Modelling & Simulation of a Rivet Shaving Process for the Protection of the Aerospace Industry against Cyber-threats

Martin Praddaude, Nicolas Hogrel, Matthieu Gay,
Ulrike Baumann, Adrien Bécue

Airbus CyberSecurity SAS Metapole 1,
bouvelard Jean Moulin CS 40001 - 78996
Elancourt Cedex France
E-mail: martin.praddaude@airbus.com

Abstract

This paper provides insights on simulation and modelling work performed within CyberFactory#1 project which aims at enhancing optimization and resilience of the Factory of the Future. The paper describes the modelling and simulation of a complete industrial process of rivet shaving, in support to the digitization of aerospace manufacturing. It provides evidence of accurate elaboration of a Digital Twin (DT) of the Roboshave system in the Airbus CyberRange (CR) environment. This work contributes to science and technology by demonstrating the feasibility of a holistic DT of a complex Cyber-Physical System(CPS) throughout its operational and informational layers, including multiple heterogeneous industrial communication protocols. It contributes to industry and practice by providing a highly realistic virtual environment for cybersecurity testing, simulation, training and decision support to enforce security of digitized industrial systems.

Keywords: Simulation, modelling, Cyber-Physical System (CPS), Operational Technology (OT), Industry 4.0, CyberRange (CR), Digital Twin (DT), Programmable Logic Controller (PLC), Industrial Internet of Things (IIoT)

doi: 10.18278/jpcs.7.2.3

Modelado y Simulación de un Proceso de Afeitado de Remaches para la Protección de la Industria Aeroespacial Contra Amenazas Cibernéticas

Resumen

Este documento proporciona información sobre el trabajo de simulación y modelado realizado dentro del proyecto CyberFactory#1, que tiene como objetivo mejorar la optimización y la resiliencia de la Fábrica del Futuro. El artículo describe el modelado y la simulación de un proceso industrial completo de afeitado de remaches, como apoyo a la digitalización de la fabricación aeroespacial. Proporciona evidencia de la elaboración precisa de un Gemelo Digital (DT) del sistema Roboshave en el entorno Cyber Range (CR) de Airbus. Este trabajo contribuye a la ciencia y la tecnología al demostrar la viabilidad de un DT holístico de un Sistema Ciberfísico (CPS) complejo en todas sus capas operativas e informativas, incluidos múltiples protocolos de comunicación industrial heterogéneos. Contribuye a la industria y la práctica al proporcionar un entorno virtual altamente realista para pruebas de ciberseguridad, simulación, capacitación y soporte de decisiones para hacer cumplir la seguridad de los sistemas industriales digitalizados.

Palabras Clave: Simulación, modelado, sistema ciberfísico (CPS), tecnología operativa (OT), industria 4.0, rango cibernético (CR), gemelo digital (DT), controlador lógico programable (PLC), Internet industrial de las cosas (IIoT)

保护太空产业不受网络威胁的铆钉打磨过程建模和模拟

摘要

本文为CyberFactory#1项目执行的模拟和建模工作提供见解，该项目旨在提升未来工厂（Factory of the Future）的优化和复原力。本文描述了完整的工业铆钉打磨过程的建模和模拟，以支持航空制造的数字化。本文提供证据，精确阐述了空客网络靶场（CR）环境中的Roboshave系统数字孪生（DT）。通过证明复杂信息物理系统（CPS）的全面数字孪生在其操作层面和信息层面（包括多个异质工业通信协

议）的可行性，本文为科学和技术作贡献。通过提供一个高度现实的虚拟环境，用于网络安全检测、模拟、训练和决策支持，以期执行数字工业系统安全，本文为工业和实践作贡献。

关键词：模拟，建模，信息物理系统（CPS），操作技术（OT），工业4.0，网络靶场（CR），数字孪生（DT），可编程逻辑控制器（PLC），工业物联网（IIoT）

Introduction

CyberFactory#1 project aims at designing, developing, integrating and demonstrating a set of key enabling capabilities to foster optimization and resilience of the Factories of the Future (FoF) (CyberFactory#1-ProjectWeb Page,2019-2022). The project outputs form a totalof12 key capabilities arranged in 3 capacity Layers:

1) Modelling and simulation;
2) Factory of the Future optimization;
3) Factory of the Future resilience.

In this paper we introduce the developments made on the Airbus CyberRange (Airbus CyberSecurity, 2021) for the modelling and simulation of a Cyber-Physical System(CPS) called Roboshave (Bécue et al., 2020), which shaves the rivets of aircraft rudders to keep them within tolerances for airworthiness and aerodynamics (Sterkenburg & Wang, 2021).

Robos have, initially a disconnected equipment, will be connected to a distributed Industrial Internet of Things (IIoT) platform (Sisinni et al., 2018) meant to support real-time monitoring (Chen, 2020), process optimization (Stefano et al., 2020) and quality control (Dutta et al., 2021) in the frame of CyberFactory#1.

