Monitoring Physical-World Access of Virtual Automation Functions

Rainer Falk and Steffen Fries
Siemens AG
Technology
Munich, Germany
e-mail: {rainer.falk|steffen.fries}@siemens.com

***Abstract*—Virtualized automation functions can be used in cyber-physical systems to influence the real, physical world using sensors and actuators connected via input-output modules. At the same time, other virtualized automation functions may be used for planning, testing, or for optimization. A reliable method for determining whether a certain virtualized automation function has access to the real, physical world is proposed, based on a cryptographically protected physical-world access attestation issued by an input/output module. It confirms which virtualized automation function has in fact access to the real-physical world via this input-output module. This allows monitoring which automation functions interact in fact with the real, physical world, and which ones are used for other, less critical purposes.**

Keywords–cyber physical system; virtual automation system; attestation; industrial security; cybersecurity; security monitoring.

I. INTRODUCTION

A Cyber Physical System (CPS) contains control devices that interact with the real, physical world using sensors and actuators. Which automation and control devices are connected via sensors and actuators to the real, physical world has implicitly been clear from the structure of physical control devices, sensors, actuators. their cabling, and the overall system engineering. When control devices are virtualized, e.g., as container or virtual machine, executed on a common compute platform, they interact with the real, physical world using remote Input-Output (IO) modules. However, it is no longer clear implicitly which virtualized control device in fact interacts with the real, physical world, and which ones are used for simulation or optimization. A Physical World Access Attestation (PWAA) can confirm reliably, which automation function accesses a specific IO module [1].

Digital twins, supporting the simulation of the CPS and its control devices, provide the possibility to perform plausibility checks of the measured real-world behavior and the expected, simulated behavior in parallel. This eases the detection of unexpected system behavior, which may indicate a failure situation or even an attack. In addition, virtualization of control devices is increasing, allowing to deploy multiple instances of virtualized control devices that look and behave identically [2]. A virtualized control device can be realized as virtual machine or container hosted on an app-enabled edge device or on a cloud infrastructure by a virtualized Automation Function (vAF). In such a deployment, it has to be distinguished which vAF instances in fact interact with the real, physical world, and which ones are used for other purposes as, e.g., training, optimization, planning, virtual commissioning, simulation, or for testing. The vAF instance that in fact has access to the real physical world is the one that is the most critical, as its operation directly affects the real world.

In the past, CPS have been often rather static. After being put into operation, changes to the configuration happen only rarely, e.g., to replace a defect component, or to install smaller upgrades during a planned maintenance window. To cope with increasing demands for flexible production and increased productivity, CPS will also increasingly become more dynamic, allowing for reconfiguration during regular operation. Such scenarios for highly adaptive production system that can be adjusted flexibly to changing production needs have been described in the context of Industry 4.0 [3]. Virtualization of control functions by vAFs also simplifies flexible reconfiguration, as changes can be performed with less effort for software-based automation functions than for changing hardware components and cabling.

In this paper, we propose a reliable method for determining which vAF instance accesses the real, physical world. A cryptographically protected Physical-World Access Attestation (PWAA) issued by an IO module confirms which vAF instance accesses that IO module. The IO module itself provides the connectivity to the real, physical world via the connected sensors and actuators. This allows determining which vAFs are the critical instances that in fact monitor and control the real, physical world.

The remainder of the paper is structured as follows: Section II gives an overview on related work, and Section III on industrial security. Section IV describes the concept of physical world access attestations, and Section V presents a usage scenario in an industrial Operation Technology (OT) environment. Section VI provides an evaluation of the presented approach. Section VII concludes the paper and gives an outlook towards future work.

II. RELATED WORK

Cybersecurity for Industrial Automation and Control Systems (IACS) is specified in the standard series IEC62443 [4]. This series provides a security framework as a set of security standards defining security requirements for the development process and the operation of IACS as well as

technical cybersecurity requirements on automation systems and the used components. An overview on industrial security and IEC62443 is given in section III.

The Trusted Computing Group (TCG) defined attestation as the process of vouching for the accuracy of information [5]. An attestation is a cryptographically protected data structure that asserts the accuracy of the attested information. The Remote Attestation procedureS (RATS) working group of the Internet Engineering Task Force (IETF) described various attestation use cases [6]. Examples are the attestation of platform integrity and the attestation of the implementation approach for a cryptographic key store. An attestation allows a communication peer to reliably determine information about the (remote) platform besides the authenticated identity.

Virtualized automation functions have been described, e.g., by Gundall, Reti, and Schotten [7] investigating opportunities and challenges of hardware and operating system-level virtualization, and by Givehchi, Imtiaz, Trsek, and Jasperneite [8] presenting a performance evaluation of a cloud-based virtualized programmable logic controller.

III. INDUSTRIAL SECURITY

A CPS, e.g., an Industrial Automation and Control System (IACS), monitors and controls a technical system. Examples are process automation, machine control, energy automation, and cloud robotics. The impact of a vulnerability in the OT system may not only affect data and data processing as in classical Information Technology (IT), but it may have an effect also on the physical world. For example, production equipment could be damaged, or the physical process may operate outside the designed physical boundaries, so that the produced goods may not have the expected quality, or even safety-related requirements could be affected. Protecting IACSs against intentional attacks is increasingly demanded by operators to ensure a reliable operation, and also by regulation [9]. This section gives an overview on industrial security, and on the main relevant industrial security standard IEC 62443 [4] detailing security requirements for development, integration, and operation of IACS.

