first version of the EA, column *Without Countermeasure (CM)*) the attacker can reach the IT services (TCC and Central ITS Station) with a very high probability. The addition of a central firewall, as shown in Figure 5, would mitigate the reachability (column *with CM*) but the attack is still possible (with a medium risk), since the attacker can exploit a path compromising unpatched/zero day known protocols (ssh).The results of these simulations provide feedback to improve the EA, resulting in the addition of the Central Firewall among the EA's assets. This new version of the EA is used to

Attack ID	Description	Without CM	With CM	Mitigation
CITS1	The attacker is connected to the corporate network and compromise the Central ITS-S and the TCC	69%	46%	Adding a Firewall as countermeasure reduce the risk, since it attacks are possible only on allowed protocols and lateral movements are limited. Additional countermeasure: systems have to be patched continuously
CITS2	The attacker compromise the maintainer's laptop and then compromise the RSUs	50%	23%	Still with the Firewall, attacks are possible. Adding IDS, Privilege Access Management, the attack goes still through sshd and then needs to find an exploit to the in-house software BXC
CITS3	The attacker perform a physical access to the RSU and compromise other RSUs	30%	30%	With the same countermeasures as CITS1 and CITS 2, the mitigation are sufficient to have a low risk of compromise

Table 2: Attack Scenario

simulate CITS2, positioning the attacker in the maintainer laptop, targeting at compromising the RSU. The result is again medium (comparable to the CITS1 with the firewall) as there is no additional countermeasure. By adding Intrusion Detection Systems (IDS), like an antivirus, and a Privilege Access Management (PAM) as a Secure Remote Access (thus monitoring and controlling all accesses) we lower the risk to an acceptable level (23%), leaving the attacker to compromise the in-house software with a very low likelihood. As previously, we provide feedback to the EA and start simulating CITS3. In this scenario, the attacker has physical access to the RSU and wants to compromise all other RSUs. We added to the model another copy of the RSU component and run the simulation. The countermeasures found for CITS2 are sufficient for CITS3, so there is no difference in the risk scoring by adding a local firewall on the RSU network. Through simulations and modifications, we were able to derive a new version of the EA for the system, to perform gap analysis and to prove the cost-effectiveness of adding some specific solutions (IDS, Firewall, PAM).[9].

5 Related Works

The concept of digital twin is introduced in many publications [19] and, although well understood by both academia and industry, several issues are still open. For instance, the *fidelity* of the digital twin with respect to the physical part, the physical-to-virtual connection, and its maintenance over the product life-cycle are points that require further analysis. In [28], authors define a method to build the digital twin. Furthermore, [7] lays down some concepts for the use of a digital twin for security in order to reduce the attack surface and to perform intrusion detection. A framework that, starting from system specifications, creates a model to be used for simulations is presented in [6], where the authors concentrate on ICS and build a digital twin by leveraging the data exchange format. Similar to these works, our approach is focused on the security aspects, but it is parametric to its EA (see Section 2), hence it can be applied to multiple systems and is independent of the reference architecture. Another difference is that our methodology not only encompasses the physical aspects of the system, but also

[9] see `https://www.dropbox.com/s/0exeadyz6t2yzin/ModelForCRITIS.sCAD?dl=0`

its business objectives, tackling security as a *cross cutting concern*, spanning from cyberphysical components to data communication, data syntax, semantics, functionalities, and business models.

Using models for security evaluations is part of a research area named threat modeling. In [20] authors evaluate the extent to which countermeasures can improve the security posture of a power grid SCADA-based system. A work that comes close to ours has been carried out in the Energy Shield project [8]. There, authors derive a model for security simulations using System Theoretic Process Analysis (STPA). We generalise this approach through a formalisation by means of Enterprise Architecture. OWASP[10] defines threat modeling as a way to identify and understand threats, evaluate mitigation practices to protect a valuable asset and define best practices on how to protect it. Our digital representation of the system enables all of the above by performing threat modeling over a digital representation of the entire system, taking into account assets, data flows and messages, as well as functionalities and business objectives.

According to the EU NIS directive [12], operators of essential services are a subset of critical infrastructures. Among the essential services we find the *cooperative intelligent transport systems (C-ITS)*, a set of services implemented by motorways, smart cities, and vehicle manufacturers, that cooperate together for a safer and greener transportation. These systems are usually built and operated in a systematic manner, based on the design of an EA blueprint [30,15]. In [4], a digital twin is built to demonstrate privacy enhancement mechanisms in the automotive industry, starting off by identifying the stakeholders. Our approach is systematic, implying that for new systems, the definition of an architectural model is part of the design, while for existing systems, architectural models are drawn by reverse engineering of the components and the connectors.

6 Conclusion and Future Work

In this paper, we defined a method to build a security-oriented Digital Twin of a cyber-physical system, starting from its architectural blueprint (EA). The EA can include security-by-design concerns for new projects or be obtained by performing architecture reconstruction and reverse engineering for existing projects. Either approach produces a catalogue of assets to protect, organized into views according to architecture viewpoints.

We then described how to map assets to components in the newly introduced Cyber Security view - the Digital Twin that will be used to perform cybersecurity simulations. For that, we employed the SecuriCAD tool, modeling the Digital Twin using a user interface front-end for the MAL language. The tool supports cyber-attack simulations based on MAL.

Finally, we applied the methodology to a real use case of a critical infrastructure - the Cooperative Intelligent Transport System (C-ITS). We mapped the typical EA views used worldwide to represent such systems into a threat-oriented

[10] See `https://owasp.org/www-community/Application_Threat_Modeling`

Digital Twin and performed security reasoning. We defined three typical cyber-attack scenarios for Operational Technology (attacker is in the IT network first, and then in the OT network) and applied countermeasures to mitigate the attack scenario. By incorporating feedback into the EA, we enabled the achievement of a desired fidelity level. In this way, we performed tasks such as Vulnerability Assessment and security testing without causing any service interruption in the running system.