In order to specify, test and verify the security and safety properties of the newly connected equipment (Abdo et al., 2018), Airbus CyberSecurity has realized a Digital Twin (DT) (Tao et al., 2019) of the Roboshave system, including simulation of a robotic arm, a profilometer, two Programmable Logic Controllers (PLCs), and Human Machine Interface (HMI). It is integrated in a virtual network environment which accurately replicates the Operational Technology (OT)network (Zhou et al., 2018), the IIoT platform and the Machine Execution System (MES). It features no less than 4 different types of industrial protocols in use within the legacy and newly added communication layers. This development helps solving acknowledged limitations of state of the art DT technology (Tao, Zhang, &Liu, 2019) (Bécue et al., 2020) and provides a demonstration of the effective combination of DT with CR for the purpose of securing Industry 4.0 (Bécue et al., 2018).

Eventually, this digital twin supports the performance of a large panel of attacks, and the definition of adequate security measures based on simulation (Bécue et al., 2018). With the Airbus OT CyberRange, complex industrial automation like Roboshave can be designed, upgraded and tested without any negative impact on the real assets. If maintained in operation, it will also support decision making, both for problems related to manufacturing efficacy or in reaction to new unexpected cyber-threats (Tao et al., 2018).

Methodology

Project Methodology

The project adopts an overall V cycle design methodology (Auriol et al., 2012) in which subcycles corresponding to each of the12 key capabilities are designed in a model-based approach by the use of DTs (Tao et al., 2018). The V cycle is performed through a sequence of work-packages with interactive stages and final deliveries corresponding to output-input transmission: WP2 Requirements and Architecture, WP3 Simulation Capabilities Development, WP4 Optimization Capabilities Development, WP5 Resilience Capabilities Development, WP6 Integration, Validation and Demonstration (ITEA, 2019-2022). The activities described in this paper belong to WP3 and the system simulation will support model-based design and development of subsequent key capabilities, namely the secure deployment of a Data Lake Exploitation capability (Miloslavskaya & Tolstoy, 2016) in scope of WP4 and the enforcement of Cyber-resilience Mechanisms scope of WP5. Eventually, it will also support hybrid (simulation-based / in operation) validation and demonstration activities in scope of WP6.

Simulation Methodology

The aim is to create a "DigitalTwin." For the simulation, it is possible to separate the different components according to Purdue Reference Model (Williams, 1994):

- On the one hand, level3 and 4 with applications such as kepware/thingworx and ERP
- On the other hand, the lower levels which correspond to the factory floor.

For levels 3 and 4, there is no particular difficulty in creating a simulation, as these are applications running on IT systems. For the levels corresponding to industrial processes, it is more difficult (Thomas, 1999), but it is becoming possible, in particular because the OT and the IT networks use protocols which are more and more similar (Tian & Hu, 2019): ethernet, TCP/IP, and the different providers create simulators for their tools.

In the following, we will indicate the method used to create a shop-floor simulation.

First, it is necessary to define more precisely what we mean by a Digital Twin (Bitton et al., 2018):

- The aim is to be able to simulate cyber-attacks and to have a similar behaviour in the simulated environment as in the real environment (Giuliano & Formicola, 2019),

- This requires the same communications between the simulated equipment as in reality (Su et al., 2017),
- For this, it is necessary to have a virtualization of the different equipment present in the real world,
- In order to be as close to reality as possible, the same projects are used in the automatons; for this, it is often necessary to use the simulators provided by the manufacturers (Negahban & Smith, 2014),
- Yet it is important to notice that vendor DTs commonly are closed proprietary technology, difficult to integrate into a full-model of overarching industrial process (Bécue et al., 2020).

In order to create the simulation as defined above, we have followed 4 steps:

- Step 1, characteristics of physical assets. The objective of this stage is to recover real equipment:
  - Processor, CPU, RAM, ROM,
  - Features, provider, software, and project
  - Communication with other assets, protocol
- Step 2, find a simulator for each asset. The objective of this stage is to find how itis possible to simulate the asset and the simulator capabilities to communicate:
  - Does the provider have a simulator? If yes, can it communicate with other simulators?
  - Does it use the same protocol as the shop floor? It is also necessary to ascertain the subject of the available licenses.
  - If no simulator is available, it must be determined how to develop one, with the goal to have the same communications.
- Step 3, find out how to simulate the physical process: with a Virtual Machine (VM)? With software? Directly with a simulator?
- Step 4, development of different virtual machines and software defined previously and make them communicate.

Use-Case Description

Airbus Defence and Space owns several sites in Spain which are dedicated to the production and the final assembly line of commercial and military aircrafts (Airbus in Spain, 2021). One of them, Tablada PreFal, next to Seville city centre, is a multi-program, multi-product, and multi-customer plant where Airbus carries out the production of main component assemblies for A400M (Airbus, Airbus A400M,2021), A330MRTT (Airbus A330MRTT, 2021), Boeing 737 (Boeing 737, 2021), C295 (Airbus C295, 2021), CN235 (Airbus C295, 2021), Eurofighter (Airbus Eurofighter, 2021), Falcon 8X (Dassault Falcon 8X, 2021) and A380 (Airbus A380, 2021). Parts of Ariane 6 spacecraft (Airbus Ariane 6, 2021) have begun to be manufactured in 2019. Tablada is modernized and updated constantly in order to be an example to follow in continuous improvement and Industry 4.0. There is a dedicated innovation ecosystem in Tablada facilities for R&D industrial means.