Cybersecurity mechanisms have been known for many years and are applied in smart devices (Internet of Things, Cyber Physical Systems, industrial and energy automation systems, operation technology). Such mechanisms target source authentication, system and communication integrity, and confidentiality of data in transit or at rest. Authentication, communication security, and authorization are also the basis for a Zero Trust (ZT) security approach. A ZT core principle is to assume that breaches may happen, and to verify explicitly security properties to improve the security posture before allowing access to resources and to avoid lateral threat movement. A ZT approach depends on security controls to assess, detect, and report attacks, and to act correspondingly. A resilience management function, as supported by the described monitoring functionality in this paper, can be used to keep an attacked CPS operational, and to recover quickly from attacks [10].

Industrial security is called also OT security, to distinguish it from general IT security. Industrial systems have not only different security requirements compared to general IT systems but come also with specific side conditions preventing the direct application of security concepts established in the IT domain in an OT environment. For example, availability and integrity of an automation system often have a higher priority than confidentiality. As an example, high availability requirements, different organization processes (e.g., yearly maintenance windows), and required component or system certifications may prevent the immediate installation of software or firmware updates.

The three basic security requirements in IT environments are confidentiality, integrity, and availability ("CIA" requirements). This CIA order corresponds to the classical priority of these basic security requirements. However, in OT systems, e.g., industrial automation systems or industrial IT, the priorities are often just the other way around: Availability of the IACS has typically the highest priority, followed by integrity. Confidentiality is often no strong requirement for control communications, but it may be needed to protect critical business know-how.

The international industrial security framework IEC 62443 [4] is a security requirements framework defined by the International Electrotechnical Commission (IEC). It addresses the need to design cybersecurity robustness and resilience into industrial automation and control systems, covering both organizational and technical aspects of security over the life cycle. Specific parts of this framework are applied successfully in different automation domains, including factory and process automation, railway automation, energy automation, and building automation. The standard specifies security for IACS along the lifecycle of industrial systems. Specifically addressed for the industrial domain is the setup of a security organization and the definition of security processes as part of an Information Security Management System (ISMS) based on already existing standards like ISO 27001 [11] or the NIST cyber security framework [12]. Furthermore, technical security requirements are specified distinguishing different security levels for industrial automation and control systems, and also for the used components. The standard has been created to address the specific requirements of IACS. Zones of an IACS having different security demands can be distinguished.

The parts of the IEC62443 standard are grouped into four clusters, covering:

– common definitions and metrics,
– requirements on setup of a security organization (ISMS related, similar to ISO 27001), as well as solution supplier and service provider processes,
– technical requirements and methodology for security on system-wide level, and
– requirements on the secure development lifecycle of system components, and security requirements to such components at a technical level.

The framework parts address different roles (actors) over different phases of the system lifecycle: The operator of an IACS operates the IACS that has been integrated by the system integrator, using components of product suppliers. In the set of corresponding documents, security requirements are

defined, which target the solution operator and the integrator but also the product manufacturer.

Part IEC62443-3-3 [13] defines technical security requirements for IACS, grouped into seven so-called foundational requirements. The foundational requirement FR6 "Timely Response to Events" defines security requirements for audit logs and continuous security monitoring. The requirements are specified in a way that they can be implemented in different ways. The approach described in this paper supports monitoring requirements for virtualized IACS components connected to the physical world.

IV. Physical World Access Attestation

A cryptographically protected PWAA is issued by an input/output (IO) module confirming in a reliable way that a certain vAF instance has in fact access to that IO module, i.e., that it has access to the physical world. This information can be used for monitoring the CPS operations as well as for adapting access permissions of the vAF. It can be reliably determined whether the intended vAFs have in fact access to the physical world. Furthermore, only those vAFs having the privilege of accessing the physical world can be granted access to perform security-critical operations during production, e.g., providing production data to a product database or executing control commands on attached actuators. Similarly, a corresponding attestation can be provided by virtual, simulated IO modules, confirming explicitly that this virtual IO module is *not* providing access to the real, physical world.

A. CPS System Model

Figure 1 shows an example of a CPS where multiple vAFs monitor and control the physical world via sensors (S) and actuators (A) connected to IO Modules (IOM). The vAFs exchange messages with IOMs over a data communication network (control network).

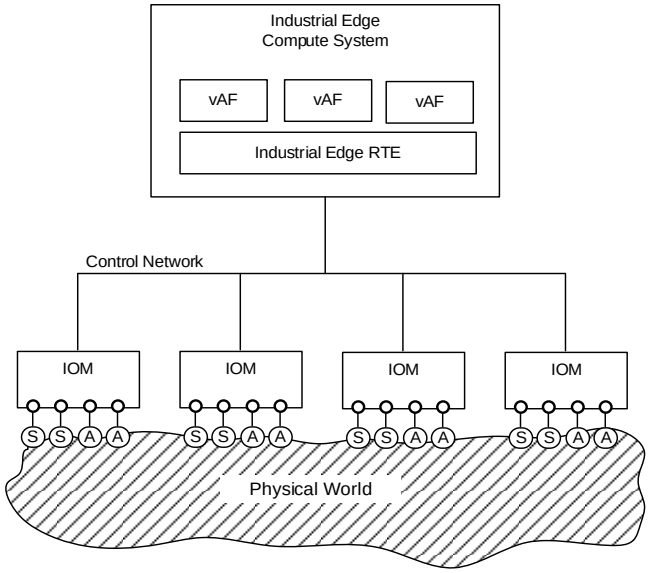

Figure 1. CPS system model

The vAFs are executed on an industrial edge compute system by an industrial edge RunTime Environment (RTE). It would also be possible that vAFs are executed on different edge compute systems or on a backend compute system (cloud-based control). A vAF can be realized, e.g., as container, as virtual machine, or also as native application executed by an operating system.

