Runtime Trustworthiness Evaluation of Evolving Cyber Physical Systems

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

Abstract—**The integrity of Cyber Physical Systems (CPS) needs to be protected to ensure a reliable, trustworthy operation. The hardware and software components of a CPS must be in a well-defined, approved configuration state. However, such system integrity protection becomes increasingly challenging with CPSs that are flexibly reconfigured to address evolving demands. An approach for integrity monitoring for such dynamic CPSs is described. Instead of preventing changes to a CPS, the focus is on detecting changes and on analyzing and checking whether the detected changes are in-line with a policy defining permitted changes. A key element is a reliable device lifecycle state attestation, so that a CPS integrity monitoring system can determine the current configuration state of CPS components and the way in which it was changed.**

Keywords–system integrity; trustworthiness; device integrity; attestation; lifecycle; resilience; cyber physical systems; Internet of Things; cyber security.

I. INTRODUCTION

The integrity and resilience of Cyber Physical Systems (CPS), e.g., technical automation and control systems, are highly relevant security objectives [1]. Unauthorized changes the configuration of a CPS have to be prevented as well as detected. Related security requirements are defined by the industrial security standard IEC62443 [2]. Such security objectives could even be pushed by related regulative requirements, as can be seen, e.g., in the proposed update to the EU Network Information Security (NIS) directive [3].

A concept for enhanced integrity monitoring of overall industrial automation and control systems, combining integrity monitoring from physical processes up to its control and support systems, has been described in [4]. Enhanced attack resilience allows an operator to keep the CPS operational, possibly with some limitations, even during an ongoing attack [5]. Particularly challenging are CPSs with a dynamically changing configuration as driven by the flexibility of IIoT and Industry 4.0. Cyber systems will become more open and dynamic to support flexible production down to "lot size 1" by supporting plug-and-work reconfiguration of manufacturing equipment and flexible adaptation of production systems to changing needs, and by increasingly adopting software-based automation and control functions. This implies that also security has to support such dynamically CPSs that are evolving over time in a practical way.

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 adapted flexibly to changing production needs have been described in the context of Industry 4.0 [6]. The flexibility starts at the device level, where smart devices allow for upgrading and enhancing the device functionality by user-downloadable apps, and by the increasing software-based realization of automation and control functions. Besides the device level, also the system of interconnected machines is reconfigured according to changing needs. Examples are Software Defined Networks (SDN) enabling a fast reconfiguration of the communication infrastructure to adapt flexibly to the communication needs and the use of wireless communications as wireless LAN of private 5G networks. Another example relates to manufacturing systems (e.g., robots) in industrial automation systems, where smart tools are attached to a robot that in turn feature also a local communication network connecting to the robot's network.

The focus of cyber security is protection against cyber attacks, their detection, and the recovery from successful cyber attacks. An increasingly important further aspect is trustworthiness, where automated checks verify whether the overall systems and the used components meet the explicitly defined trustworthiness criteria. However, the concept of trustworthiness is subjective. The presented approach checks for changes within a CPS to determine whether the CPS configuration is in a permitted, trustworthy state.

Section II gives an overview on related work. After describing shortly industrial CPS in Section III, previous work on protecting integrity of cyber physical systems and their components is summarized in in Section IV. The monitoring of reliable device lifecycle information based on lifecycle state attestations is described in Sections V and VI, extending CPS integrity monitoring information. Approaches for analyzing detected lifecycle state attestations are described Section VII. Section VIII evaluates the presented approach. Section IX concludes the paper and gives an outlook towards future research.

II. Related Work

The objective of CPS system integrity and CPS resilience is to support the trustworthiness of CPS. While not new, the concept of trustworthiness is gaining increasing interest in ongoing research and standardization: The standard ISO/IEC TS 5723 [7] published in 2022 defines trustworthiness of systems and the characteristics of trustworthiness, addressing products, services, technologies as well as the trustworthiness of organizations that are providing these. A common understanding and description of trustworthiness characteristics allows stakeholders to judge whether their trustworthiness expectations are met. Mohammadi describes in [8] a trustworthiness framework for CPS that covers development phases like requirements engineering and system design, but also run-time maintenance, and evidence-based assurance. Also, evaluation of trustworthiness during CPS runtime is covered by monitoring its trustworthiness properties. Jiang proposed a data-driven vulnerability analysis for CPS using machine learning [9]. Northern, Burks, Hatcher, Rogers, and Ulybyshev described a methodology to determine a hardened CPS configuration by analyzing cyber vulnerabilities [10]. Cyber risk scores for different CPS configurations are compared, and vulnerable CPS components are replaced or reconfigured. Malik and Tosh described a framework for the dynamic risk assessment and analysis of CPS using multi-formatted knowledge bases derived from open-source vulnerability databases [11]. M. Tapia, P. Thier, S. Gößling-Reisemann performed an empirical study on the vulnerability and resilience of cyber-physical power systems [12]. A resilience management approach is proposed that targets a better handling of CPS failures. The proposed resiliency measures address the categories technology, organizational security policies and procedures, human factor, and regulations. Akbarzadeh and Katsikas described a cybersecurity risk assessment method that addresses the interactions and interdependencies between the cyber and the physical components using a model of the CPS and its components [13].

Requirements related to resilience on device level have been addressed in different standards. The Trusted Computing Group (TCG) specified requirements for cyber resilient modules and building blocks [14]. It describes architectural elements on device level for resilience (resilience target, resilience engine, resilience authority), as well as building blocks as, e.g., storage protection and attention signal generators. Recommendations for resiliency of platform firmware and data have been described by [15], supporting a rapid and secure recovery from attacks on platform firmware of computer devices. Also, the standard ETSI EN303 645 on baseline security requirements for consumer IoT includes resilience-related requirements [23].