The RoboShave system has been implemented into the Boeing 737 (Boeing 737, 2021) rudder assembly area. A rudder is composed of multiple parts joined together with rivets. The rivets have to be as flat as possible and to remain within tolerances specified in the requirements (Sterkenburg & Wang, 2021). For that, each rivet is manually shaved to give the rudder the essential aerodynamic characteristics required by such an aircraft part. This impractical operation performed by an operator is very time consuming and slows down the complete production line (Sarh et al., 2009). Following its sense of innovation, Tablada PreFal benefits from the RoboShave system, which has been designed to fulfil an ambitious objective: automate a tedious work with tight tolerances inside a high-rate production line.

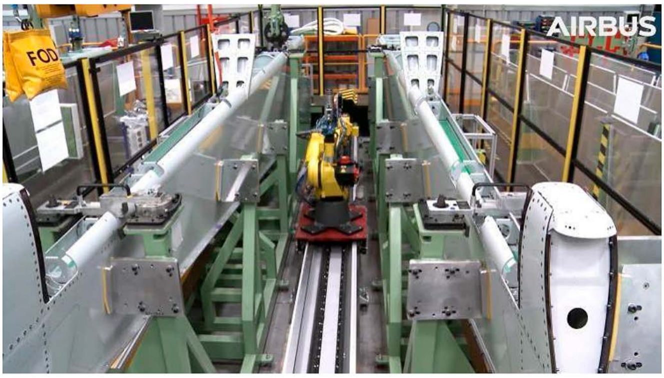

Figure 1. *RoboShave system overview.*

The RoboShave system could be described as a robotic arm whose role is to shave rudder rivets and to automatically check that the shaving operation has been performed successfully. At first, the RoboShave identifies the orientation of the rivet, then the rivet is shaved and to finish the RoboShave checks that the rivet remains inside the tolerances.

This system is planned to be connected with a cooperative network from which the work orders are sent. The data produced by the RoboShave system will be collected in a data lake (Miloslavskaya Tolstoy, 2016) for the purpose of process monitoring, optimization and control (Qin, 2012). The deployment of an IIoT platform extends the attack surface (Sisinni et al.,2018) but this data collection with the deployment of the appropriate technologies based on Artificial Intelligence and Security Incident and Event Monitoring tools will allow to implement predictive maintenance (Lee et al., 2019) techniques, and detect intrusions to secure the production level.

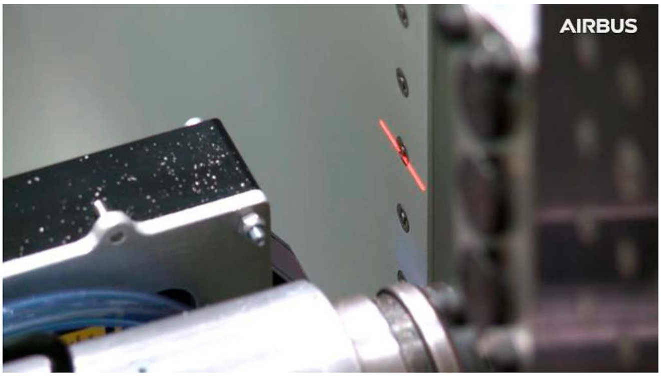

***Figure 2.** First step, the RoboShave identifies the rivet.*

Cyber-Range Tool Description

Airbus CyberRange is an advanced simulation platform that can be used to model IT / OT systems composed of tens or hundreds of machines and play realistic scenarios including real cyber-attacks. The platform manages several environments, isolated ones from the others, as well as from the legacy IT / OT from the organization (Airbus CyberSecurity, 2021). By means of these capabilities, users can immerse themselves in an environment customized to look like their system in operation. This supports several use cases including operational qualification, testing, and training (Bécue et al., 2018). For the hardware, the tool exists in 2 main forms:

- Physical platform: High performance servers stored in a mobile box, on site, switches, hosting VMware, vSphere Infrastructure.
- Cloud Platform: the CyberRange platform is also available in the Cloud, allowing a flexible and multisite collaborative experience.

To use the hardware, Airbus CyberSecurity has developed the software LADE (Life And Death Engine): set of web and micro services simplifying the deployment of virtualized infrastructures, running cyber-attacks, tests and scenarios. LADE allows hybrid infrastructures management. This management software significantly reduces the delay between designing the simulation and having it deployed.

The CyberRange offers independent work zones, which represents a virtual environment dedicated to a user or a group of users. As a fully customizable platform, the Airbus CyberRange graphical user interface allows users to customize their working environment, add notes and key command lines to help them pursue exercises (Airbus CyberSecurity,2021). Each work zone is totally isolated from the other work zones, so the actions of one participant do not interfere with the other participants working on other work zones. Each work zone can accommodate standalone replicas of a network architecture or information systems. Interconnecting work zones is possible by connecting a firewall or router in each zone to a shared zone. For further information, reference is made to the Airbus CyberSecurity website (Airbus CyberSecurity, 2021).