As depicted in Figure 1, an IOM is directly connected to physical sensors and actuators that in turn provide the interaction with the real, physical world. Thus, these IO modules are crucial as they control on one hand the actions to be performed in the physical world, but also provide monitoring data received from the physical world via the sensors.

B. Physical-World Access Attestation

An IOM authenticates the vAF that is accessing the IOM, e.g., by using a mutual certificate-based network authentication, e.g., Transport Layer Security (TLS) [14], Datagram TLS (DTLS) [15], QUIC [16], IKEv2 [17], or MAC security [18]. The IOM creates a cryptographically protected attestation, i.e., the PWAA, that confirms reliably which vAF is accessing this IOM, thereby confirming that the identified vAF has access to the sensors/actuators connected to the IOM, and thereby consequently having access to the physical world.

The PWAA confirms, based on the authenticated communication session between a vAF and the IOM, that the authenticated vAF has currently access to the physical world via this IOM. In addition, the PWAA may also provide additional information like information about the sensors and actuators connected to the IOM (e.g., identifier, type, calibration data), or about its location. The IOM may include a fixed, configurable location information, or may determine its location dynamically using a localization system.

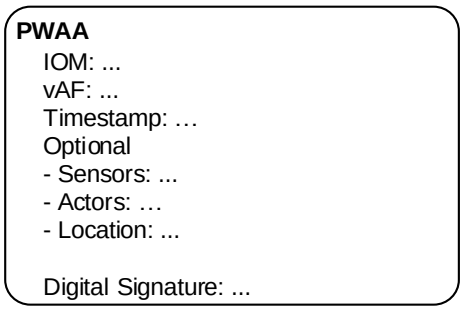

Figure 2. Physical world access attestation

Figure 2 visualizes the main elements of a PWAA. It indicates the IOM, the vAF, and it includes furthermore a timestamp to ensure freshness, and a digital signature of the IOM issuing the PWAA. The identification of the IOM and also the vAF may be done based on the credentials used for the mutual authentication between both. Optionally, the PWAA can comprise also an information on the sensors and actuators to which the indicated vAF has access, or on its location. The digital signature ensures that any manipulation of the PWAA can be detected. The PWAA can be encoded, e.g., as JSON Web Token (JWT) [19], as Concise Binary

Object Representation (CBOR) [20], or as encoded Abstract Syntax Notation One (ASN.1) [21]. The digital signature can be realized using common cryptographic signature schemes, e.g., RSA signature, ECDSA, EdDSA [22], or a post-quantum safe digital signature scheme as CRYSTALS-Dilithium [23] or FALCON [24].

C. IO Module with Real-world Access Attestation

The PWAA is issued by an IOM depending on the authenticated entity that is accessing the IOM. Consequently, the IOM includes an attestation unit that determines the content to be attested depending on the authenticated vAF that is connected to the IOM, and that creates and provides the cryptographically protected PWAA.

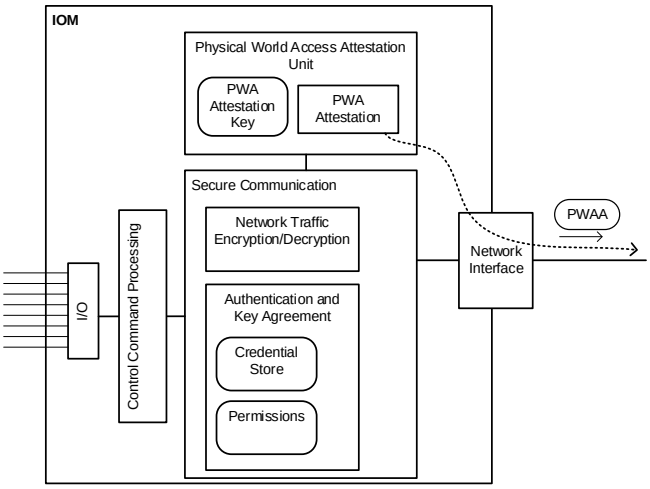

Figure 3. IO module with physical world access attestation

Figure 3 shows an IOM that includes an attestation unit that determines and provides the PWAA to a relying party, e.g., a CPS management system, a device management server, or a dedicated physical world access monitoring system. The IOM comprises an input-output interface (I/O) to which sensors and actuators can be connected. The IOM can be accessed via its network interface using a mutually authenticated secure communication session. The physical world access attestation unit determines which vAF has been authenticated by the IOM to establish a secure communication session, and builds a cryptographically protected PWAA. The digital signature of the PWAA may be build using the same credentials as used for mutual authentication or by distinct ones.

D. Adapting Access Permissions

The PWAA provided by an IOM is verified by a relying party, e.g., a production management system. Depending on the PWAA, it can adapt access control information related to the vAF that is indicated by the PWAA. Thereby, the PWAA can be seen as a context information that is used for access control decisions. This approach is related to a zero-trust security concept, where context information of both the requester and the responder is taken into account for making access control decisions.