Segovia, Rubio-Hernan, Cavalli and Garcia-Alfarometrics define a metric based on control theory to quantify the cyber-resilience level of a CPS based on the design, structure, stability, and performance under attack [16]. The metric is related to the mathematically modelled control function of a CPS. Khazraei. Hallyburton, Gao, Wang and Pajic describe how deep learning can be applied for vulnerability analysis of CPS control mechanisms [17].

III. Industrial Cyber Physical Systems

A CPS, e.g., an industrial automation and control system, monitors and controls a technical system. Examples are process automation, machine control, energy automation, and cloud robotics. Figure 1 shows an example of an industrial automation and control system, comprising

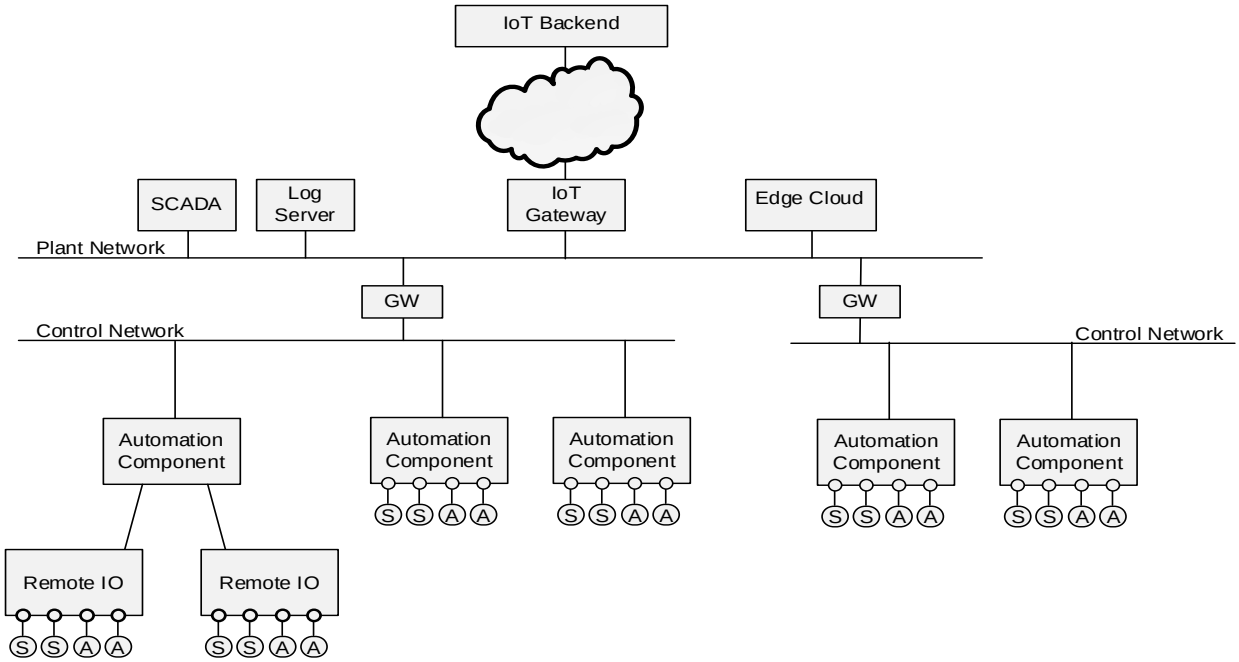

Figure 1. Example CPS System

different control networks connected to a plant network and a cloud backend system. Automation control equipment with sensors (S) and actuators (A) is connected directly with automation components, or via remote input/output modules. The technical process is controlled by measuring its current state using the sensors, and by determining the corresponding actuator signals. Separation of the network is typically used to realize distinct control networks with strict real-time requirements for the interaction between sensors and actuators of a production cell, or to enforce a specific security policy within a production cell. Such an industrial automation and control system is an example of a CPS. Industrial automation and control systems are utilized in various automation domains, including discrete automation (factory automation), process automation, railway automation, energy automation, and building automation.

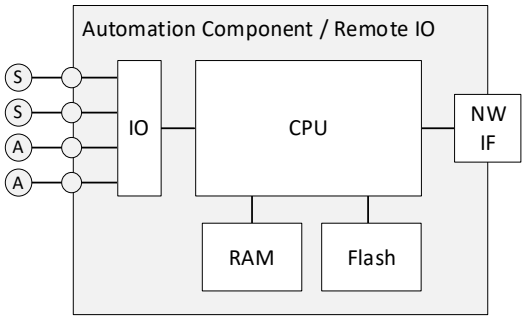

Figure 2. Automation Component

Figure 2 shows the typical structure of automation components of a CPS that monitor and control the physical world using sensors (S) and actuators (A). The monitoring and control functionality is defined by its firmware/software that is executed on a central processing unit (CPU) and the corresponding configuration data, both stored in non-volatile memory (Flash). A network interface (NW IF) allows communication with other devices, e.g., via Ethernet or via wireless communications as wireless local area network (WLAN) or a private 5th generation (5G) mobile communication system.

In cyber physical systems, the impact of a vulnerability in the OT system may not only affect data and data processing as in classical 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.

IV. CPS System Integrity protection

Information Technology (IT) security 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. System integrity takes a broader approach where not only the integrity of individual components (device integrity) and of network communications are addressed, but where integrity shall be ensured at the overall system level of multiple interconnected devices.

