replication. In simulation mode, the digital twins run independently from their physical counterparts, e.g., to conduct security tests. In contrast, the replication mode mirrors the physical devices' program states to their digital twins. In this mode, malicious behaviour can be detected in two ways: First, a comparison between the inputs and outputs of physical devices and those of digital twins may reveal differences that would indicate malicious behaviour or faults that caused the real devices to deviate from their virtual replicas. Second, if abnormal conditions of the physical process emerge in the virtual environment as well, the framework is able to detect violations of safety and security rules, by continuously monitoring the state of digital twins.

In [1], we present a proof of concept to demonstrate the feasibility of the proposed approach. We used AutomationML [2] as a data format, to specify our exemplary production system. In addition to the CPS's specification, we explicitly defined safety and a security rules. The prototypical implementation of the framework is based on Mininet [3] and integrates a transcompiler for IEC 61131-3 programming languages as well as a Modbus TCP/IP stack. In this way, we were able to equip the digital twins with the required features to replicate the component logic of the physical devices that are part of our test bed.

For future work, we intend to focus on the simulation aspects of digital twins by developing a feature that would allow users to recover historical states of digital twins and replay their execution. In this way, certain scenarios can be repeated for further analysis, e.g., to understand the propagation of malware.

Link:
Source code of CPS Twinning on GitHub: https://kwz.me/hds

References:
[1] M. Eckhart, A. Ekelhart: "Towards Security-Aware Virtual Environments for Digital Twins", Proc. of the 4th ACM Workshop on Cyber-Physical System Security. ACM, 2018.
[2] R. Drath, et al.: "AutomationML-the glue for seamless automation engineering", ETFA 2008.
[3] B. Lantz, B. Heller, N. McKeown: "A network in a laptop: rapid prototyping for software-defined networks", Proc.of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, ACM, 2010.

Please contact:
Matthias Eckhart, TU Wien, Austria
matthias.eckhart@tuwien.ac.at
https://www.sqi.at/

Andreas Ekelhart,
SBA Research, Austria
AEkelhart@sba-research.org
https://www.sba-research.org/

Enabling Security and Safety Evaluation in Industry 4.0 Use Cases with Digital Twins

by Markus Tauber (FH Burgenland) and Christoph Schmittner (AIT)

The digital twin of a system should contain not only the existing information but also an up-to-date picture of the current status. While this is easy with physical properties, which can be measured by sensors, it is more challenging to measure and to provide an up-to-date picture of properties like security and safety. We have investigated the modelling of such dependencies in use cases related to transparency as well as to self-adaptability. Based on our experience we propose further extensions of domains like reliability. This also has the potential to provide legal support to Industry 4.0 use cases when required.

The uptake of technologies and approaches from the Internet of Things (IoT) together with flexible Cloud-based support technologies has enabled numerous and diverse digitisation and Industry 4.0 scenarios and use cases, ranging from smart manufacturing to smart-buildings and smart farming. Each domain has a different environment, and an application must be able to react, i.e. to be smart, to changes in the environment. Such changes need to be monitored and it is important that the application still operates in a trustworthy manner in the face of environmental changes.

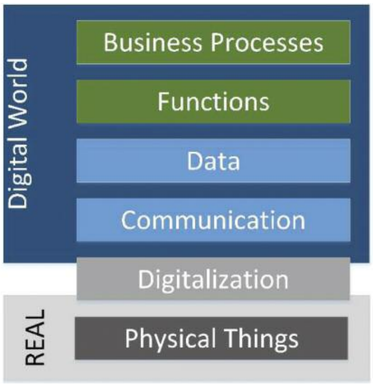

Figure 1: Industry 4.0 Layer-Model.

Digital twins can help to organise and handle all the data that is generated by IoT elements. Digital twins are a digital representation of a real system, with the history of all changes and developments. Figure 1 gives an overview of how Industry 4.0 is structured and divided between the "real" and the "digital world". The starting point was to have a collection and a standardised digital representation of the real or physical "thing" for easier management. The digital twin is intended as a shell that contains and manages, depending on the application and needs, different sub-models [3].

Although there are already security and safety oriented sub-models based on the IEC 62443 and IEC 61508/61511 these are currently intended as static information. From [1]: "Administration Shell (=digital twin) of Smart Manufacturing Components should be able to carry the (security-) information”. This is in our opinion insufficient for dynamic and changeable IoT devices where the system, which is providing a service, could be not only distributed geographically but also be managed by multiple parties and be used in changing environments and domain contexts. To ensure secure, safe and reliable operation it is necessary to have a constant view of the configuration and influenced security and safety properties. This is also important for legal reasons – which could be considered an additional dimension of the digital twin, which often considers the modelling of aspects in the physical dimension in the cyber dimension.