E. Integrating with System Integrity Monitoring

The PWAAs provided by IOMs can also be used by a CPS integrity monitoring systems as described in [25]. It allows to determine reliably which vAF instances are the "real" ones that in fact have access to the physical world. Those vAFs are the ones that are subject to the operative CPS integrity monitoring. Other vAF instances may be used for simulations, tests, or as redundant backup functions.

Monitoring of PWAAs allows to detect if a vAF that is not intended to be used for operational control of real-world systems is connect to an IOM giving access to the physical world.

V. USAGE EXAMPLE

This section describes the usage of PWAA for CPS in an exemplary way. Figure 4 shows a CPS usage scenario comprising two control networks for two production networks (zone1, zone2) and a plant network. It can realize, e.g., a discrete production process on a manufacturing shop floor or a process automation system. The automation system is virtualized, i.e., it is realized by virtual automation functions (vAF) that are executed on an on-premise compute infrastructure (Industrial Edge Compute System) or in a backend computing infrastructure, e.g., a hyperscaler cloud or a multiaccess edge computing infrastructure of a mobile communication network. An industrial edge Run-Time Environment (RTE) executes the vAFs.

The vAFs interact with the real-world using sensors (S) and actuators (A) that are connected directly to IOMs. Sensors can measure, e.g., temperature, pressure, movement speed, power consumption, or detect physical objects. Actuators can cause a movement of a tool or the produced good, influence a motor speed, open or close a valve. The vAFs and the IOMs communicate via a communication network, e.g., Ethernet, WLAN, or using a 5G mobile shopfloor communication system.

In addition to the IOMs connected to the control network, also remote IO modules (rIOM) connected to the IOMs can be used. The IO modules (IOM, rIOM) provide a PWAA to a physical world access monitoring system. Optionally, also the RTEs executing the vAFs can provide attestations confirming to which IOMs a vAF is connected.

The physical world access monitoring system determines which vAFs have access to the physical world. Depending on the monitoring results, an authorization token, e.g., an OAUTH token [26], a verifiable credential [27], or an attribute certificate [28], can be provided to the vAF, or it can be granted the permission to perform a startup procedure of a technical system, e.g., a production machine. It is also possible to adapt access permissions of a vAF, e.g., to access a production management system or a Supervisory Control And Data Acquisition (SCADA) system.

Moreover, based on the context information contained in the PWAA, a pwAccess monitoring system as shown in Figure 4 can use this information to derive a system state based on specific sensor and actuator information. This system state can characterize if the system is operating in normal mode, in alert mode, or even in emergency mode,