A. Industrial Security

Protecting industrial automation and control systems against intentional attacks is increasingly demanded by operators to ensure a reliable operation, and also by regulation. The main relevant industrial security standard that describes security from a holistic view is IEC 62443 [2]. Security requirements defined by the industrial security standard IEC 62443 range from security processes during development and operation of devices and systems, personal and physical security, device security, network security, and application security, addressing the device manufacturer, the integrator as well as the operator of the industrial automation and control system.

Industrial security is also called Operation Technology (OT) security, to distinguish it from general IT security. Industrial systems have different security priorities and requirements compared to common IT systems. Typically, availability and integrity of an automation system have higher priority than confidentiality.

Specific requirements and side conditions of industrial automation systems like high availability, planned configuration (engineering info), scheduled maintenance windows, long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements have to be considered when designing an OT security solution.

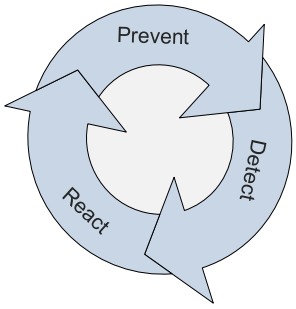

Figure 3. Prevent Detect React Cycle

Overall, security has to address the areas prevent, detect, and react, see Figure 3. It is not sufficient to only define security measures to protect against attacks. The cycle shows also the need for detecting attacks, and to define measures to react adequately once an attack has been detected. The approach describes in this paper puts more effort on the "detect" and "react" phases than on the "prevent" phase with the intention to supported increased CPS productivity by allowing for high flexibility of CPS reconfigurations.

B. Device Integrity

The objective of device integrity is to ensure that a single device is not manipulated in an unauthorized way, ensuring that it operates as genuine device. Integrity protection includes the integrity of the device firmware, the integrity of

the device configuration, but also its physical integrity. The main technologies to protect device integrity are:

- Secure boot: A device loads at start-up only unmodified, authorized firmware.
- Measured boot: The loaded software modules are checked at the time they are loaded. Usually, a cryptographic hash value is recorded in a platform configuration register of a hardware of firmware Trusted Platform Module (TPM). The configuration information can be used to grant access to keys, or it can be attested towards third parties.
- Protected firmware update: When the firmware of a device is updated, the integrity and authenticity of the firmware update is checked. The firmware update image can be digitally signed.
- Application whitelisting: Only allowed, known applications can be started on a device. A whitelist defines which application binaries can be started.
- Runtime integrity checks: During operation, the device performs a self-test of security functionality and integrity checks to verify whether it is operating as expected. Integrity checks can verify the integrity of files, configuration data, software modules, and runtime data as the process list, i.e., the list of currently executed processes.
- Process isolation, kernel-based Mandatory Access Control (MAC): Hypervisors or kernel-based MAC systems can be used to isolate different classes of software (security domains). An attack or malfunction of one security domain does not affect other security domains on the same device.
- Tamper evidence, tamper protection: The physical integrity of a device can be protected, e.g., by security seals or by tamper sensors that detect opening or manipulation of the housing.
- Device integrity self-test: A device performs a self-test to detect failures. The self-test is performed typically during startup and is repeated regularly during operation.
- Operation integrity checks: measurements on the device can be compared with the expected behavior in the operative environment. An example is the measurement of connection attempts to/from the device, based on parameters of a Management Information Base (MIB).

The established approaches to protect device integrity focus on its IT-related functionality of a device. The main protection objective for device integrity is to ensure that the device's control functionality operates as designed. However, the integrity of input/output interfaces, sensors, and actuators are typically out of scope. In typical industrial environments, applying a strong tamper protection to each control device, sensor, and actuator would not be economically feasible. A strong physical tamper protection is not common at device level, as it would complicate not only the production of a devices, but also the test, service, and repair. Therefore, protecting device integrity of used devices alone would be too limited to achieve the goal of protection the integrity of an overall CPS.

C. Cyber Physical System Integrity Monitoring

Classical approaches for protecting device and system integrity target at preventing any changes and compare the current configuration to a fixed reference policy. More flexible approaches are needed to protect integrity for flexibly reconfigurable and self-adapting CPSs. In previous work [4], we described an integrated, holistic approach for ensuring CPS integrity as an extensible framework to include integrity information from IT-based functions and the physical world of a CPS. This allows integrating integrity information from the digital and the physical world. Trusted physical integrity sensors can be installed as add-on to existing automation and control systems. One-way gateways can be used to extract integrity monitoring information from closed control networks, while ensuring freedom from interference for the control function.

Integrity does not only affect single devices, but also the overall system level comprising a set of interconnected devices. The main approaches to protect system integrity are collecting and analyzing information at system level [4]:

- Device inventory: Complete and up-to-date list of installed devices (including manufacturer, model, serial number version, firmware version, current configuration, installed software components, location)
- Centralized Logging: Devices provide log data, e.g., using Open Platform Communication Unified Architecture (OPC UA) protocol, Simple Network Management Protocol (SNMP), or syslog protocol, to a centralized logging system for further analysis. This may be done in a Security Information and Event Management (SIEM) System and lead to reactions on identified cybersecurity events.
- Runtime device integrity measurements: A device integrity agent provides information gathered during the operation of the device (see also subsection B above). It collects integrity information on the device and provides it for further analysis. Basic integrity information includes the results of a device self-test, and information on the current device configuration (firmware version, patches, installed applications, configuration). Furthermore, runtime information can be gathered and provided for analysis (e.g., process list, file system integrity check values, partial copy of memory).
- Network monitoring: The network communication is intercepted, e.g., using a network tap or a mirror port of a network switch. A challenge is the fact that network communication is increasingly encrypted.
- Physical Automation process monitoring: Trusted sensors provide information on the physical world that can be used to cross-check the view of the control

system on the physical world. Adding trusted sensors to existing installation allows for a smooth migration from legacy systems to systems providing integrated sensors as they can be used for plausibility checks.