Roboshave Process Simulation

To achieve the DigitalTwin associated with the Roboshave system, it is first necessary to establish an overall state of the art of the technology involved. First, we learn about the industrial process in all its layers: asset, integration, communication, information, functional, and business layers, as defined in the Reference Architecture Model for Industry 4.0 (Zezulka et al., 2016). To do this, we establish communication with plant management which will be maintained over time. System information is acquired in formal (written documentation) or in formal manners (Stone& Sawyer, 2006). The experience feedback accessible through direct involvement of Roboshave operators is a very important data source in order to obtain all the process subtleties. In addition, it enables the verification of the validity and value of the Digital Twin at any time during construction by having it tested and adopted by manufacturing practitioners (Bärring et al., 2020). With this procedure, we identify the list of physical assets present in the system which need to be included in the scope of simulation. In the case of Roboshave, this scope includes a robotic arm Robot FANUC M-20iA/35M (FANUC M2000 Series, 2021), a profilometer Gocator2120 (LMI3D GOCATOR, 2021), a safety PLC Sick Flexi Soft (SICK Flexi-Soft, 2021), a PLC Siemens S7-1500 (SIEMENS Simatic S7-1500, 2021), and an HMI Siemens TP1500-Comfort (SIEMENS Simatic HMI, 2021). The Physical System in scope of the simulation is called Physical Twin (PT). It is described in Figure 3.

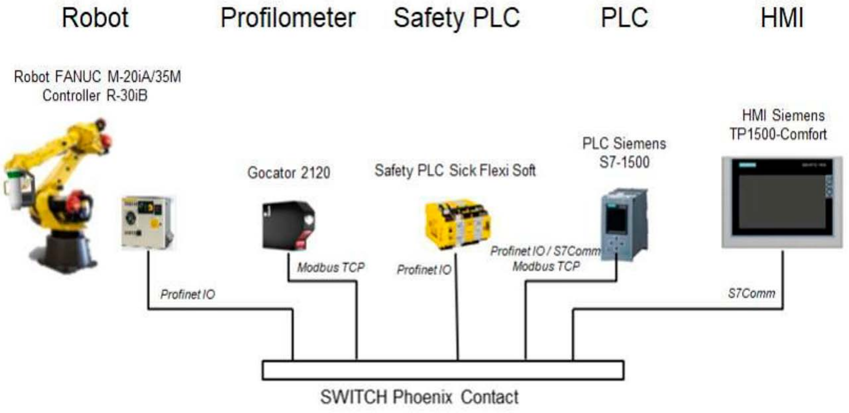

Figure 3. Roboshave System Physical Twin.

We make sure to gather as much information as possible about the constituting elements: equipment manufacturer, product version, technical characteristics, operation modes, hardware and software, connectivity, etc. (Rodič, 2017). In addition, we recover the endemic parts to Roboshave, such as the PLC and HMI projects, but also the various descriptions on the functionalities of the process. We expect to obtain the description of the operations that can be used subsequently in cybersecurity scenarios, such as the different nominal / degraded modes, the segregation of roles in the management of the process, or the expected behaviors of the system depending on the moment (Lou, Guo, Gao, Waedt, & Parekh, 2019). We are also looking for information related to interactions between different assets (Bao, Guo, Li, & Zhang, 2019). Once the industrial system has been understood in depth, the Digital Twin can be built. The DT of Roboshave system, reproducing all elements of its Physical-Twin (TW) is described in Figure 4.

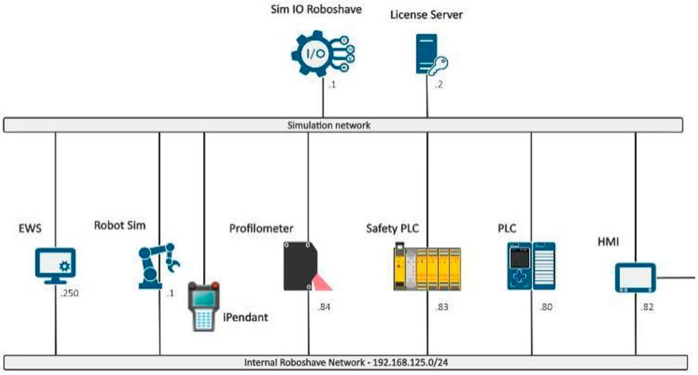

Figure 4. Roboshave System Digital Twin.

For this realization, we relied on the CyberRange virtualization platform from Airbus CyberSecurity (Airbus CyberSecurity, 2021). The tool offers many features to achieve the main objective, such as the ability to build virtual machines on demand, or to perform inter-machine communications. However, certain limitations such as the only Ethernet support as a means of data transmission, or the use of virtualization servers based on x86 processor architectures, will require adaptations to make the Digital Twin functional in this particular context. Indeed, in the industrial world, we can find PLCs operating on particular architectures such as Advanced RISC (Reduced Instruction Set Computing) Machines (ARM) with real-time functionalities (Murti, Jati, Mawardi, & Agustina, 2014).Also industrial systems are commonly interconnected by means of field buses, or even simply with power cables (Kolla, Border, & Mayer, 2003).

In the case where the asset has characteristics that are incompatible with Digital Twin environment constraints, there are three possibilities, listed in decreasing order of application preference:

1. The Digital Twin (DT) environment adapts to the reality of the PhysicalTwin (PT). In this case, in-depth work is undertaken, often very long and expensive, to align the simulation tool on the characteristics of the PT. In our example, the potential changes of the DT from x86 to ARM, or from Ethernet to a field bus would require the acquisition of new compatible equipment, which had little business relevance.