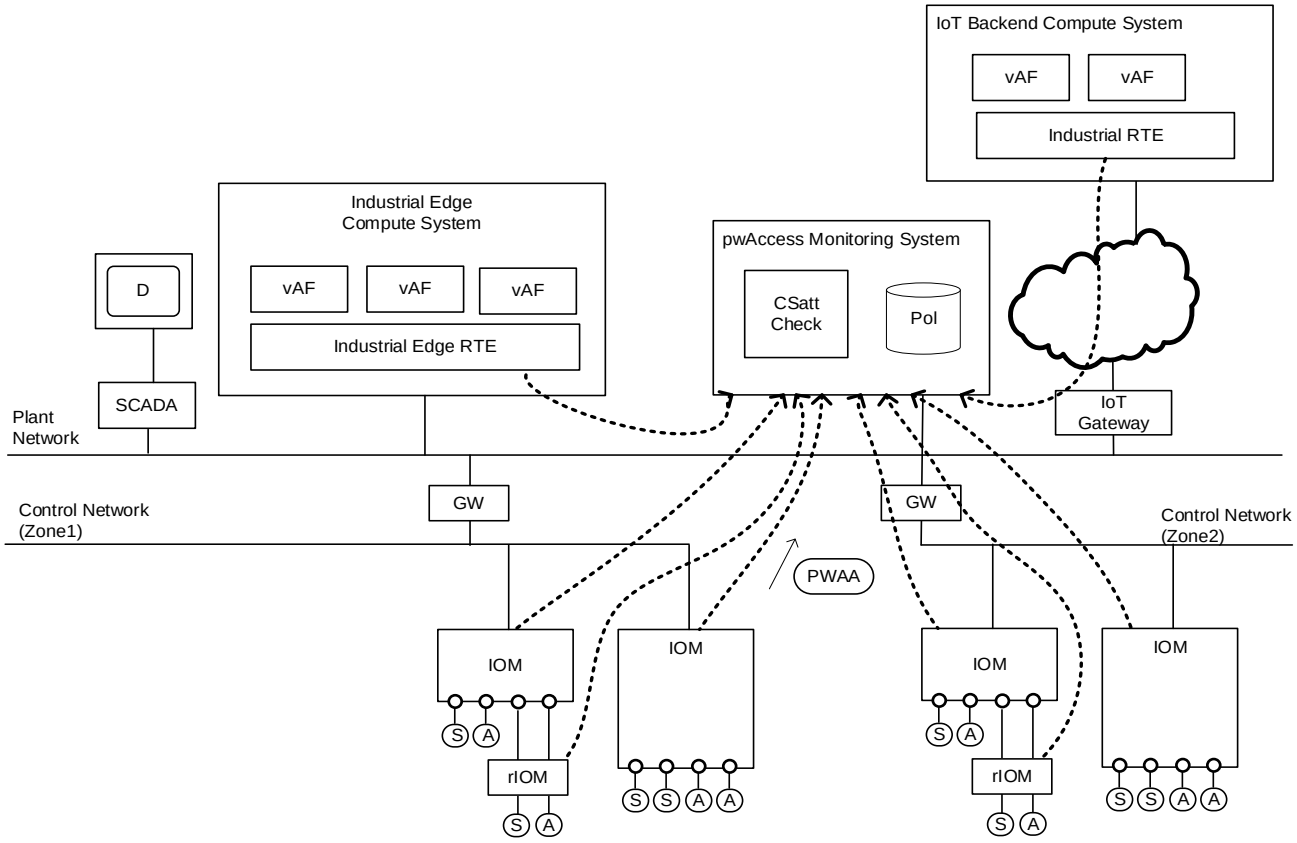

Figure 4. Example PWAA usage scenario

based on the evaluation of the actual measured values with potentially simulated and thus expected values. This derived system state in turn may influence further access decisions. This may be specifically important for systems in a critical infrastructure, like a power generation or distribution facility.

Here, it may be important to bind access decisions on the overall system state to ensure reliable operation of the system.

Furthermore, external provided system state information may also influence the access decision. An example may be the information about a maintenance period, to ensure that certain operation of a system is not possible during this time. Likewise, information about the operational environment can be considered, e.g., if a fire is detected in the production facilities.

The physical world access monitoring system is shown as dedicated component. However, it is also possible to realize it as virtualized function, e.g., as virtual machine or as container executed on an edge computing platform.

VI. EVALUATION

This section gives an evaluation of the presented PWAA concept from the perspective of the operator of a CPS, and from the perspective of the IOM implementation. Furthermore, performance impact and provisioning aspects are discussed.

Operator perspective: Availability and the flexibility to adapt to changing production requirements are important requirements for OT operators [29]. The proposed approach allows to apply strict cybersecurity controls automatically only when really needed, i.e., for operational real-world systems. The information may be utilized to report a system overall health state, which in turn can be considered in further access decisions. Other installations can be handled more openly, providing more flexibility.

Implementation perspective: The IOMs have to provide cryptographic attestations. This required support for basic cryptographic operations (cryptographic algorithms, key store, key management) is already available on IO modules that allow authenticated network access. So, only the additional functionality to create and provide attestations has to be implemented.

Performance perspective: The creation of an attestation is expected to have a negligible impact on the real-time performance of the IOM. For example, the signature can be generated during the authentication and key agreement phase of the secure communication protocol between IOM and vAF. Certain parts of the PWAA may also be prepared based on the locally available sensor information to require only minor lookup and completing of the information structure during the actual authentication and authorization phase.

Provisioning perspective: Additional key material has to be provisioned for protecting attestations, as the attestation key should be different to the device authentication key of IO module to have separate key material for different cybersecurity usages. Here, it may be assumed that for certificate management an automated interaction based on typical certificate management protocols like the Certificate Management Protocol CMP [30], Enrollment over Secure Transport EST [31], or the Simple Certificate Enrolment Protocol SCEP [32] is applied to overcome the burden of manual administration. In this context, a separate attestation key pair may be managed in addition to device authentication keys.

The risk reduction that can be achieved by the proposed PWAA can be evaluated using a Threat and Risk Analysis (TRA). A TRA is typically conducted at the beginning of the product design or system development, and updated after major design changes, or to address a changed threat landscape. In a TRA, possible attacks (threats) on the system are identified. The impact that would be caused by a successful attack and the probability that the attack happens are evaluated to determine the risk of the identified threats. The risk evaluation allows to prioritize the threats, focusing on the most relevant risks and to define corresponding security measures. Security measures can target to reduce the probability of an attack by preventing it, or by reducing the impact of a successful attack.

As long as the technology proposed in the paper has not been proven in a real-world operational setting, it can be evaluated conceptually by analyzing the impact that the additional security measure would have on the identified residual risks as determined by a TRA. However, TRAs for real-world CPS are typically not available publicly. Nevertheless, an illustrative example may be given by an automation system as depicted in Figure 4. It can be detected if a vAF that is not intended to be used for operational control is connected inadmissibly to an IOM that is connected to the real, physical world. Based on this detection, an alarm can be triggered to inform security administrators, or the connection could be blocked automatically by the IOM. Thereby, if a vAF that would be used rather for uncritical purposes as tests, simulation, or optimizations would by connected inadvertently or by ignorance to a real-world IOM where it would impact the real, physical word, could be detected in short time, so that corresponding countermeasures can take place.

Threat	Likelihood	Impact	Risk
Device communication intercepted	unlikely	moderate	minor
Device communication manipulated	unlikely	critical	moderate
Wrong vAF connected to physical-world IOM	likely	critical	major
⋮	⋮	⋮	⋮

Figure 5. Example Threats of a Threat and Risk Analysis

Figure 5 shows a simplified table as used typically in a TRA to collect and evaluate relevant threats to a technical system or component. Some selected threats are shown as example entries. Realistic TRAs for real-world systems and components usually contain a much longer list of threats. The likelihood and the impact of the threat is determined by judgement of competent personal, usually in a team including technical experts and people responsible for the product or system, and preferably also people involved in operation. To ensure consistency, typically criteria are defined that specify the conditions to assign a certain category. It has shown to be useful to define and document explicitly the criteria leading to the categorization of likelihood and impact, including also the made assumptions on the operational environment to ensure consistency and to allow for review.

