System Integrity Monitoring for Industrial Cyber Physical Systems

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

***Abstract*—Cyber physical systems are technical systems that are operated and controlled using information and communication technology. Protecting the integrity of cyber physical systems is a highly important security objective to ensure the correct and reliable operation and to ensure high availability. A comprehensive protection concept of the system integrity involves several axes: the component level ranging from sensors/actuator devices up to control and supervisory systems, planning and configuration management, and the system life cycle. It allows detecting integrity violations on system level reliably by analyzing integrity measurements from a multitude of independent integrity sensors, capturing and analyzing integrity measurements of the physical world, on the field level, and of control and supervisory systems. Trusted sensors can be used as add-on in existing industrial automation and control systems to allow for cross-checking with sensor measurements of the control system.**

Keywords–system integrity, device integrity; cyber physical systems; Internet of Things, embedded security; cyber security.

I. INTRODUCTION

With ubiquitous machine-oriented communication, e.g., the Internet of Things and interconnected cyber physical systems (CPS), the integrity of technical systems is becoming an increasingly important security objective. This paper is an extended version of [1] that describes an approach for enhanced integrity monitoring of industrial automation and control systems.

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) [2]. 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 communication is addressed, but where integrity shall be ensured at the system level of interconnected devices. This purpose is in particular challenging for dynamically changing cyber physical systems, that come with the Industrial Internet of Things (IIoT) and Industrie 4.0. Cyber systems will become more open and dynamic to support flexible production down to lot size 1 (plug-and-work reconfiguration of manufacturing equipment), and flexible adaptation to changing needs (market demand, individualized products).

The flexibility starts on the device level, where smart devices allow for upgrading and enhancing device functionality by downloadable apps. But 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. 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 robots network. These tools may be connected only temporarily.

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.

This paper describes an integrated, holistic approach for ensuring CPS integrity. After summarizing system security requirements coming from relevant industrial security standard IEC 62443 [2] in Section II, an overview for protecting device integrity and system integrity is described in Sections III and IV. The presented approach for integrity monitoring is 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, see Section V. Using one-way gateways to extract integrity monitoring information from closed control networks, while ensuring freedom from interference, is described in Section VI. A new approach for integrity monitoring of encrypted communications is described in Section VII. An approach for evaluation in an operational security management setting is outlined in Section VIII. Related work is summarized in Section IX, and Section X concludes the paper.

II. SYSTEM INTEGRITY REQUIREMENTS

Protecting industrial automation control systems against intentional attacks is increasingly demanded by operators to ensure a reliable operation, and also by regulation. This section gives an overview on industrial security, and on the main relevant industrial security standard IEC 62443 [2] and integrity security requirements.

A. Industrial Security

Industrial security is called also Operation Technology security (OT Security), to distinguish it from general information technology (IT) security. Industrial systems have not only different security requirements compared to general IT systems, but come also with specific side conditions that prevent that security concepts established in the IT domain can be applied directly in an OT environment. For example, availability and integrity of an automation system have often a higher priority than confidentiality. High availability requirements, different organization processes (e.g., yearly maintenance windows), and required certifications may prevent the immediate installations of updates.

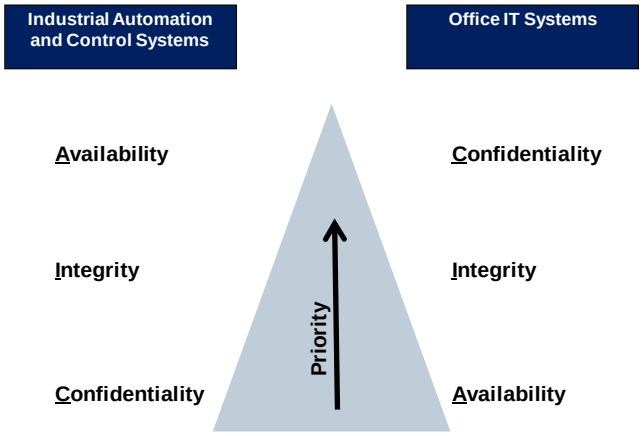

Figure 1. The CIA Pyramid [3]

The three basic security requirements are confidentiality, integrity, and availability. They are also named "CIA" requirements. Figure 1 shows that in common IT systems, the priority is "CIA". However, in automation systems or industrial IT, the priorities are commonly just the other way round: Availability has typically the highest priority, followed by integrity. Confidentiality is often no strong requirement for control communication, but may be needed to protect critical business know-how. Shown graphically, the CIA pyramid is inverted (turned upside down) in many automation systems.

Specific requirements and side conditions of industrial automation systems like high availability, planned configuration (engineering info), long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements have to be considered when designing a security solution. The security requirements, for instance defined in IEC 62443, can be mapped to different automation domains, including energy automation, railway automation, building automation, process automation.