– Physical world integrity: Trusted sensors (of physical world), integrated monitoring of embedded devices and IT-based control systems, and of the technical process allow now quality of integrity monitoring as physical world and IT world are checked together.

The captured integrity information can be used for system runtime integrity monitoring to detect integrity violations in real-time. Operators can be informed, or actions can be triggered automatically. Furthermore, the information is archived for later investigations. This allows that integrity violations can be detected also later with a high probability, so that corresponding countermeasures can be initiated (e.g., plan for an additional quality check of produced goods). The integrity information can be integrated in or linked to data of a production management system, so that it can be investigated under which integrity conditions certain production steps have been performed. Product data is enhanced with integrity monitoring data related to the production of the product. Moreover, the data may also be used in the context of supply chain security to support trustworthiness claims.

An intelligent analysis platform performs data analysis (e.g., statistical analysis, big data analysis, artificial intelligence) and triggers suitable respondence actions (e.g., alarm, remote wipe of a device, revocation of a device, stop of a production site, planning for additional test of manufactured goods). The analysis can combine monitoring information originating from IT-related control functions, from physical security systems, as well as from the operation of the actual technical process.

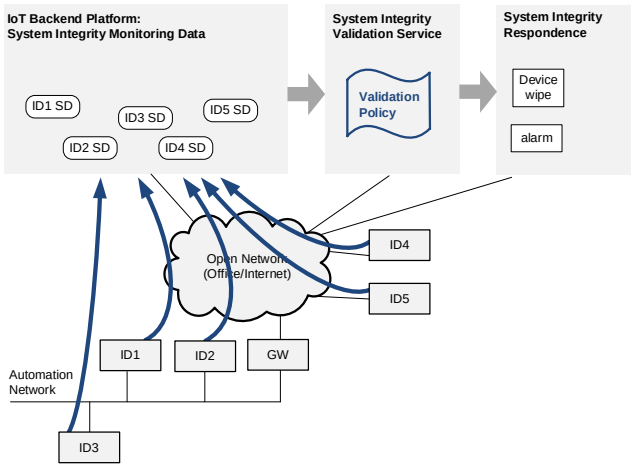

Figure 4. CPS Integrity Monitoring System [4]

Figure 4 shows an example for an IoT system with IoT devices (ID1, ID2, etc.) that communicate with an IoT backend platform. The devices provide current integrity monitoring information to the backend platform. The devices can be automation devices that include integrity measurement functionality, or dedicated integrity sensor devices. The device monitoring system itself has to be protected against attacks, following the industrial security standard IEC 62443.

An integrity data validation service checks the obtained integrity measurement data for validity using a configurable validation policy. If a policy violation is detected, a corrective action is triggered. For example, an alarm message can be displayed on a dashboard. Furthermore, an alarm message can be sent to the IoT backend platform to terminate the communication session of the affected IoT device. Moreover, the device security service can be informed so that it can revoke the devices access permissions or revoke the device authentication credential.

The integrity monitoring events are analyzed using known data analysis tools. As stated before, in industrial environments, it is also important to have reliable information about the system integrity of a production system for the time period during which a certain production batch was performed. This allows performing the verification also afterwards to check whether during a past production batch integrity-violations occurred.

The final decision whether a certain configuration is accepted as correct is up to human operators. After reconfiguration, or for a production step, the configuration is to be approved. The approval decision can be automated according to previously accepted decisions, or preconfigured good configurations.

D. Resilience Under Attack

Being resilient means to be able to withstand or recover quickly from difficult conditions [18]. It shifts the focus of "classical" IT and OT security, which put the focus on preventing, detecting, and reacting to cyber-security attacks, to the aspect to continue to deliver an intended outcome despite an adverse cyber attack taking place, and to recover quickly back to regular operation. More specifically, resilience of a system is the property to be resistant to a range of threats and withstand the effects of a partial loss of capability, and to recover and resume its provision of service with the minimum reasonable loss of performance [19].

Risk management, the established approach to cyber security, identifies threats and determines the risk depending on probability and impact of a potential attack. The objective is to put the focus of defined security measures on the most relevant risks, reducing the probability that a successful attack takes place, and reducing the impact of successful attacks, e.g., by detect successful attacks by security monitoring allowing to react, e.g., by shutting down a CPS. Resilience, however, puts the focus on a reduction of the impact of successful attacks, where the system can stay operational with a degraded performance or functionality, and to recover quickly from a successful attack. Robustness is a further related approach that tries to keep the system operational *without* a reduction of the system performance, i.e., to withstand attacks.

Figure 5 illustrates the concept of cyber resilience: Even if an attack is carried out, the impact on the system operation, i.e., the performance or functionality of the

system, is limited [5]. The effects of an attack are "absorbed", so that the system stays operational, but with limited performance or functionality. A recovery takes place to bring the system up to the regular operation.