The corresponding risk is determined based on the determined likelihood and impact, see Figure 6. The TRA with prioritized risks is the basis for security design decisions, focusing on the most critical risks. It is the basis to define a security concept that includes suitable protection measures. Protection measures may not be technical measures only, but include as well organizational and personal security measures (e.g., performing regularly security audits and security trainings). Likewise, for certain security measures that cannot be realized directly using installed system components, an operator may define compensating counter measures. An example is the introduction of additional security components for network traffic protection to avoid the replacement of a larger number of system components that are not capable of protecting exchanged data on their own. It is both possible that a security measure reduces the likelihood or the impact of relevant threats. The residual risk has to be accepted by management decision.

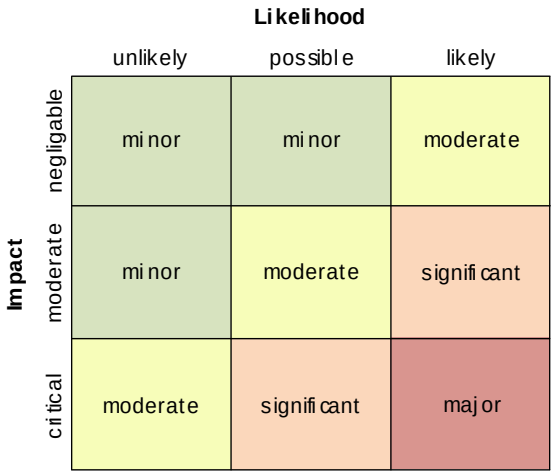

Figure 6. Risk Mapping

Figure 6 shows how the determined likelihood and the impact categories can be mapped to the corresponding risk value. In the example, the three categories unlikely, possible, and likely are used to describe the likelihood. For the impact, the three categories negligible, moderate, and critical are used. In practice, also more fine-granular rankings can be used, distinguishing, e.g., four or five different categories. Also, the risk evaluation can in general include further categories, e.g., disastrous.

For the example threats shown in Figure 5, the risk that the device communication is intercepted is evaluated as minor, as the assumption in the example is that the device communication is protected cryptographically (e.g., by the Transport Layer Security protocol TLS [14] encrypting user data), and that the data would anyhow not reveal highly sensitive information. This results in a "minor" risk. In control communications within industrial automation systems, the confidentiality of control commands and of sensor measurements is often not very critical – but it may be different in specific operator environments when they would reveal sensitive operational parameters of the technical process.

The risk that the communication is manipulated, leading to a manipulated control operation, is unlikely as well, as the communication is assumed to be protected cryptographically in transit (e.g., by the Transport Layer Security protocol TLS [14] using mutual authentication with authenticated encryption, ensuring that user data cannot be manipulated without being detected). However, the impact is evaluated as critical, as, without any further protection, this threat could lead to arbitrary effects on the device operation and therefore also on the CPS. This results in a "moderate" risk.

The risk that a wrong, illegitimate vAF connects to a physical-world IOM is ranked here as major, as the assumption is that authorized operational personnel can flexibly setup and use vAFs, e.g., for simulation, optimization, as well as for control operations. Therefore, it is likely that unintentionally or carelessly a vAF that is not intended and released for operational control operations is connected to a real-world IOM. The impact would be critical as the correct, reliable control operation of the technical system could be affected.

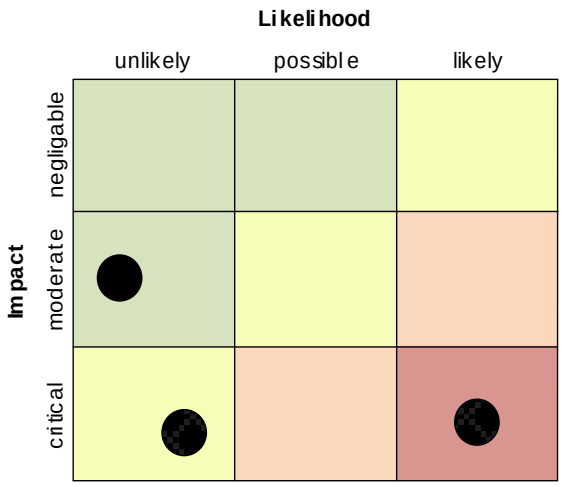

Figure 7. Risk Reporting for the Example Threats without Resilience-Under-Attack Protection

An overview on the determined risks can be shown in a graphical risk reporting as shown in Figure 7. It gives an easily understandable representation on the distribution of identified risks. This representation can be useful to depict the overall risk exposure of a CPS if many risks have been identified. In particular, the example shows the identified "major" risk (red field).

As the impact of the threat cannot easily be reduced in the assumed deployment scenario, the focus is to reduce the likelihood. Besides security training of operational personnel, a further approach to improve the identified "major" risk is to include in CPS integrity monitoring a detection function that identifies with short delay if a vAF that is not intended and released for operational control operations is connected to a real-world IOM. For this purpose, a positive list of vAFs that are approved for operational control of the technical system can be defined. The PWAAs of IOMs are collected regularly and analyzed to determine if a vAF that is not on the positive list is included in a PWAA. An alarm can be triggered to inform operational personnel and security responsibles about the security event and to trigger suitable reaction.