Defined security measures range from security processes, personal and physical security, device security, network security, and application security. No single security technology alone is adequate, but a combination of security measures addressing prevention, detection, and reaction to incidents is required ("defence in depth").

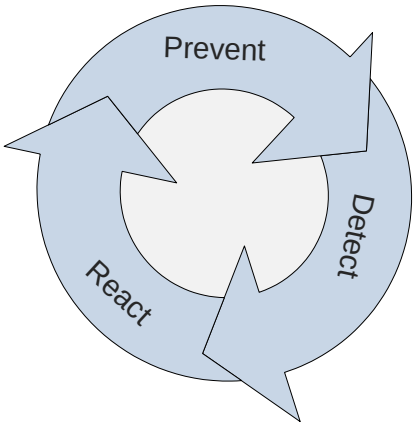

Figure 2. Prevent Detect React Cycle

Also, overall security has to address the areas prevent, detect, and react, see Figure 2. It is not sufficient to only define measures to protect against attacks. The capability has also foreseen to detect attacks, and to define measures to react adequately once an attack has been detected.

B. Overview IEC 62443 Industrial Security Standard

The international industrial security standard IEC 62443 [2] is a security requirements framework defined by the International Electrotechnical Commission (IEC). It is applied successfully in different automation domains, including factory and process automation, railway automation, energy automation, and building automation.. The standard specifies security for industrial automation and control systems (IACS) and covers both, organizational and technical aspects of security. Specifically addressed 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 27002. 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 industrial automation and control systems. In the set of corresponding documents, security requirements are defined, which target the solution operator and the integrator but also the product manufacturer.

As shown in Figure 3, different parts of the standard are grouped into four clusters covering

- common definitions and metrics;
- requirements on setup of a security organization (ISMS related, comparable to ISO 27001 [4]), 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.

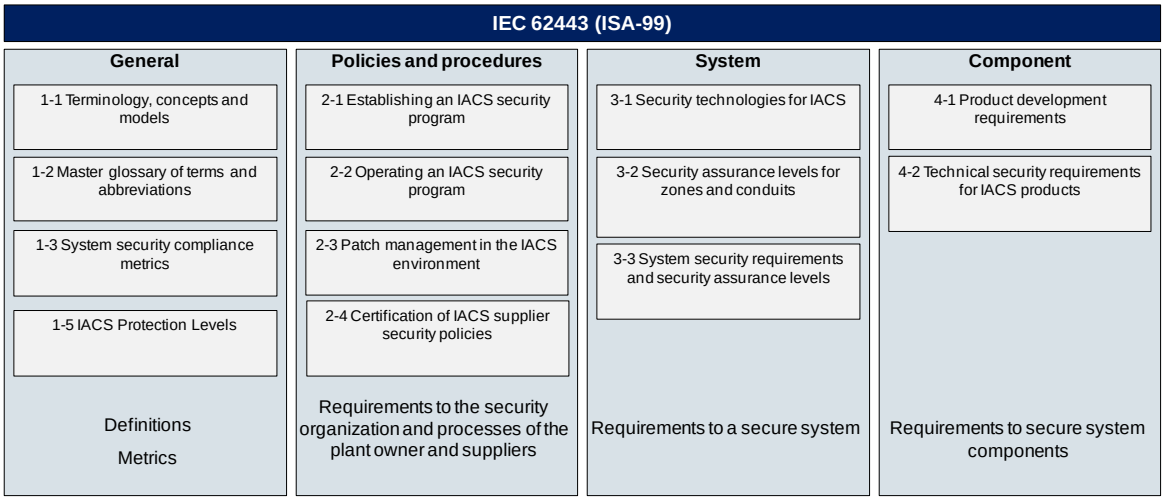

Figure 3. IEC 62443 Industrial Security Standard – Overview

Figure 4 below gives an overview on which parts of IEC 62443 are relevant for the different roles. The operator of an automation system operates the automation and control system that has been integrated by the system integrator, using components of product suppliers.

According to the methodology described in IEC 62443-3-2, a complex automation system is structured into zones that are connected by and communicate through so-called "conduits" that map for example to the logical network protocol communication between two zones. Moreover, this document defines Security Levels (SL) that correlate with the strength of a potential adversary as shown in Figure 5 below. To reach a dedicated SL, the defined requirements have to be fulfilled. IEC 62443 part 3.3 defines system security requirements. It does help to focus only on certain facets of security. The security requirements defined by IEC 62443 part 3.3 help to ensure that all relevant aspects are addressed.