Although MAL and SecuriCAD are powerful tools, they cannot capture a detailed-level system design. For instance, at this moment, protocol-specific risks and device peculiarities are not taken into account. Therefore, as a future work we aim to define a way of grouping architectural assets to automatically determine the specifications of digital twin components to be reused, for a more efficient modeling process. Moreover, we aim at making the target modeling language parametric as well, to avoid a vendor lock-in.

References

1. Apache kafka. Available at `https://kafka.apache.org`. Last accessed Oct 6, 2021.
2. Peter Augustine. Chapter four - the industry use cases for the digital twin idea. In Pethuru Raj and Preetha Evangeline, editors, *The Digital Twin Paradigm for Smarter Systems and Environments: The Industry Use Cases*, volume 117 of *Advances in Computers*, pages 79–105. Elsevier, 2020.
3. Adrien Bécue, Yannick Fourastier, Isabel Praça, Alexandre Savarit, Claude Baron, Baptiste Gradussofs, Etienne Pouille, and Carsten Thomas. Cyberfactory1 — securing the industry 4.0 with cyber-ranges and digital twins. In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, pages 1–4, 2018.
4. Violeta Damjanovic-Behrendt. A digital twin-based privacy enhancement mechanism for the automotive industry. In *2018 International Conference on Intelligent Systems (IS)*, pages 272–279, 2018.
5. Marietheres Dietz, Manfred Vielberth, and Günther Pernul. Integrating digital twin security simulations in the security operations center. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, New York, NY, USA, 2020. Association for Computing Machinery.
6. Matthias Eckhart and Andreas Ekelhart. Towards security-aware virtual environments for digital twins. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, CPSS '18, page 61–72, New York, NY, USA, 2018. Association for Computing Machinery.
7. Matthias Eckhart and Andreas Ekelhart. *Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook*, pages 383–412. Springer International Publishing, Cham, 2019.
8. Energy Shield. Developing the cyber toolkit that protects your energy grid, 2021.
9. ETSI. EN 302 637-3, Intelligent Transport Systems (ITS);Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, 2014.
10. ETSI. Intelligent Transport Systems (ITS);Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range, 2015.

11. European Commission. Cooperative, connected and automated mobility (CCAM), 2021.
12. European Parliament and the Council. Directive EU 2016/1148, 2016.
13. Michael Grieves. Digital twin: Manufacturing excellence through virtual factory replication. 03 2015.
14. The Open Group. Togaf 9.2, 2019.
15. ICT4CART. A connected future for automated driving, 2021.
16. Intelligent Transport Systems Australia. ITS Australia, 2021.
17. ISO. ISO/IEC 20922:2016 Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1, 2016.
18. Pontus Johnson, Robert Lagerström, and Mathias Ekstedt. A meta language for threat modeling and attack simulations. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, New York, NY, USA, 2018. Association for Computing Machinery.
19. David Jones, Chris Snider, Aydin Nassehi, Jason Yon, and Ben Hicks. Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29:36–52, 2020.
20. Matus Korman, Margus Välja, Gunnar Björkman, Mathias Ekstedt, Alexandre Vernotte, and Robert Lagerström. Analyzing the effectiveness of attack countermeasures in a SCADA system. In *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, SPSR-SG@CPSWeek 2017, Pittsburgh, PA, USA, April 21, 2017*, pages 73–78. ACM, 2017.
21. Gunther Koschnick. Industrie 4.0: The industrie 4.0 component, 2015.
22. Kendrik Yan Hong Lim, Pai Zheng, and Chun-Hsien Chen. A state-of-the-art survey of digital twin: techniques, engineering product lifecycle management and business innovation perspectives. *Journal of Intelligent Manufacturing*, 08 2020.
23. Qiuchen Lu, Xiang Xie, James Heaton, Ajith Kumar Parlikad, and Jennifer Schooling. From bim towards digital twin: Strategy and future development for smart asset management. In Theodor Borangiu, Damien Trentesaux, Paulo Leitão, Adriana Giret Boggino, and Vicente Botti, editors, *Service Oriented, Holonic and Multi-agent Manufacturing Systems for Industry of the Future*, pages 392–404, Cham, 2020. Springer International Publishing.
24. Xinyue Mao, Mathias Ekstedt, Engla Ling, Erik Ringdahl, and Robert Lagerström. Conceptual abstraction of attack graphs - A use case of securicad. In Massimiliano Albanese, Ross Horne, and Christian W. Probst, editors, *Graphical Models for Security - 6th International Workshop, GraMSec@CSF 2019, Hoboken, NJ, USA, June 24, 2019, Revised Papers*, volume 11720 of *Lecture Notes in Computer Science*, pages 186–202. Springer, 2019.
25. NIST. Cybersecurity framework, 2021.
26. OASIS. Advanced message queuing protocol (amqp) version 1.0, 2012.
27. Paulius Paskevicius, Robertas Damasevicius, and Vytautas Stuikys. Change impact analysis of feature models. volume 319, pages 108–122, 09 2012.
28. Behrang Ashtari Talkhestani, Nasser Jazdi, Wolfgang Schloegl, and Michael Weyrich. Consistency check to synchronize the digital twin of manufacturing automation based on anchor points. *Procedia CIRP*, 72:159–164, 2018. 51st CIRP Conference on Manufacturing Systems.
29. The Open Group. Reference Architectures and Open Group Standards for the Internet of Things – Four Internet of Things Reference Architectures, 2021.
30. United States Department of Transportation. Intelligent Transportation Systems, Joint Program Office, 2021.