2. The PhysicalTwin (PT) adapts to the constraints of the Digital Twin (DT) platform. This option should be chosen only if the technology in use suffers from already acknowledged obsolescence or limitations which we aim to overcome. In most cases, it is a costly option that may require a requalification of the manufacturing system. In our example, the potential changes of the PT from ARM to x86, or from field bus to Ethernet would require a requalification of the Roboshave System, which is prohibitive in terms of cost and delay.

3. In some cases, where DT and PT cannot fully align because of particular constraints, the best compromise should be found between the functionalities retained and those to be withdrawn. This compromise should be made according to the considered use and misuse cases. In our example, we want our Digital Twin to operate in x86 architecture, communicating exclusively over Ethernet, but behave in the same way from a functional point of view as the legacy ARM system. With this limitation, we acknowledge that attacks on process variables will be effective, but attacks related to the real-time answers of the system cannot be tested.

4. In this search for adaptation, it is necessary to undertake in-depth search of simulation solutions related to the industrial processing assets. The various criteria are the measured rate of realism, the possible level of exploitation within the virtualization platform, and the time/cost constraints that the solution induces (Hlupic & Paul, 1999). We noticed that the simulation market was more and more expanded, and it had started to affect manufacturers in a concrete way. Indeed, an effective line of research for the construction of a Digital Twin is the use of products from the initial equipment manufacturer (Cabral, Wenger, & Zoitl, 2018). We can compare these solutions to custom-made development of our own simulators in the form of a two entries table to highlight the advantages and disadvantages of vendor-made solutions (Buy) against tailor-made solutions (Make). Such a comparative table is summarized in Table 1.

In Roboshave, most components have existing simulators offered by original equipment manufacturer. RoboGuide software from Fanuc (FANUC Roboguide, 2021) can be used to simulate the robotic arm. GoEmulator from LMI3D (LMI3D Virtual 3D Smart Sensor, 2021) can be used to simulate the profilometer. PLC SimAdvanced (SIEMENS S7PLC SimAdvanced,2021) can be used for PLC simulation. The HMI can be simulated by WinCC software (SIEMENS, SIEMENS WinCC, 2021). Using the original equipment simulator provides a guarantee of quality and time saved, because it theoretically behaves exactly like the physical asset (Post, Groen, & Klaseboer, 2017).

However, some of these simulators suffer from compatibility limitations or constrainful license terms, which limit the range of investigations with consideration for security testing. In order to overcome these issues, we had to be in close collaboration with providers to solve them. Also despite this evolution in the industrial landscape, we have noticed that there are many devices that do not have their Digital Twin equivalent, especially brands that have never had the need to enter this market. We then proceeded as follows: first of all, we our intentions to the equipment manufacturer, sharing interest in the opportunity to enter the simulation market. Depending on manufacturer willingness and conditions, we may or may not work in collaboration. Table 1 provides a summary of Make / Buy choices, where the selected solution is marked.

Table 1. *Compared Simulations*

Asset	Solution 1 (Buy)	Solution 2 (Make)
Robot Sim .1	RoboGuide from Fanue ✓ -Limited connectivity	RoboDK +Free to use
Profilometer .84	GoEmulator from LMI -Software limitation	Airbus CyberSecurity simulator +Linux compatible ✓
Safety PLC .83	PLCSimAdv from Siemens -Software limitations	Airbus CyberSecurity simulator +development ✓
PLC .80	PLCSimAdv from Siemens +Good Compatibility ✓	Airbus Cybersecurity simulator -Limited Fidelity
HMI .82	WinCC from Siemens +Good Compatibility ✓	Open HMI -Limited Fidelity

Apart from intrinsic component processes, system connectivity also needs comprehensive simulation. Some important links that have been modelled are:

- the S7Comm link between PLCSimAdv (PLC) and WinCC (HMI) to exchange process data
- the S7Comm link between WinCC(HMI) and EWS to load Siemens project
- the S7Comm link between PLCSimAdv (PLC) and EWS to load Siemens project
- the Modbus TCP link between PLCSimAdv (PLC) and Airbus CyberSecurity simulator (Profilometer)
- the Profinet link between PLC and Robot/Safety PLC

It is important to notice that several protocols in use within this list are not supported by the vendor solution.

This is how the development of our own Profinet simulation stack was launched. Profinet is an industrial standard for data communication over Ethernet, designed for collecting data from, and controlling equipment under tight time constraints. The support of this protocol was not yet available during the assembly of this Digital Twin, it is important in Roboshave and is reusable in many other industrial systems (Dias, Sestito, Turcato, & Brandão, 2018). Therefore, we had to undertake extensive research into the operation of this protocol, with the help of the specifications, in order to integrate it technically. This work resulted in a system allowing to capture the communicating devices in Profinet on a network, and to establish a relation between the subsystems. This implementation is represented in Figure 5.

The Profinet layer developed by Airbus CyberSecurity supports certain functionalities resulting from the specifications indicated in IEC61158-5-10 (IEC-International Electrotechnical Commission, 2014) & IEC 61158-6-10 (IEC-InternationalElectrotechnical-Commission, 2019), and can be associated with industrial data processing software such as virtual PLCs, or virtual HMIs. In addition, micro-developments had to be done for various purposes, in particular for the exploitation of the various APIs offered by the manufacturers of simulation software. These have made it possible to change certain variables which are supposed to be modified only by physical behavior (movements, sensors, actuators).