Part 3-3 of IEC 62443 [5] defines seven foundational requirements group specific requirements of a certain category:

– FR 1 Identification and authentication control
– FR 2 Use control
– FR 3 System integrity
– FR 4 Data confidentiality
– FR 5 Restricted data flow
– FR 6 Timely response to events
– FR 7 Resource availability

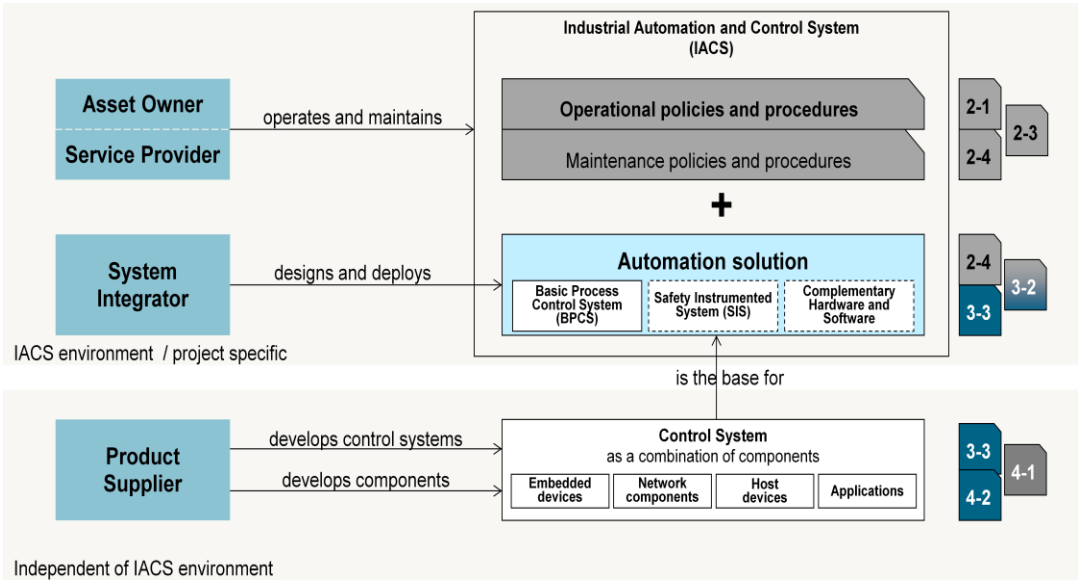

Figure 4. Application of IEC 62443 parts by different roles

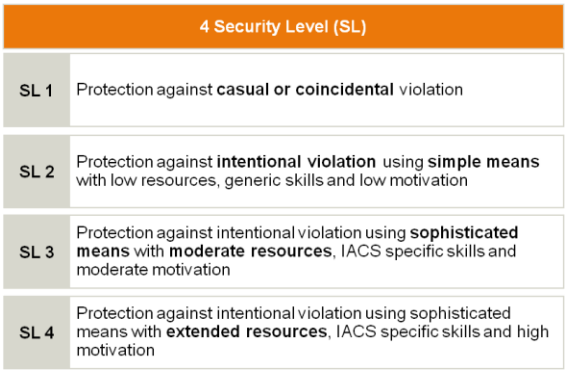

Figure 5. IEC 62443 defined Security Level

For each of the foundational requirements there exist several concrete technical security requirements (SR) and requirement enhancements (RE) to address a specific security level. In the context of communication security, these security levels are specifically interesting for the conduits connecting different zones.

Four Security Levels (SL1, SL2, SL3, SL4) are defined that correlate with the strength of a potential adversary as shown in Figure 5. To reach a dedicated security level, the requirements (SR) and potential requirement enhancements (RE) defined for that security level have to be fulfilled. The standard foresees that a security requirement can be addressed either directly, or by a compensating countermeasure. The concept of compensating countermeasures allows to reach a certain security level even if some requirements cannot be implemented directly, e.g., as some components do not support the required technical features. This approach is in particular important for existing industrial automation and control systems, so called "brown-field installations", as existing equipment can be continued to be used.

The security level of a zone or a conduit (a conduit connects zones) is more precisely a security level vector with seven elements. The elements of the vector designate the security level for each foundational requirement. This allows defining the security level specific for each foundational requirement. If, e.g., confidentiality is no security objective within a zone, the security level element corresponding to FR4 "Data confidentiality" can be defined to be SL1 or even none, although SL3 may be required for other foundational requirements (e.g., for FR1, FR2, and FR3). So, the resulting security level vector for a zone could be SL=(3,3,3,1,2,1,3) or SL=(2,2,2,0,1,1,0).

Different types of SL vectors are distinguished, depending on the purpose:

– SL-T: A target security level vector is defined by the IACS operator based on his risk assessment, defining which security level shall be achieved by each zone and conduit.

– SL-A: The achieved security level vector designates the current status, i.e., the security level that is actually achieved by each zone and conduit. In particular for brown-field installations, it is common that a targeted security level cannot be set-up immediately. The gap between the targeted and the actually achieved security level can be made transparent.