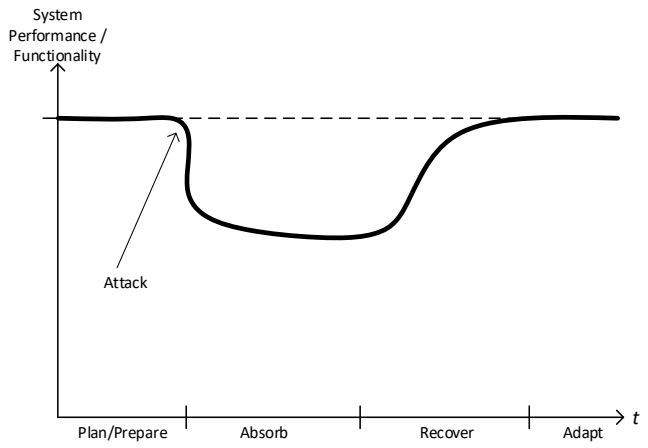

Figure 5. Concept of Cyber Resilience [5]

In adaptation of resilience, the system might be enhanced to better prepare for future attacks leading to a sort of self-healing functionality. In a cyber physical environment, a main objective is that the CPS stays operational and that its integrity is ensured. In the context of an industrial automation and control system, that means that intended actions of the system in the physical world continue to take place even when the automation and control system of the CPS should be attacked successfully.

V. LIFECYCLE CONFIGURATION CHANGE MONITORING

A main concept presented in this paper is an enhancement to the system-level integrity monitoring system, described in Section IV.C. Instead of comparing integrity measurements describing the current configuration status to a fixed reference policy, the changes to the CPS components and to their configuration are validated during CPS operation. An integrity violation is detected if changes are detected that are not in-line with a policy on what and how changes are applied and when. The changing configuration of CPS components along their lifecycle in the operation of a dynamically evolving CPS is validated to determine whether the CPS is in a trustworthy, authorized state (CPS system integrity).

Lifecycle state agents on the CPS components act as integrity sensors that collect lifecycle state information of a device and provide it in the form of a lifecycle state attestation to the system integrity monitoring system.

Figure 6 shows the basic concept of a CPS lifecycle-change integrity monitoring system. Devices (D) provide Life Cycle State Attestations (LCSA) to a CPS lifecycle-change integrity monitoring system. The CPS lifecycle-change integrity monitoring system determines changes on device lifecycle states based on the provided LCSA attestations, and it validates whether the detected changes are in-line with a lifecycle change validation policy.

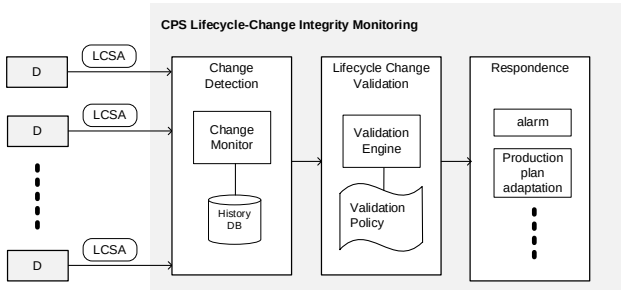

Figure 6. CPS Lifecycle Change Monitoring

The lifecycle change validation policy defines which changes are permitted so that the CPS is considered to be still in a trustworthy configuration state. If the lifecycle change validation policy is violated, e.g., an alarm can be generated, or the CPS operation of the production plan can be adapted accordingly.

VI. DEVICE LIFECYCLE STATE ATTESTATION

Different lifecycle states of industrial IoT devices can be distinguished, including factory default state, commissioned, operational, failure, network connected, provisioned, repair, service, or being put out of service. The current lifecycle state of a device can be determined based on its current configuration data. Some security standards, e.g., ETSI EN 303645 on Consumer IoT Security includes an example of a device life cycle model [23]. Besides the life cycle phase information, also the parts of the specific configuration can be provided as part of the life cycle attestation and analyzed. It is not assumed that a common life-cycle model is explicitly supported by the devices, as in a real-world CPS, different device types originating from various manufacturers are used. Instead, the available information of the device configuration is taken as basis to derive/estimate the related life-cycle phase, at least if it is not provided explicitly.

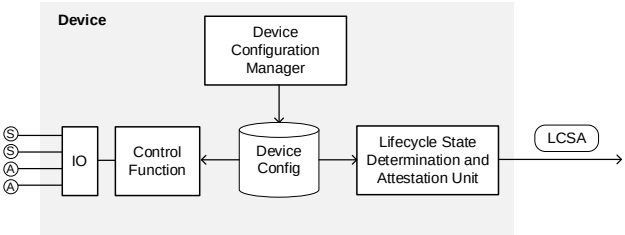

Figure 7. Control Device with Lifecycle State Attestation

A device can determine its own lifecycle state and confirm it externally by a device lifecycle state attestation. Figure 7 shows a device, e.g., a control device for monitoring and controlling a technical process via sensors (S) and actuators (A) by a control function that interacts via an input-output unit (IO) with the sensors and actuators, according to the device configuration established by a device configuration manager. The lifecycle state attestation unit determines the device lifecycle state based on the current

device configuration and creates a cryptographically protected LCSA. Besides the current lifecycle state, also previous lifecycle states can be kept and attested, providing a more comprehensive information on the device lifecycle history. Alternatively, the lifecycle state may be determined and attested by an external add-on component, allowing that a LCSA can be provided also for legacy devices that do not have an integrated functionality for determining and attesting the device lifecycle state.

The LCSA can be provided in a dedicated attestation data structure, i.e., a data structure that describes the current lifecycle state of the device, and that is protected by a cryptographic checksum, i.e., a digital signature or a message authentication code. However, it is also possible to encode the life cycle information in a device credential, e.g., a device authentication certificate, a device attribute certificate, a device authentication token, or a verifiable credential.

