Security Safety and Organizational Standard Compliance in Cyber Physical Systems

Ani Bicaku, Christoph Schmittner, Patrick Rottmann, Markus Tauber and Jerker Delsing

***Abstract*—In Industry 4.0 independent entities should inter-operate to allow flexible and customized production. To assure the parties that individual components are secured to inter-operate, we investigate automated standard compliance. The standard compliance is defined based on given sets of security and safety requirements for which measurable indicator points are derived. Those reflect configurations of systems recommended by security, safety or process management relevant standards and guidelines, which help to demonstrate the state of compliance. We propose in this paper an approach to automate such an assessment when components are inter-operating with each other by using a monitoring and standard compliance verification framework. The framework will assure the parties that services or devices within their organizations operate in a secure and standard compliant way, without compromising the underlying infrastructure.**

***Index Terms*—Security, safety, organizational, standard, compliance, monitoring, Cyber Physical Systems.**

I. INTRODUCTION

THE increasing demand for flexible and customized production brings new challenges to the existing manufacturing systems. To address these challenges, lots of research has been conducted to pave the way for the fourth industrial revolution, known as Industry 4.0, which aims to optimize production by sharing physical and cyber resources [1]. This may also include inter-operation between individual companies or legal entities within large enterprises. Existing technologies, such as Internet of Things, System of Systems, Cyber Physical Systems, cloud computing and Service Oriented Architectures, allow for such inter-operation already [2]. Nevertheless, it is important for entities to assure that the components inter-operate in a safe and secure manner and prove it at any point of time.

In the industrial environments, the fulfilment of security, and safety requirements of devices autonomously communicating with each other plays a fundamental role. Consequences of security incidents in different areas or dimensions, can be for example interruption or modification of an operational process, or even sabotage with intention to cause harm. Manipulating or interrupting such systems could also affect safety, which can have consequences such as environmental damage, injury or loss of life [3]. To allow interoperability, flexibility and customized production from the industrial devices to the backend infrastructure and to prevent failures during business process execution, organizational aspects should be in place. According to Gaitanides et al., [4] the main goal of process management is customer satisfaction. To achieve this the quality products and services must be improved, cycle time must be reduced and cost must be kept as low as possible. A correct configuration of systems is the key to support proper business process execution and audits or compliance checks of system configurations should provide a method to monitor and verify a valid state.

Security, safety and organizational incidents are tolerated more easily if one can show that they occurred despite system compliance with all applicable security regulations. This can be achieved via manual audits, which are often based on existing standards and guidelines.

The new technologies and requirements of Industry 4.0 create a new demand for standardization, which plays a key role in improving security and safety across different regions and communities. In the last years, different standard organizations have been established, mostly initiated from industry, and have published various standards in different fields and topics. Despite the extensive research [5], [6], [7], and a considerable number of widely accepted security, safety, legal and organizational standards, existing approaches are incapable of meeting the requirements imposed by challenges and issues in Industry 4.0.

In order to address the aforementioned concerns, in our previous work [8], we have proposed an initial approach to automatically verify standard compliance by using a monitoring and standard compliance verification framework, as shown in Figure 1. In this paper we extend the framework with MOIs to assure that the system is compliant with organizational standards.

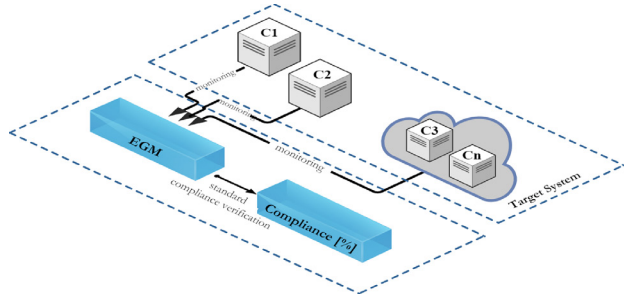

Fig. 1: High level view of standard compliance verification

The monitoring and standard compliance framework, built on our previous work [9], uses an Evidence Gathering Mechanism to collect evidence from a number of components in the target system based on a set of measurable indicator points. The Measurable Indicator Points, categorized in measurable security indicators, measurable safety indicators and measurable organizational indicators, are extracted from existing standards and guidelines to address target system

DOI: 10.36244/ICJ.2019.1.1

specific requirements (e.g. access control systems for the production line should be resistant against side-channel attacks). The information gained from the MIPs is then used by the compliance module to define if the target system is operating in a secure and standard compliant way.