– SL-C: The security level capability describes the reachable security level a component is capable of, if properly configured, without additional compensating counter measures employed. This also means that depending on the SL-T not all security features of a component may be used in certain installations.

C. IEC 62443 Integrity Requirements

One of the seven foundational security requirements defined in Part 3-3 of IEC 62443 [5], targets specifically integrity. Integrity requirements cover in particular the following areas:

– Overall system integrity

– Communication integrity

– Device integrity

The following examples from IEC 62443-3-3 [5] illustrate some of the integrity-related requirements:

– FR3, SR3.1 Communication integrity: "The control system shall provide the capability to protect the integrity of transmitted information".

– FR3, SR3.4 Software and information integrity: "The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest."

– FR3, SR3.8 Session integrity: "The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs."

– FR5, SR 5.2 Zone boundary protection: "The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk -based zones and conduits model."

Corresponding to the system requirements defined in IEC 62443-3-3, also security requirements are defined for individual components (devices). These requirements are defined by IEC 62443 part 4-2 [6] that is currently specified. Different types of components are distinguished, which are "software application", "embedded device", "host device", and "network device".

D. Practical Application of IEC 62443

The standard IEC 62443 has been applied successfully by operators, integrators, and manufacturers in various projects. It is common that documentation and technical designs of real-world deployments are not made public or shared with competitors. However, some examples for applying IEC 62443 are available publicly:

A publication of applying the IEC 62443 standard to the Ukrainian power plant gives some insight concerning how the standard can be applied in a concrete setting [7]. In particular, it shows that a sound, comprehensive security concept is needed that covers security requirements broadly and at a consistent level. The German industrial association "Zentralverband Elektrotechnik- und Elektronikindustrie e.V." (ZVEI) published an overview document on IEC 62443 that includes a simple example, showing the application to a simplified automation system [8].

For the integration of decentralized energy resources into the digital grid, the standard IEC 62351-12 [9] maps the security solution specified for decentralized energy resources to the security requirements in IEC 62443-3-3, arguing that the security requirements are addressed comprehensively.

III. PROTECTING DEVICE INTEGRITY

The objective of device integrity is to ensure that a (single) device is not manipulated in an unauthorized way. This includes the integrity of the device firmware, of the device configuration, but also the physical integrity. Main technologies to protect device integrity are (see Figure 6):

- 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) [10][11]. The configuration information can be used to grant access to keys, or it can be attested towards thirds 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 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 MAC systems like SELinux [12], AppArmor [13], or SMACK [14], can be used to isolate different classes of software (security domains). An attack or malfunction 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 functionality of some devices can be extended by extensions (App). Here, the device integrity has to cover also the App runtime environment: Only authorized, approved apps can be downloaded and installed. Apps are isolated during execution (managed runtime environment, hypervisor, and container). Host-based intrusion detection systems (HIDS) as, e.g., OSSEC [15] can be used for runtime integrity checks on devices, detecting unauthorized changes to the file system.

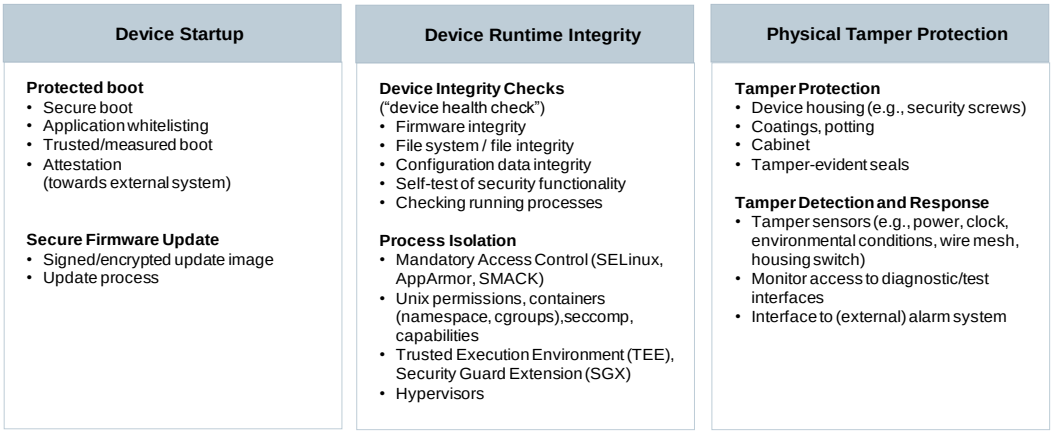

Figure 6. Device Integrity Security Technologies

The known approaches to protect device integrity focus on the IT-related functionality of a device (with the exception of tamper protection). Also, a strong tamper protection is not common on device level. The main protection objective for device integrity shall 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 the each control device, sensor, and actuator would not be economically feasible. Therefore, protecting device integrity alone would be too limited to achieve the goal of protection the integrity of an overall CPS.