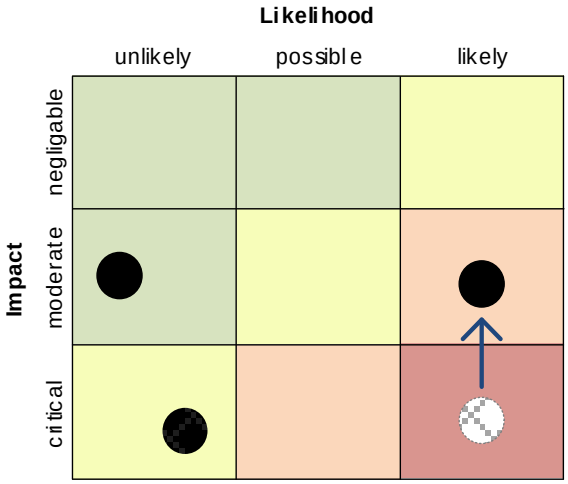

Figure 8. Risk Reporting for the Example Threats with Resilience-Under-Attack Protection

Monitoring PWAAs during CPS operation can reduce the impact of the identified threat, thereby improving the overall risk exposure. This effect is illustrated in Figure 8. In the example shown, the impact of the major risk reduces from critical to moderate, the risk is reduced correspondingly to moderate. Thereby, also the overall risk situation of the overall CPS is improved.

As the evaluation in a real-world CPS requires significant effort, and as attack scenarios cannot be tested that could really have a (severe) impact on the physical world, a simulation-based approach or using specific testbeds are possible approaches, allowing to simulate the effect on the physical world of certain attack scenarios with compromised components in a simulation model of the CPS, or to evaluate it in a protected testbed, e.g., a CPS test system. The simulation would have to include not only the IT-based control function, but also the physical world impact of an attack. Using physical-world simulation and test beds to evaluate the impact of attacks have been described by Urbina, Giraldo et al. [33]. They allow to analyze the impact of successful attacks on the physical world in a safe evaluation environment.

VII. Conclusion and Future Work

The physical-world access attestation and the corresponding evaluation in a process monitoring system proposed in this paper allows to determine reliably which vAFs have in fact access to the real, physical world, i.e., to operational real-world technical systems. This information allows to apply stricter cybersecurity controls automatically specifically to those vAFs and their hosting platforms that are determined to be critical for the real-world CPS operation. It may also improve the operational reliability.

The exact implementation size and performance overhead of a technical realization has still to be evaluated. Cryptographic building blocks are needed to build a physical-world access attestation. As cryptographic building blocks available already within an IOM, e.g., for secure communication with vAFs, can be reused, the overhead in terms of implementation size is expected to be minor. As physical-world access attestations have to be created only rarely compared to protecting real-time control communications, also the overall performance overhead is estimated to be minor.

From a practical perspective, however, it is considered to be more important to determine the usefulness in practical use in operational automation systems, i.e., to what degree monitoring the physical-world access attestations allows to enhance flexibility in CPS planning and operation, and to increase operational efficiency by reducing the time needed for reconfiguring real-world technical systems while still being compliant with the required cybersecurity level. Furthermore, it can be investigated how the monitoring the physical-world access attestations can be best combined with monitoring further attestations, e.g., confirming the integrity of compute platforms and the runtime environment on which vAFs are executed.

References

[1] R. Falk and S. Fries, “Physical World Access Attestation”, CYBER 2023, The Eighth International Conference on Cyber-Technologies and Cyber-Systems, pp 8-11, 2023 [Online]. Available from: https://www.thinkmind.org/index.php?view=article&articleid=cyber_2023_1_20_80021 [retrieved: May, 2024]

[2] M. Gundall, D. Reti, and H. D. Schotten, “Application of Virtualization Technologies in Novel Industrial Automation: Catalyst or Show-Stopper?”, arXiv:2011.07804v1, Nov. 2020, [Online]. Available from: https://arxiv.org/abs/2011.07804 [retrieved: May, 2024]

[3] Plattform Industrie 4.0, “Industrie 4.0 Plug-and-produce for adaptable factories: example use case definition, models, and implementation”, Plattform Industrie 4.0 working paper, June 2017, [Online]. Available from: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/Industrie-40-Plug-and-Produce.pdf [retrieved: May, 2024]

[4] IEC 62443, “Industrial Automation and Control System Security” (formerly ISA99), [Online]. Available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx [retrieved: May, 2024]

[5] Trusted Computing Group, “Glossary”, 2012, [Online]. Available from https://trustedcomputinggroup.org/wp-content/uploads/TCG_Glossary_Board-Approved_12.13.2012.pdf [retrieved: May, 2024]

[6] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan, “Remote ATtestation procedureS (RATS) Architecture”, Internet Request for Comments RFC9334, 2023, [Online]. Available from: https://datatracker.ietf.org/doc/rfc9334/ [retrieved: May, 2024]

[7] M. Gundall, D. Reti, and H. D. Schotten, “Application of Virtualization Technologies in Novel Industrial Automation: Catalyst or Show-Stopper?”, arXiv:2011.07804v1, Nov. 2020, [Online]. Available from: https://arxiv.org/pdf/2011.07804 [retrieved: May, 2024]

[8] O. Givehchi, J. Imtiaz, H. Trsek, and J. Jasperneite, “Control-as-a-service from the cloud: A case study for using virtualized PLCs”, 10th IEEE Workshop on Factory Communication Systems (WFCS 2014), Toulouse, France, 2014, pp. 1-4. Available from: https://ieeexplore.ieee.org/document/6837587 [retrieved: May, 2024]

[9] EU Commission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020”, COM/2022/454 final, Sep., 2022, [Online]. Available from: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [retrieved: May, 2024]