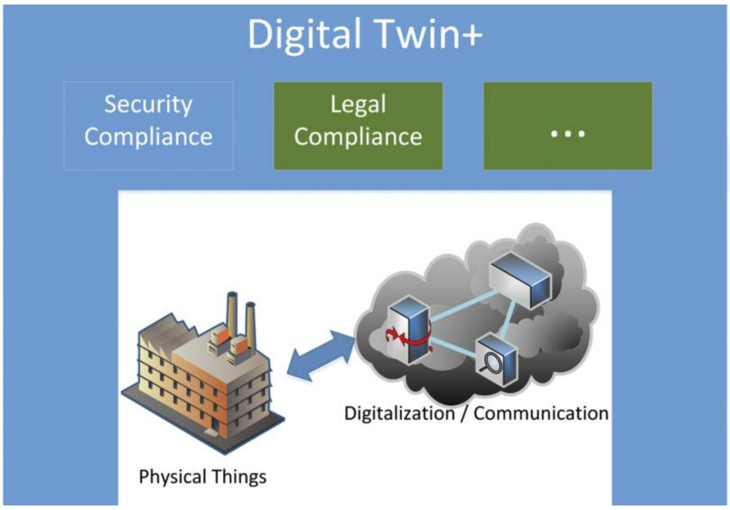

Figure 2: Digital twin with compliance.

Figure 2 gives an overview of the intended architecture. Besides the “physical thing” network, security and safety are considered as parts of the thing, monitored and stored in the digital twin. If an organisation can demonstrate that, a system is complying to certain security and safety standards by assuring that the required properties are fulfilled, legal and contractual obligations are easier to meet. Regardless of the domain, something that individual applications tend to have in common is that sensors and actuators interact with some cloud-based monitoring and control mechanism. Such cloud-based IoT solutions in this context can be a public cloud service such as “Microsoft IoT Hub” [L1], or a private cloud environment such as “VMware IoT Solutions” [L2] or even a physically very close entity, such as the hardware “Arrowhead local cloud” [2] infrastructure.

Methods and tools for analysing and monitoring the effect of a change and giving a holistic and easy to understand picture are not yet available. For instance, SySML is able to capture parts of the behaviour in state machine diagrams where the different states and potential transitions of individual components can be modelled but this is not focused on dependencies between security, safety and related dependencies based on larger composition of components cannot be described.

This particularly important in terms of effects on and interactions between security, safety and reliably. We focus on security and safety because of the potential exploitation of IoT devices as bot nets or industrial attacks, for instance. Safety is important since many of the IoT use cases interact with and affect the physical world, with risk of human or environmental harm. Security is also paramount because automatic actions must be able to rely on the data that is provided [3].

In the past we have worked on identifying related issues during design time in cases where trustworthy components are required and depicted this in a meta model [4]. We have also used this approach to model and describe dependencies and components in systems which adapts itself to a changing environment [5].

Based on our recent experience we propose to consider multiple dimensions when talking about a digital twin. We have done this with safety and security, and realised that there are more dimensions to consider. Each of them has to be described in a way specific to its domain and then linked to the other dimensions, i.e. the physical world, the digital application, cyber security, safety and in a next step reliability. This will allow us to verify the degree to which an automatically or autonomously triggered action can be based on trustworthy or reliable data. Recording this information will also support legal cases. An integration of such a topic to digital twins would provide a powerful method and tool for designing future complex and smart systems of systems.

This work has received funding from the SemI40 and Productive4.0 project, under grant agreement No 692466 and 737459. The project is co-funded by grants from Austria, Germany, Italy, France, Portugal and ECSEL JU.

Links:
[L1] https://kwz.me/hda
[L2] https://kwz.me/hdT

References:

[1] The Federal Ministry for Economic Affairs and Energy (BMWi), “Structure of the Administration Shell: Ttrilateral Perspectives from France, Italy and Germany”, 2018.
[2] A. Bicaku, et al.: “Interacting with the arrowhead local cloud: On-boarding procedure”, in IEEE Industrial Cyber-Physical Systems (ICPS), 2018.
[3] D. Miorandi, et al.: “Internet of things: Vision, applications and research challenge”, Ad hoc networks 10, pp. 1497-1516, 2012.
[4] A. Bicaku, et al.: “Towards trustworthy end-to-end communication in industry 4.0,” in INDIN’17, Emden, 2017.
[5] M. Sila, et al.: “Towards flexible and secure end-to-end communication in industry 4.0”, in INDIN’17, Emden, 2017.

Please contact:

Markus Tauber
FH Burgenland, Austria
+43 5 7705-4321
markus.tauber@fh-burgenland.at

Christoph Schmittner
Austrian Institute of Technology GmbH, AIT
Christoph.schmittner@ait.ac.at