IV. System Integrity Monitoring

The next level of integrity is on the system level comprising a set of interconnected devices. The main approaches to protect system integrity are collecting and analyzing information on system level:

- 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 [16], SNMP [17], or syslog protocol [18], to a centralized logging system.
- Runtime device integrity measurements: A device integrity agent provides information gathered during the operation of the device. It collects integrity information on the device and provides it for further analysis. Basic integrity information are 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 trusted sensors.
- 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 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 counter-measures 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.

A. System Overview

Agents on the system components acting as integrity sensors collect integrity information and optionally determine an integrity attestation of the collected information. To allow for flexibility in CPS, the approach puts more focus on monitoring integrity and acting when integrity violations are detected, than on preventing any change that has not been pre-approved by a static policy.

The approach is based on integrity sensors that provide integrity related measurements. 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).

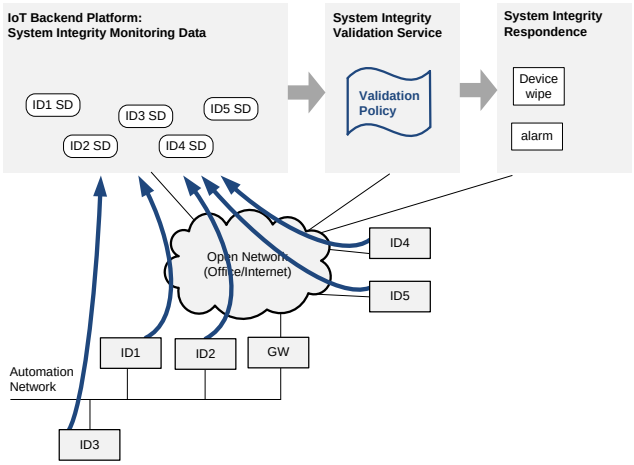

Figure 7. Validation of Device Monitoring Data

Figure 7 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 itself, 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 dash board. 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.

B. Integrity Sensors

The integrity monitoring framework foresees to include a variety of integrity measurements. Depending on the specific application scenario, meaningful integrity sensors can be deployed. Depending on the evolving needs, additional sensors can be deployed as needed.

- Physical world (technical process)
- Physical world (alarm systems, access control systems, physical security as, e.g., video surveillance)
- Device world (malware, device configuration, firmware integrity)
- IT-based control systems (local, cloud services, edge cloud)
- Infrastructure (communication networks)

Flexible extension with additional integrity sensors (even very sophisticated as, e.g., monitoring power fingerprint). The described approach is open to develop and realize sophisticated integrity measurement sensors. So the solution is design to allow evolution and innovation. Integrity sensors have to be protected against attacks so that they provide integrity measurements reliably.

C. Integrity Verification

The integrity monitoring events are analyzed using known data analysis tools. The system integrity can be monitored both online. 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).

As integrity measurements are collected from a multitude of integrity sensors, integrity attacks can be detected reliably. Even if some integrity sensors should be disabled or manipulated to provide malicious integrity measurements, still other integrity sensors can provide integrity information that allows detecting the integrity violation. Checking integrity using measurements from independent integrity sensors and on different levels (physical level, field devices, control and supervisory systems) allows detecting integrity violations by checking for inconsistencies between independent integrity measurements.

V. Trusted Physical Integrity Sensor

A specific approach described in Section IV is the cross-checking of regular sensor measurements used by the industrial automation and control system with independently obtained sensor measurements that are provided by a trusted sensor node. Trusted sensor nodes can be added as add-on security sensors to existing industrial and automation control systems, providing an additional layer of integrity protection. Those trusted sensors and the corresponding analysis algorithms can be updated flexibly and independently from the actual industrial automation and control system. The specific security measures protecting trusted sensors do not interfere with real-time communication requirements or regulatory certification requirements of the actual automation system.

Trusted sensors are used in specific applications as in smart metering to obtain trustworthy information on consumed energy, or for digital tachographs to obtain trustworthy information on driving time and speed for trucks. However, such security-oriented solutions are quite complex, so that it is not realistic to assume that such solutions replace all sensors (and actuators) in industrial automation and control system. Therefore, the intention is to augment existing automation and control system solutions with specific additional trusted sensors. Such trusted sensors can feature specific security measures to provide trusted, integrity protected sensor measurements for consistency and plausibility checking:

- Physical protection (tamper protection): Trusted sensor nodes can be realized with tamper protected housing, and special tamper protected security controllers. Additional tamper sensors integrated with the trusted sensor can detect when the trusted sensor is relocated from his mounting point.
- Cryptographically protected communication: The communication can be protected using common cryptographic protocols, e.g., the Internet security protocol (IPsec) [19] or the transport layer security (TLS) [20] protocol.
- Source authentication: The trusted sensor node can authenticate to other parts of the system to vouch for its credibility.