VII. Device Lifecycle State Analysis

A simple approach for validating CPS configuration changes would be the manual analysis of detected configuration changes and a manual approval of detected changes by OT personnel. Manual checking and approval would however not scale well for larger CPS that are frequently reconfigured. Therefore, an automatic validation of detected configuration changes is needed. The CPS Lifecycle-change Integrity Monitoring system determines the changes to the CPS configuration based on the obtained device lifecycle state attestations. It validates whether changes are in-line with a lifecycle change validation policy that defines the permitted types of changes to the CPS configuration. If the lifecycle change validation policy is violated, e.g., an alarm can be generated, or the CPS operation or a production plan can be adapted accordingly.

The lifecycle change validation policy defining permitted changes of lifecycle states can be preconfigured. However, this would require significant effort for explicitly defining rules for permitted configuration changes. Therefore, an automated learning system, based on artificial intelligence, is proposed that learns from good examples of permitted changes. In an initial introduction phase, good changes (allowed changes from a system operation level) have to be marked by the OT personnel. Over time, the system learns from these good examples. This approach is conceptually similar to a network firewall for which the filter policy is determined automatically during a learning phase.

Such a self-learning of permitted changes leads to an automated learning of what changes lead to a trustworthy CPS. It is in real-world practice often not easy to determine explicit rules on which specific properties make a component or a change being considered as trustworthy. By learning from good and bad examples, the attributes that are relevant for the trustworthiness evaluation can also be determined over time automatically. The system learns which attributes of a lifecycle state attestation are relevant for determining which changes are permitted. This self-learning approach allows also for subjective trust policies: Different users, i.e., operators of similar CPSs, can give examples of what they consider to be trustworthy or not so trustworthy. Depending on these examples, a trustworthiness evaluation policy is derived. In contrast to conceptually similar approaches like the example of firewalls in learning mode, this approach is more open as even the attributes (criteria) that are relevant for making trust decisions do not have to be predefined. It allows also to distinguish varying operational concepts for CPSs that are operated by different OT operators.

VIII. Evaluation

From the perspective of a real-world CPS, the approach presented in Sections V, VI and VII is not self-contained, but is an extension to other, well-established security measures to protect a CPS. The main advantage comes by the support for increasingly dynamic, evolving CPS. To ensure that a CPS and its components are in a trustworthy state, it is not ensured that the configuration corresponds to a fixed reference, but to check whether the detected changes are acceptable. This approach can compensate when classical, rather strict security controls preventing heavy changes to a CPS cannot be applied anymore in the same way as for static CPS deployments.

The security of a cyber system can be evaluated in practice in various approaches and stages of the system's lifecycle:

- Threat and Risk Analysis (TRA) of cyber system
- Checks during operation to determine key performance indicators (e.g., check for compliance of device configurations).
- Security testing (penetration testing)

During the design phase of a cyber system, the security demand is determined, and the appropriateness of a security design is validated using a TRA. Assets to be protected and possible threats are identified, and the risk is evaluated in a qualitative way depending on probability and impact of threats. The effectiveness of the proposed enhanced device authentication means can be reflected in a system TRA.

The main evaluation using security tools is performed during secure operation, when as part of an overall operational security management appropriate technologies are deployed that, in combination, reduce the risk to an acceptable level. The new approach presented in this paper provides an additional element, integrated into the overall system security architecture that is used to reduce the risk of integrity violations, despite a dynamically changing CPS configuration.

For the applicability to real-world CPS environments, the approach allows for:

- Flexibility for updates: The device life cycle integrity monitoring system can be updated independently from the actual CPS. Therefore, updates can be installed also outside the scheduled maintenance windows of the CPS.
- It can be installed as add-on to existing automation systems (brownfield). It can be introduced stepwise, starting with lifecycle monitoring for most relevant devices.

– It can be installed as an add-on system that does not endanger the reliable operation of a CPS or invalidate its certifications.

Such non-technical properties simplify the adoption in real-world CPS, and they are often important factors for acceptance by OT operators.

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, and on key performance indicators (KPI) of automation and production systems like uptime, availability, output. Actually, the approach of evaluation the impact of different approaches to handle security on KPIs that are not directly security-related is typically not done systematically in the security community. The motivation of the lifecycle security monitoring intends to give high flexibility to reconfigure industrial CPS to changing needs, while still ensuring the required level of security.

It is also an open point how to balance security controls addressing different phases (prevent, detect, react) in an optimized way. The approach described in this paper puts less emphasis on restrictive security measures on the "protect" phase but rather intends to compensate that by automated monitoring of configuration changes ("detect") and to use the high flexibility for CPS reconfiguration to flexibly react also to detected security problems ("react"), improving thereby also the resiliency. Putting these considerations in the context of a TRA, means shifting the focus for reducing identified risks to an acceptable level from reducing the likelihood of a threat occurrence ("prevent") to reducing its impact ("detect" and "react").

Threat	Likelihood	Impact	Risk
Device communication intercepted	unlikely	moderate	minor
Device communication manipulated	unlikely	critical	moderate
Vulnerability in unpatched device exploited	likely	critical	major
Device replaced by fake device	possible	moderate	moderate
⋮	⋮	⋮	⋮

Figure 8. Example Threats of a Threat and Risk Analysis

Figure 8 shows a simplified table as used typically in a threat and risk analysis to collect and evaluate relevant treats to a technical system or component. Some threats are shown as examples. Actual TRAs for real-world systems and components include usually 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, developers, and people responsible for the product or system. The corresponding risk is determined based on likelihood and impact. It has shown to be useful to define and document explicitly the criteria leading to the categorization of likelihood and impact, including also the assumptions made on the operational environment. 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 defines suitable measures for reducing the risk to an acceptable level.