[10] R. Falk and S. Fries, “Enhanced Attack Resilience within Cyber Physical Systems”, International Journal On Advances in Security, vol 16 no 1 & 2, pp. 1-11, June 2023, [Online]. Available from https://www.thinkmind.org/articles/sec_v16_n12_2023_1.pdf [retrieved: May, 2024]

[11] ISO/IEC 27001, “Information technology – security techniques – Information security management systems – requirements”, October 2013, [Online]. Available from: https://www.iso.org/standard/54534.html [retrieved: May, 2024]

[12] NIST, “Framework for Improving Critical Infrastructure Cybersecurity”, Version 1.1, National Institute of Standards and Technology, April, 2018, [Online]. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [retrieved: May, 2024]

[13] IEC 62443-3-3:2013, “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels”, Edition 1.0, August 2013. Available from: https://webstore.iec.ch/publication/7033 [retrieved: May, 2024]

[14] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3”, Internet RFC8446, August 2018, [Online]. Available from: https://datatracker.ietf.org/doc/rfc8446 [retrieved: May, 2024]

[15] E. Rescorla, H. Tschofenig, and N. Modadugu, “The Datagram Transport Layer Security (DTLS) Protocol Version 1.3”, Internet RFC9147, April 2022, [Online]. Available from: https://datatracker.ietf.org/doc/rfc9147 [retrieved: May, 2024]

[16] M. Duke, “QUIC Version 2”, Internet RFC9369, December 2023, [Online]. Available from: https://datatracker.ietf.org/doc/rfc9369 [retrieved: May, 2024]

[17] C. Kaufmann, P. Hoffman, Y. Nir, and P. Eronen, “Internet Key Exchange Protocol Version 2 (IKEv2)”, Internet RFC7296, October 2014, [Online]. Available from: https://datatracker.ietf.org/doc/rfc7296 [retrieved: May, 2024]

[18] “IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control”, IEEE Std 802.1X-2020, February 2020, [Online]. Available from: https://ieeexplore.ieee.org/document/9018454 [retrieved: May, 2024]

[19] M. Jones, J. Bradley, and N. Sakimura, “JSON Web Token (JWT)”, Internet RFC7519, May 2015, [Online]. Available from: https://datatracker.ietf.org/doc/rfc7519 [retrieved: May, 2024]

[20] C. Bormann and P. Hoffman, "Concise Binary Object Representation (CBOR)", Internet RFC8949, December 2020, [Online]. Available from: https://datatracker.ietf.org/doc/rfc8949 [retrieved: May, 2024]

[21] "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU X.690, February 2021, [Online]. Available from: https://www.itu.int/rec/T-REC-X.690 [retrieved: May, 2024]

[22] "Digital Signature Standard (DSS)", FIPS 186-5, February 2023, [Online]. Available from: https://doi.org/10.6028/NIST.FIPS.186-5 [retrieved: May, 2024]

[23] "CRYSTALS-Dilithium", [Online]. Available from: https://pq-crystals.org/dilithium/index.shtml [retrieved: May, 2024]

[24] "FALCON" [Online]. Available from: https://falcon-sign.info/ [retrieved: May, 2024]

[25] R. Falk and S. Fries, "Dynamic Trust Evaluation of Evolving Cyber Physical Systems", CYBER 2022, The Seventh International Conference on Cyber-Technologies and Cyber-Systems, pp. 19-24, 2022, [Online]. Available from: http://thinkmind.org/index.php?view=article&articleid=cyber_2022_1_30_80022 [retrieved: May, 2024]

[26] D. Hardt (Editor), " The OAuth 2.0 Authorization Framework", Internet Request for Comments RFC6749, 2012, [Online]. Available from: https://datatracker.ietf.org/doc/rfc6749/ [retrieved: May, 2024]

[27] D. Longley and M. Sporny, "Verifiable Credential Data Integrity 1.0 – Securing the Integrity of Verifiable Credential Data", W3C Working Draft 15 May 2023, [Online]. Available from: https://www.w3.org/TR/vc-data-integrity/ [retrieved: May, 2024]

[28] "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T X.509, October 2019, [Online]. Available from: https://www.itu.int/rec/T-REC-X.509-201910-I/en [retrieved: May, 2024]

[29] R. Falk and S. Fries, "System Integrity Monitoring for Industrial Cyber Physical Systems", Journal on Advances in Security, vol 11, no 1&2, July 2018, pp. 170-179, [Online]. Available from: www.iariajournals.org/security/sec_v11_n12_2018_paged.pdf [retrieved: May, 2024]

[30] C. Adams, S. Farrell, T. Kause, and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", Internet Request for Comments RFC4210, 2005, [Online]. Available from: https://datatracker.ietf.org/doc/rfc4210 [retrieved: May, 2024]

[31] M. Pritikin, P. Yee, and D. Harkins, "Enrollment over Secure Transport", Internet Request for Comments RFC7030, 2013, [Online]. Available from: https://datatracker.ietf.org/doc/rfc7030 [retrieved: May, 2024]

[32] P. Gutmann, "Simple Certificate Enrolment Protocol", Internet Request for Comments RFC8894, 2020, [Online]. Available from: https://datatracker.ietf.org/doc/rfc8894 [retrieved: May, 2024]

[33] D. Urbina, J. Giraldo, N. O. Tippenhauer, and A. Cardenas, "Attacking fieldbus communications in ICS: applications to the SWaT testbed", Singapore Cyber-Security Conference (SG-CRC), IOS press, pp. 75–89, 2016, [Online]. Available from: http://ebooks.iospress.nl/volumearticle/42054 [retrieved: May, 2024]