VI. Freedom of Interference

When integrating trusted sensors in a real-time critical or safety-critical industrial automation and control system, it has to be ensured reliably that the trusted sensors cannot interfere with the control operations. This can be achieved by separating the control network and the integrity monitoring network physically, or at least logically using virtual networks.

However, integrity monitoring information has to be provided also from closed, isolated control networks. Actually, the most critical control systems are often realized

in isolated networks. Actually, IEC 62443 system security requirement SR5.1(3) requires for security level SL4 to both logically and physically separate critical control networks. A physical isolation goes beyond a physical segmentation of control networks that is already required for security level SL2.

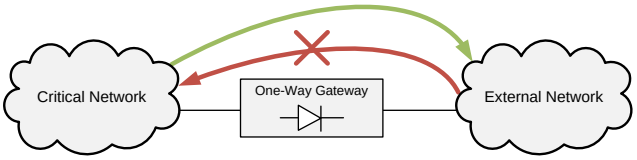

Figure 8. Unidirectional One-Way Gateway

Freedom of interference for network communication can be realized using special one-way gateways [21], as depicted in Figure 8. A one-way gateway ensures that a data communication can take place only in one direction, in particular from a critical control network to an external network. It is not possible to influence or even modify the control communication within the critical control network from the external network, as required by safety authorities and regulator. A data capturing unit (DCU) provides for passive, unidirectional data capture with no interference to the monitored network.

VII. Integrity Monitoring of Encrypted Communications

A specific part of monitoring the system integrity is the network communication. However, network communication is encrypted more-and-more, e.g., using the Transport Layer Security (TLS) protocol [20]. In contrast to earlier versions of the TLS protocol, the most recent version TLS1.3 [22], currently under development, supports only cipher-suites realizing authenticated encryption. Both confidentiality and integrity/authenticity of user communication is protected. No cipher suite providing integrity-only protection is supported by TLS version 1.3, anymore. So, only basic IP header data can be analyzed. This is not sufficient for integrity monitoring of TLS-protected industrial control communication.

A protocol specific solution to enable monitoring of encrypted communication channels by trusted middleboxes is provided by mcTLS [23]. With mcTLS, trusted middleboxes can be incorporated into a secure sessions established between a TLS Client and a TLS Server. Figure 9 shows the basic principle of mcTLS. A TLS authentication and key agreement is performed between a TLS client and a TLS server. As part of the handshake, the TLS client indicates those TLS middleboxes that shall be incorporated within the TLS session. As part of the authentication and key agreement between client and server the middleboxes are incorporated into the message exchange to also possess the (encrypted) key material of the established TLS session using the extension mechanism of TLS.

The basic approach is to perform an enhanced handshake involving middleboxes into the handshake phase of TLS, see Figure 9.

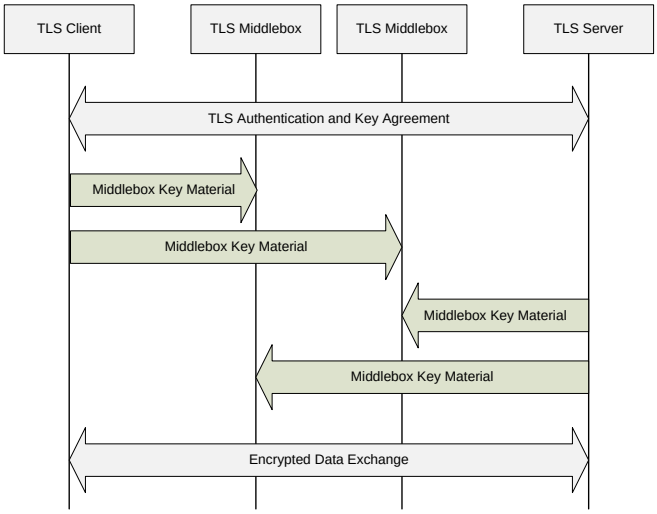

Figure 9. Multi-Context TLS

Specifically, middleboxes are authenticated during the handshake and thus known to both communicating ends. Moreover, each side is involved in the generation of the session key, which is also provided to the middlebox. There is also additional keying performed for the exchange of pure end-to-end keys. Specific key material known to the middlebox is used to decrypt the traffic and check the integrity. The end-to-end based keys are used to protect integrity end-to-end. The latter approach ensures that the middlebox can only read and analyze the content of the communication in the TLS record layer, but any change done by the middlebox is detected by an invalid end-to-end integrity check value. This approach has the advantage that it provides an option to check the associated security policy during the session setup and at the same time monitor traffic as an authorized component. The drawback is that the solution focuses solely on TLS and cannot be applied to other protocols without changes.