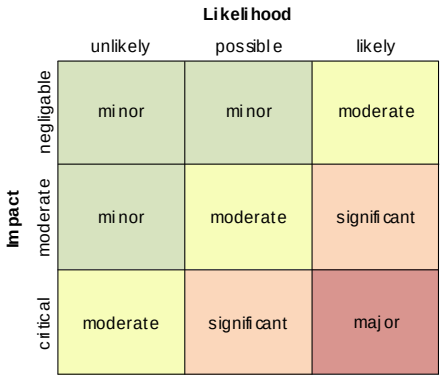

Figure 9. Risk Mapping

Figure 9 shows how the mapping of likelihood and impact 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. It can be seen that a reduction of the risk can be achieved by both, by reducing the likelihood as well as by reducing the impact.

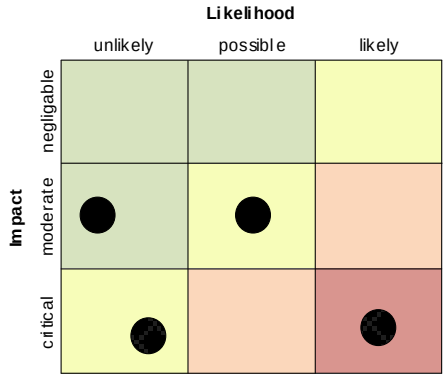

Figure 10. Risk Reporting for the Example Threats

An overview on the determined risks can be shown in a risk reporting as shown in Figure 10. It gives an easily understandable graphical representation on the distribution of risks. This representation can be useful if many risks have been identified. In particular, the example also shows one major threat as well as a moderate threat with critical impact.

The effect of reducing the risk by limiting the impact is illustrated in Figure 11. As, shown in the example, the impact of the two risks with critical impact reduces from critical to moderate, the risk is reduced correspondingly. Thereby, also the overall risk situation of the overall CPS in which the considered device is used, is improved.

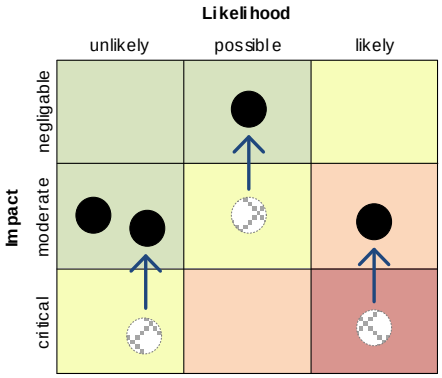

Figure 11. Reducing risk be limiting the impact

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 or evaluate in a protected testbed the effect on the physical world of certain attack scenarios with compromised components. 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. [24]. However, we are not aware of research work that analyzes systematically the impact of different security approaches on operational KPIs of a CPS, e.g., based on simulations or by analyzing data or operational real-world CPSs.

IX. CONCLUSION

Ensuring device and system integrity is an essential security feature for cyber physical systems and the (industrial) Internet of Things. This must be ensured from the beginning using the security design principle of "defense in depth". It allows to support system integrity based on the information provided from single components or devices that build the CPS.

This paper proposed a framework for ensuring system integrity in flexibly adaptable cyber physical systems. With new concepts for flexible automation systems coming with Industrial IoT / Industry 4.0, the focus of system integrity clearly has to move from preventing changes to device and system configuration to having transparency on the device and system configuration and checking it for compliance.

The approaches for integrity monitoring in industrial automation and control systems described in this paper focuses on the operational phase by relying on lifecycle attestations for single components building a CPS. This approach enhances the existing systems, with an attestation about a specific state in the lifecycle, which allows an industrial monitoring system to evaluate the current life cycle state with the expected one. This can be done in addition to classical system monitoring, which verifies configuration and system behavior against expected patterns.

Integrity in a broader sense has to cover the whole life cycle, from development, secure procurement, secure manufacturing, and supply chain security up to the commissioning phase in the operational environment. This lifecycle information can then be used to enhance the current system state information. Due to the life cycle information available on the device or its associated management system, feedback to manufacturer can be provided in case of failure, in which the problem may be traced back to a specific production step. This also allows the manufacturer to better react in future versions of a device. It also allows for informing other users of the same component or systems about potential failure scenarios or situations.

Security-critical operations of a device, e.g., use for control operations, provisioning operational keys, or providing sensitive commissioning data is performed only for devices being in an expected state. A device can be used for regular operational purposes only if, according to its lifecycle, it is in a valid lifecycle state, and if this lifecycle state has been established in a permitted way.

A main objective of the described approach is to support the increase of CPS productivity that is coming with the flexible production of industry 4.0, supporting "lot size 1". The described security approach supports a high flexibility of CPS reconfigurations while still ensuring an appropriate security level. Integrity of the CPS is not ensured by preventing changes to the CPS configuration, but by reliably determining performed configuration changes and by validating whether they are permitted.

Possible future research could analyze systematically the impact of different security approaches on operational KPIs as productivity, defective goods, or whether tight production schedules are met by simulating complete CPS systems under different usage situations and under different attack scenarios. A further approach may be the integration of simulation into existing production environments using a digital twin. This digital twin would then be operated under the same conditions as the physical devices with the option to virtually manipulate parameters of the operational environment to stipulate extreme cases and thus better prepare for timely reactions to potential real events. While such analysis is considered to require some effort, it could provide the bases to come up with security designs for complex CPS that optimize operational KPIs while still reliably ensuring the targeted level of security.