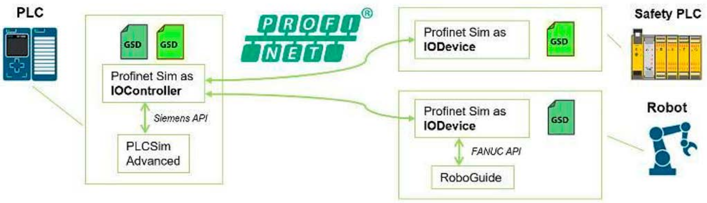

***Figure 5**. Profinet Simulator Concept.*

On Roboshave, we can find different networks with various objectives. These are simulated through virtual networks. However, the program displaying the evolution of the robotic arm in 3D does not necessarily support the possibility of integrating presence sensors which send well-formatted data as expected by the central PLC. In addition, it is normally electrical impulses that are expected. Consequently, it is through an additional simulation network that the robot will send and receive the information to the IO simulator, that a given sensor has changed its state. This network is also used for licensing constraints imposed by manufacturers. As a result, the networks on the real system remain free of noise relating to the simulation (Lu et al., 2020).

Validation Plan

In order to validate the level of fidelity of the digital twin, we carry out a verification phase which uses the physical twin as the model to be achieved. To do this, unit tests are carried out on the simulated machines themselves, as well as according to the capabilities of the complete topology and its interactions. These tests validate the level of the digital twin according to the latter's ability to approximate the behavior of the physical twin. The metrics associated with these tests make it possible to quantify a result. They relate to various aspects: execution time, same behavior between DT and PT with same input conditions, data set exchanged in virtualized network, behavior of the assembly according to the technical parameters inserted.

This validation is performed by carrying out a succession of technical and functional tests applied to all aspects of the process. Here are some examples of these tests that can be applied to this use case: Nominal and complete rivet shaving procedure, "Coupon test" procedure, "Open Doors" procedure, Disconnect the Safety PLC and attempt operations known to be dangerous for humans over HMI. Once they have been carried out, this Digital Twin can be used for various purposes: cybersecurity tests, pre-production tests, behavior tests, security tests under specific conditions, industrial log recovery and deployment tests of products adjacent to the initial system etc. (Bécue et al., 2020).

To go further in the digital twin validation process, we can make sure to apply cyber attacks on the latter, which would be replicable on the physical twin. By taking into account the integration constraints, a scope for cyber attacks can be defined to know the limits of the topology. In the event that an attacker reaches Roboshave's internal network, the latter would have the possibility of practicing simple but well-known attacks such as Man-In-The-Middle through ARP (Address Resolution Protocol) Poisoning between OT components, in order to spy on business data (Nam et al., 2012). exchanged, or to cut off the corresponding communications, and thus put the industrial system to an unstable state. The possible consequences of this attack can be loss of the industrial process control by the operator because the link between the HMI and the PLC is cut off, and the data monitored by MES are changed directly from the process in order to raise wrong alarms.

Conclusion and Perspectives

With this work we have demonstrated the feasibility of a holistic simulation of a critical industrial process performed by a complex CPS. It provides advance against state of the art by solving acknowledged limitations of the current technology in terms of simulation framework openness and cosimulation capacity (Bécue et al., 2020). Future work will consist of the diversification of entire cyber scenarios to be developed with punctual attacks in a risk-based approach according to misuse-cases which have been defined and prioritized in previous project works. Further simulation will be integrated to model other systems included in the IIoT platform such as the Autoclave and the Gap Guns. These DTs will support future design of process optimization and cyber-resilience mechanisms in the frame of CyberFactory#1 (CyberFactory#1-Project Web Page, 2019-2022). An example of a protection mechanism which will be implemented is the deployment of combined user and device access control mechanism compatible with IIoT constraints, based on Airbus CymID solution (Airbus Cybersecurity, 2021). Further security reinforcement mechanisms can be the deployment of OT Itrusion Detection Systems enabling to detect the aforementioned attacks and timely respond (Han, Xie, Chen, & Ling, 2014). In this context, the DT can be used as a decision support tool for response optimization (Bécue, Maia, Feeken, Borchers, & Praca 2020) or as a prediction tool for threat anticipation (Pokhrel, Katta, & Colomo-Palacios, 2020).

References

Abdo, H., Kaouk, M., Flaus, J., & Masse ,F.(2018). A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. *Computers & security,72*,175-195.

Auriol, G., Shukla, V., Baron, C., & Fourniols, J.Y. (2012). *Chapter System Engineering Method for System Design.* Intech Open.

Bao, J., Guo, D., Li, J., & Zhang, J.(2019). The modelling and operations for the digital twin in the context of manufacturing. *Enterprise Information Systems, 13(4)*, 534-556.

Bärring,M., Johansson,B.,& Shao,G. (2020). DigitalTwin for Smart Manufacturing: The Practitioner's Perspective. *ASME International Mechanical Engineering-*

Congress and Exposition (Vol.84492, p. V02BT02A015). American Society of Mechanical Engineering.

Bécue, A., Fourastier, Y., Praça, I., Savarit, A.,Baron, C., Gradussofs, B., & Thomas, C. (2018). CyberFactory #1—Securing the industry 4.0 with cyber-ranges and digital twins. *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*,(pp.1-4).

Bécue, A.,Maia, E., Feeken, L., Borchers, P., & Praca, I. (2020). A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future. *Applied Sciences,10(13)*,44-82.