The TLS-variant mcTLS allows middleboxes to analyze the TLS-protected communication, e.g., to detect potential security breaches This approach enables communication checking the contents of the communication session without breaking end-to-end security. Hence, with mcTLS, the contents of encrypted data communication, in particular of industrial control communication, can be checked.

Note that mcTLS is only one potential solution for allowing monitoring of encrypted communication. There are further approaches currently being discussed in different standardization groups. Hence, mcTLS is used here just as example as it provides for authenticated and authorized middleboxes, visible and known to the communicating entities.

VIII. EVALUATION

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 threat and risk analysis. 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 of 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 component, in form of a trusted sensor, integrated into the overall system security architecture that is used to provide additional (secure) measurements to reduce the risk of integrity violations. Compared to existing solutions covering IT-related aspects only, the integrity of the control application and the physical world are interconnected. The solution approach does not intend to have a single technology, but it realizes a system-oriented approach that can evolve as part of the security management life cycle covering prevent, detect, and response, as shown in Figure 2.

Applicability to industrial automation environments of the proposed approach allows for:

- Updatability: integrity monitoring system can be updated independently from control system
- Add-on to existing automation systems (brownfield)
- Freedom of interference (do not invalidate reliable operation or certifications)

IX. RELATED WORK

A security operation center (SOC) is a centralized unit for detecting and handling security incidents. Main functionalities are continued security monitoring reporting, and post-incident analysis [24][25]. Security incident and Event management (SIEM) systems can be used within a SOC to analyze security monitoring data. Compliance management systems support a centralized reporting of server configuration in data centers.

Host-based intrusion detection systems (HIDS) as SAMHAIN [26] and OSSEC [15] analyze the integrity of hosts and report the results to a backend security monitoring system. Network based intrusion detection systems (NIDS) capture the network traffic, e.g., using a network tap or a mirroring port of a network switch, and analyze the traffic. Examples are SNORT [27] and Suricata [28].

Two main strategies can be followed by an intrusion detection system (IDS): Known malicious activities can be looked for (signature based detection), or any change compared to a learned reference network policy is detected (anomaly detection). They can be applied also in industrial automation and control networks. Premaratne, Samarabandu, Sidhu et al. simulated attacks on an energy automation substation and developed an IDS to detect these attacks [29]. The risk of an attack on the energy distribution system of is determined based on the current power consumption. Fovine, Carcano, et al. have proposed a state-based IDS that monitors the cyber-physical state evolution of a supervisory control and data acquisition (SCADA) system [30].

An "automotive thin profile" of the Trusted Platform Module TPM 2.0 has been specified [31]. A vehicle is composed of multiple control units that are equipped with TPMs. A rich TPM manages a set of thin TPMs, so that the vehicle can be represented by a vehicle TPM to the external world. Technical solutions for protecting against tampering of smart meters are described in [32].

Approaches to utilize the context information on the CPS operation, device capabilities, device context to enhance the authentication of a single device, have been described by the authors of this paper in previous work [33]. The effect of an integrity attack on the degradation of a control system has been investigated by Mo and Sinopoli [34].

X. CONCLUSION

Ensuring system integrity is an essential security feature for cyber physical systems and the Internet of Things. The security design principle of "defense in depth" basically means that multiple layers of defenses are defined. This design principle can not only be applied at the system level, but also at the level of a single security mechanism.

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 / Industrie 4.0, the focus of system integrity 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. This paper focused on integrity of devices, communication, and cyber systems. The addition of trusted physical sensors allows for cross-checking trusted measurements with the state of the industrial automation and control system. One-way data gateways can be used to provide integrity monitoring information from closed control networks to external networks for evaluation. Furthermore, approaches for integrity monitoring of encrypted communications have been presented.

The approaches for integrity monitoring in industrial automation and control systems described in this paper focus on the operation phase. Nevertheless, 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.

REFERENCES

[1] R. Falk, S. Fries, "Enhancing Integrity Protection for Industrial Cyber Physical Systems", The Second International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2017, November 12 - 16, 2017, Barcelona, Spain, available from: http://www.thinkmind.org/index.php?view=article&articleid=cyber_2017_3_30_80031 2018.01.23

[2] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99), available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx 2018.01.23

[3] R. Falk, S. Fries, "Advanced Device Authentication for the Industrial Internet of Things", International Journal on Advances in Internet Technology, vol. 10, no 1&2, pp. 46-56, 2017, available from: http://www.iariajournals.org/internet_technology/inttech_v10_n12_2017_paged.pdf 2018.05.15

[4] ISO/IEC 27001, "Information technology – Security techniques – Information security management systems – Requirements", October 2013, available from: https://www.iso.org/standard/54534.html 2018.01.23

[5] 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

[6] IEC 62554-4.2, "Industrial communication networks - Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components", CDV:2017-05, May 2017