REFERENCES

[1] 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 January, 2023]

[2] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99), available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx [retrieved January, 2023]

[3] European Commission, "Proposal for a directive of the European parliament and of the council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", COM(2020) 823 final. 2020/0359(COD), Dec. 2020, [Online]. Available from https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=COM:2020: \ 823:FIN [retrieved January, 2023]

[4] R. Falk and S. Fries, “System Integrity Monitoring for Industrial Cyber Physical Systems”, International Journal On Advances in Security, volume 11, numbers 1&2, pp. 170-179, 2018, [Online]. Available from https://www.thinkmind.org/index.php?view=article&articleid=sec_v11_n12_2018_14 [retrieved January, 2023]

[5] R. Falk and S. Fries, “Enhancing the Resilience of Cyber-Physical Systems by Protecting the Physical-World Interface”, International Journal On Advances in Security, volume 13, numbers 1 and 2, pp. 54-65, 2020, [Online]. Available from: http://www.thinkmind.org/index.php?view=article&articleid=sec_v13_n12_2020_5 [retrieved January, 2023]

[6] 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 January, 2023]

[7] ISO/IEC TS 5723:2022 “Trustworthiness – vocabulary”, July 2022. Available from: https://www.iso.org/standard/81608.html [retrieved January, 2023]

[8] N. G. Mohammadi, “Trustworthy cyber-physical systems: a systematic framework towards design and evaluation of trust and trustworthiness”, Springer, January 2019.

[9] Y. Jiang, “Vulnerability analysis of critical infrastructures”, PhD thesis, University of Skövde, 2022, [Online]. Available from: https://www.researchgate.net/profile/Yuning-Jiang-7/publication/363174252_PhD_Thesis_-_Vulnerability_Analysis_for_Critical_Infrastructures/links/631467bd61e4553b9564e7ff/PhD-Thesis-Vulnerability-Analysis-for-Critical-Infrastructures.pdf [retrieved January, 2023]

[10] B. Northern, T. Burks, M. Hatcher, M. Rogers, and D. Ulybyshev, “VERCASM-CPS: vulnerability analysis and cyber risk assessment for cyber-physical systems”, Information 2021, 12(10), 408, MDPI, 2021 [Online]. Available from: https://www.mdpi.com/2078-2489/12/10/408 [retrieved January, 2023]

[11] A. A. Malik and D. K. Tosh, “Dynamic risk assessment and analysis framework for large-scale cyber-physical systems”, SESA 22(30):1, EAI, 2022, [Online]. Available from: https://eudl.eu/doi/10.4108/eai.25-1-2022.172997 [retrieved January, 2023]

[12] M. Tapia, P. Thier, and S. Gößling-Reisemann, “Vulnerability and resilience of cyberphysical power systems – results from an empirical-based study”, artex paper 222, Univ. of Bremen, April 2020, [Online]. Available from: https://www.uni-bremen.de/fileadmin/user_upload/sites/artec/Publikationen/artec_Paper/222_paper.pdf [retrieved January, 2023]

[13] A. Akbarzadeh and S. K. Katsikas, “Dependency-based security risk assessment for cyber-physical systems”, International Journal of Information Security, Springer, August 2022, [Online]. Available from: https://link.springer.com/article/10.1007/s10207-022-00608-4 [retrieved January, 2023]

[14] Trusted Computing Group, “Cyber resilient module and building block requirements”, Version 1.0 Revision 0.2, June 2022, [Online]. Available from: https://trustedcomputinggroup.org/resource/cyber-resilient-module-and-building-block-requirements/ [retrieved January, 2023]

[15] A. R. Regenscheid, "Platform firmware resiliency guidelines", SP800-193, NIST, May 2018, [Online]. Available from: https://www.nist.gov/publications/platform-firmware-resiliency-guidelines [retrieved January, 2023]

[16] M. Segovia, J. Rubio-Hernan, A. R. Cavalli, and J. Garcia-Alfaro, "Cyber-resilience evaluation of cyber-physical systems," 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), 2020, pp. 1-8. Available from https://ieeexplore.ieee.org/document/9306741 [retrieved January, 2023]

[17] A. Khazraei. S. Hallyburton, Q. Gao, Y. Wang, and M. Pajic, "Learning-based vulnerability analysis of cyber-physical systems", ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS), 2022. Available from: https://cpsl.pratt.duke.edu/sites/cpsl.pratt.duke.edu/files/docs/khazraei_iccps22.pdf [retrieved January, 2023]

[18] P. England, R. Aigner, A. Marochko, D. Mattoon, R. Spiger, and S. Thom, “Cyber resilient platforms”, Microsoft Technical Report MSR-TR-2017-40, Sep. 2017, [Online]. Available from: https://www.microsoft.com/en-us/research/publication/cyber-resilient-platforms-overview/ [retrieved January, 2023]

[19] Electronic Communications Resilience&Response Group, “EC-RRG resilience guidelines for providers of critical national telecommunications infrastructure”, version 0.7, March 2008, available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62281/telecoms-ecrrg-resilience-guidelines.pdf [retrieved January, 2023]

[20] ISO/IEC 27001, “Information technology – Security techniques – Information security management systems – Requirements”, October 2013, available from: https://www.iso.org/standard/54534.html [retrieved January, 2023]

[21] 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 January, 2023]

[22] IEC 62443-4.2:2019, “Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components”, Feb. 2019. Available from: https://webstore.iec.ch/publication/34421 [retrieved January, 2023]

[23] EN 303 645, “Cyber Security for Consumer Internet of Things: Baseline Requirements”, ETSI, V2.1.1 (2020-06), June 2020. Available from: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf [retrieved January, 2023]

[24] 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 January, 2023]