Bitton, R., Gluck, T., Stan, O., Inokuchi, M.,Ohta, Y., Yamada, Y., & Shabtai, A.(2018). Deriving a cost-effective digital twin of an ICS to facilitate security evaluation. *European Symposium on Research in Computer Security*, (pp. 533-535).

Bouzgou, K.& Ahmend-foitih, Z. (2014). Geometric modeling and singularity of 6DOF Fanuc 200IC robot. In Fourth edition of the *International Conference on the Innovative Computing Technology (INTECH 2014)*, (pp.208-214).

Cabral, J., Wenger, M., &Zoitl, A. (2018). Enable co-simulation for industrial automation by an FMU exporter for IEC 61499 models. *IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA) (Vol. 1)* (pp.449-455). IEEE.

Chen, W. (2020). Intelligent manufacturing production line data monitoring system for industrial internet of things. *Computer Communications,151*,31-41.

Dias, A. L., Sestito, G. S., Turcato, A.C., & Brandão, D. (2018). Panorama, challenges and opportunities in PROFINET protocol research. *13th IEEE International Conference on Industry Applications (INDUSCON)*(pp.186-193). IEEE.

Dutta, G., Kumar, R., Sindhwani, R., &Singh, R. K. (2021). Digitalization priorities of quality control processes for SMEs: a conceptual study in perspective of Industry 4.0 adoption. *Journal of Intelligent Manufacturing*,1-20.

Giuliano, V., & Formicola, V. (2019). ICSrange: A simulation-based cyber range platform for industrial control systems. *15th European Dependable Computing Conference (EDCC2019).* eprint arXiv:1909.01910.

Han, S., Xie, M.,Chen, H. H., &Ling, Y. (2014). Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE systems journal, 8(4),* pp. 1052-1062.

Hlupic, V., & Paul, R. J. (1999). Guidelines for selection of manufacturing simulation software. *IIE transactions,31(1),*(pp.21-29).

IEC-International Electrotechnical Commission.(2014). *IEC 61158-5-10.*

IEC-International Electrotechnical Commission. (2019). *IEC61158-6-10.*

Kolla, S., Border, D., & Mayer, E.(2003). Fieldbus networks for control system implementations. *Electrical Insulation Conference and Electrical Manufacturing and Coil Winding Technology Conference (Cat.No.03CH37480)*, (pp.493-498).

Lee, W.J., Wu, H., Yun, H., Kim, H., Jun, B. M., & Sutherland, J.W. (2019). Predictive maintenance of machine tool systems using artificial intelligence techniques applied to machine condition data. *ProcediaCirp,80*,506-511.

Lou, X., Guo, Y., Gao, Y., Waedt, K.,& Parekh, M.(2019). An idea of using DigitalTwin to perform the functional safety and cybersecurity analysis. *INFORMATIK 2019.* Bonn: Gesellschaft für Informatik e. V.

Lu, Y., Liu, C., Kevin, I., Wang, K., Huang, H., & Xu, X. (2020). DigitalTwin-driven smart manufacturing: Connotation, reference model, applications and research issues. *Robotics and Computer-Integrated Manufacturing,61,101837.*

Miloslavskaya, N., & Tolstoy, A. (2016). Big data, fast data and data lake concepts. *Procedia Computer Science,88*,300-305.

Murti, M.A., Jati, A.N., Mawardi, L., & Agustina, S.A. (2014). Software Architecture of Ladder Compiller to Opcode for Micro PLC Based on ARM Cortex Processor. *Journal of Automation and Control Engineering Vol,2(4).*

Nam, S. Y., Jurayev, S., Kim, S. S., Choi, K., &Choi, G. S. (2012). Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN. *EURASIP Journal on Wireless Communications and Networking, 2012(1)*,1-17.

Negahban, A., & Smith, J. S. (2014). Simulation for manufacturing system design and operation: Literature review and analysis. *Journal of Manufacturing Systems,33(2),*241-261.

Pokhrel, A., Katta, V., & Colomo-Palacios, R. (2020). DigitalTwin for Cybersecurity Incident Prediction: A Multivocal Literature Review. *IEEE/ACM 42nd International Conference on Software Engineering Workshops* (pp.671-678).

Post, J., Groen, M., & Klaseboer, G. (2017). Physical model based digital twins in manufacturing processes. *10th forming technology forum* (pp.87-92). University of Twente.

Qin, S. J. (2012). Survey on data-driven industrial process monitoring and diagnosis. *Annual review sin control, 36(2),* 220-234.

Rodič, B. (2017). Industry4.0and the new simulation modelling paradigm. *Organizacija,50(3).*

Sarh, B., Buttrick, J., Munk, C., & Bossi, R. (2009). Aircraft manufacturing and assembly. In *Springer handbook of automation* (pp. 893-910). Heidelberg: Springer.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M.(2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE transactions on industrial informatics,14(11)*,4724-4734.

Stefano, F., Benzi, F., & Bassi, E. (2020). IIoT based efficiency optimization in logistics applications. *Asian Journal of BasicScience & Research, 2(4)*, 59-73.

Sterkenburg, R., & Wang, P. H .(2021). *Standard aircraft handbook for mechanics and technicians.* McGraw-Hill Education.