[7] Patrice Bock, Jean-Pierre Hauet, Romain Françoise, and Robert Foley: "Ukrainian power grids cyberattack - A forensic analysis based on ISA/IEC 62443", ISA InTech magazine, 2017, https://www.isa.org/templates/news-detail.aspx?id=152995 2018.01.23

[8] ZVEI: "Orientierungsleitfaden für Hersteller zur IEC 62443" [German], ZVEI Whitepaper, 2017, https://www.zvei.org/presse-medien/publikationen/orientierungsleitfaden-fuer-hersteller-zur-iec-62443/ 2018.01.23

[9] IEC 62351-12, Power systems management and associated information exchange - Data and communications security - Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems, https://webstore.iec.ch/ 2018.01.23

[10] Trusted Computing Group: "TPM Main Specification", Version 1.2, , available from http://www.trustedcomputinggroup.org/resources/tpm_main_specification 2018.01.23

[11] Trusted Computing Group, "Trusted Platform Module Library Specification, Family 2.0", 2014, available from http://www.trustedcomputinggroup.org/resources/tpm_library_specification 2018.01.23

[12] SELinux, "Security Enhanced Linux", available from: https://selinuxproject.org/page/Main_Page 2018.01.23

[13] AppArmor, "AppArmor Security Project", available from: http://wiki.apparmor.net/index.php/Main_Page 2018.01.23

[14] SMACK, "Simplified Mandatory Access Control Kernel", available from: https://www.kernel.org/doc/html/latest/admin-guide/LSM/Smack.html 2018.01.23

[15] OSSEC, "Open Source HIDS SECurity", web site, 2010 - 2015, available from http://ossec.github.io/ 2018.01.23

[16] OPC Foundation, "OPC Unified Architecture (UA)", available from: https://opcfoundation.org/about/opc-technologies/opc-ua/ 2018.01.23

[17] J. Case, R. Mundy, et al., "Introduction and Applicability Statements for Internet Standard Management Framework", RFC3410, available from: https://tools.ietf.org/html/rfc3410 2018.01.23

[18] R. Gerhards, "The Syslog Protocol", RFC5424, March 2009, available from: https://tools.ietf.org/html/rfc5424 2018.01.23

[19] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", RFC4301, December 2005, acailable from https://tools.ietf.org/html/rfc4301 2018.01.23

[20] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, Aug. 2008, available from http://tools.ietf.org/html/rfc5246 2018.01.23

[21] Siemens: "Enhancing the first line of defense - Uni-directional communication to enable a connected world, whitepaper, December 2017, available from https://www.siemens.com/dcu 2018.01.23

[22] E. Rescorla: "The Transport Layer Security (TLS) Protocol Version 1.3", Internet draft (work in progres), September 2017, available from: https://tlswg.github.io/tls13-spec/draft-ietf-tls-tls13.html 2018.01.23

[23] D. Naylor, K. Schomp, et al., "Multi-Context TLS (mcTLS), Enabling Secure In-Network Functionality in TLS," available from http://mctls.org/ 2018.01.23

[24] B. Rothke, "Building a Security Operations Center (SoC)", RSA Conference, 2012, available from https://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf 2018.01.23

[25] McAffee Foundstone® Professional Services, "Creating and Maintaining a SoC", Intel Security Whitepaper, available from: https://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf 2018.01.23

[26] R. Wichmann, "The Samhain HIDS", fact sheet, 2011, available from http://la-samhna.de/samhain/samhain_leaf.pdf 2018.01.23

[27] "SNORT", web site, available from https://www.snort.org/ 2018.01.23

[28] "Suricata", web site, available from https://suricata-ids.org/ 2018.01.23

[29] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, et al., "An Intrusion Detection System for IEC61850 Automated Substations", IEEE Transactions on Power Delivery, Volume: 25, Issue 4, pp. 2376-2383, Oct. 2010

[30] I.N. Fovino, A. Carcano, T. De Lacheze Murel, A. Trombetta, et al., "IDS Modbus/DNP3 State-based Intrusion Detection System", 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2010, IEEE

[31] Trusted Computing Group, "TCG TPM 2.0 Automotive Thin Profile", level 00, version 1.0, 2015, available from http://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin 2018.01.23

[32] Texas Instruments: Anti-tamper Techniques to Thwart Attacks on Smart Meters, TI Training, 2018, available from https://training.ti.com/node/1128354 2018.01.23

[33] R. Falk and S. Fries, "Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things", The First International Conference on Advances in Cyber-Technologies and Cyber-Systems, CYBER 2016, October 9 - 13, 2016 - Venice, Italy , available from http://www.thinkmind.org/index.php?view=article&articleid=cyber_2016_4_20_80029 2018.01.23

[34] Y. Mo and B. Sinopoli, "On the Performance Degradation of Cyber-Physical Systems Under Stealthy Integrity Attacks", IEEE Transactions on Automatic Control 61.9 (2016): 2618-2624.