Stone, A., & Sawyer, P. (2006). Identifying tacit knowledge-based requirements. *IEE Proceedings-Software, 153(6)*,211-218.

Su, W., Antoniou, A., & Eagle, C. (2017). Cybersecurity of industrial communication protocols. *22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*(pp. 1-4). IEEE.

Tao, F., Qi, Q., Zhang, M., Zhang, H., & Sui, F. (2018). Digital twin-driven product design, manufacturing and servicewith big data. *Int. J. Adv. Manuf. Technol. 2018, 94*, 3563–3576.

Tao, F., Zhang, H., & Liu, A. (2019). Nee, A.Y.C. Digital Twin in Industry: State-of-the-Art. *IEEE Trans. Ind. Inform. 2019,15*, (pp. 2405–2415.).

Thomas, P.J. (1999). *Simulation of industrial processes for control engineers.*Elsevier.

Tian, S., & Hu, Y. (2019). The role of OPC UA TSN in IT and OT convergence. *2019 Chinese Automation Congress (CAC)* (pp.2272-2276). IEEE.

Williams, T. J. (1994). The Purdue enterprise reference architecture.*Computers in industry, 24(2-3),* 141-158.

Zezulka, F., Marcon, P.,Vesely, I., & Sajdl, O. (2016). Industry 4.0–An Introduction in the phenomenon. *IFAC-PapersOnLine, 49(25)*,8-12.

Zhou, L., Zhang, L.,& Ren, L. (2018). Modelling and simulation of logistics service selection in cloud manufacturing. *Procedia CIRP, 72*, 916-921.

Web References

Airbus.(2021, 07 08). *Airbus A330MRTT*. Retrieved from Airbus: https://www.airbus.com/defence/a330mrtt.html

Airbus.(2021, 07 08). *Airbus A380*. Retrieved fromAirbus: https://www.airbus.com/aircraft/passenger-aircraft/a380.html

Airbus.(2021, 07 08). *Airbus A400M*. Retrieved from Airbus: https://www.airbus.com/defence/a400m.html

Airbus.(2021, 07 08). *Airbus Ariane6*. Retrieved from Airbus: https://www.airbus.com/space/launchers-deterrence/ariane-6.html

Airbus.(2021, 07 08). *Airbus C295*. Retrieved from Airbus: https://www.airbus.com/defence/c295.html

Airbus.(2021, 07 08). *Airbus C295*. Retrieved from Airbus: https://www.airbus.com/company/history/defence-history/transport-aircraft.html#C295

Airbus.(2021, 07 08). *Airbus Eurofighter*. Retrieved from Airbus: https://www.airbus.com/defence/eurofighter.html

Airbus.(2021, 07 08). *Airbus in Spain*. Retrieved from Airbus: https://www.airbus.com/company/worldwide-presence/spain.html

Airbus CyberSecurity. (2021, 07 07). *CyberRange*. Retrieved from Airbus Cybersecurity: https://airbus-cyber-security.com/products-and-services/prevent/cyber range/#scroll1

Airbus Cybersecurity. (2021, 09 16). *CymID*. Retrieved from Airbus Cybersecurity:https://airbus-cyber-security.com/wp-content/uploads/2020/12/Airbus-CyberSecurity_CymID_EN.pdf

Boeing. (2021, 07 08). *Boeing 737*. Retrieved fromBoeing: https://www.boeing.com/commercial/737max/

Dassault. (2021, 07 08). *Dassault Falcon 8X*. Retrieved from Dassault Aviation: https://www.dassault-aviation.com/fr/civil/la-famille-falcon/falcon-8x/

FANUC. (2021, 07 12). *FANUC M2000Series*. Retrieved from FANUC: https://www.fanuc.eu/fr/en/robots/robot-filter-page/m-2000-series

FANUC. (2021, 07 12). *FANUC Roboguide*. Retrieved from FANUC: https://www.fanuc.eu/fr/en/robots/accessories/robog uide

ITEA. (2019-2022). *CyberFactory#1-ProjectWeb Page*. Retrieved fromITEA4: https://itea4.org/project/cyberfactory-1.html

LMI3D. (2021, 07 12). *LMI3DGOCATOR*. Retrieved from LMI3D: https://lmi3d.com/brand/gocator-3d-smart-sensors/

LMI3D. (2021, 07 12). *LMI3DVirtual3DSmartSensor*. Retrieved fromLMI3D: https://lmi3d.com/virtual-3d-smart-sensor/

SICK. (2021, 07 12). *SICKFlexi-Soft*. Retrieved from SICK: https://www.sick.com/ag/en/senscontrol-safe-control-solutions/safety-controllers/flexi-soft/c/g186176

SIEMENS. (2021, 07 12). *SIEMENS S7PLC Sim Advanced*. Retrieved from SIEMENS: https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/1031 6003

SIEMENS. (2021, 07 12). *SIEMENS Simatic HMI*. Retrieved from SIEMENS: https://new.siemens.com/global/en/products/automation/simatic-hmi/panels/comfort-panels.html

SIEMENS. (2021, 07 12). *SIEMENS Simatic S7-1500*. Retrieved from SIEMENS: https://new.siemens.com/global/en/products/automation/systems/industrial/plc/simatic-s7-1500.html

SIEMENS. (2021, 07 12). *SIEMENS WinCC*. Retrieved from SIEMENS: https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-v7.html