The reminder of the paper is organized as follows. Section II reviews widely used security and safety standards/best practice guidelines and research on monitoring (security, safety and organizational) and compliance. Section III presents the overall architecture of the framework and the standard compliance verification approach. In Section IV an end-to-end communication use case and a representative set of MIPs is provided and we conclude our work in Section V.

II. Related Work

To enable the global usability of the products and systems, standardization in the industrial environment is of utmost importance. The new technologies and requirements of Industry 4.0 create a new demand for standardization, which plays a key role in improving security, safety and organizational aspects across different areas and in different communities. In the last years, several organizations have published various standards in different fields and topics. ENISA [1], ETSI [2], ISO [3] and IEC [4] are some of the most popular standardization bodies.

ISO 27000-series standards [10], also known as ISMS family of standards, deal with a different area of information security including requirements, implementation guidelines and risk management. The standards cover almost all the aspects of technology and business addressing cyber-security, privacy, confidentiality and other aspects of security issues by providing updates on the latest technologies and threats.

ISO/IEC 15408 [11], known as Common Criteria, provides a framework where the security functionality of IT products and the assurance requirements during a security evaluation can be specified. The CC evaluation is divided in three parts. The CC part 1, provides general concepts of IT security and defines the core concept of a TOE. The CC part 2 - Security functional components, includes a catalog of security functional components and categorizes them in a hierarchical order based on families, classes and components. The CC part 3 - Security assurance components, defines the assurance requirements of the TOE expressed in a PP or a ST. It also includes the EAL that defines the scale for measuring assurance for each component of the TOE. Nevertheless, CC has only focused on security evaluation without considering safety or legal aspects.

IoT Security Compliance Framework [12] is an assurance guideline for organizations used to provide structured evidence to demonstrate conformance with best practice guidelines. The compliance scheme in this document is based on risk profiles for different systems and environments including: (i) business processes, (ii) devices and aggregation points, (iii) networking and (iv) cloud and server elements. The compliance process is based on a set of requirements of organizations and products by defining five classes of compliance on a scale from 0 to 4. The compliance process determines also the levels of confidentiality, integrity and availability (C-I-A) for each compliance class. In order to apply the required level of security and to maintain the level of trust for IoT systems, each requirement includes an ID, the compliance class, and the applicability category.

A recent review of the literature on IoT security and trust is conducted in [13]. The authors evaluate relevant existing solutions related to IoT security, privacy and trust. The existing work is analyzed based on topics such as authentication, access control, privacy, policy enforcement, trust, confidentiality and secure middleware. In [13] the main research challenges in IoT security, the most relevant solutions and the questions that arise for future research related to security and trust in IoT are presented. The overview shows that available solutions involve different technologies and standards, but a unified vision for security requirements is still missing.

Julisch [14] introduces the compliance problem by focusing on security requirements. In this paper, security is the state of being safe from threats and the security compliance is the evidence (assurance) that a given set of requirements is met, which can be security requirements or other security mechanisms imposed by standards. He underlines that, in order to narrow the gap between academia and industry, it is necessary to focus more research on the question of security compliance to help organizations to comply with best practices guidelines and standards.

For safety the basic safety standard is IEC 61508 [15] “Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related System”. This standard is developed as a domain independent standard which can be adapted for all domains without a domain-specific standard. The process industry, based on IEC 61508, IEC 61511 [16] developed the ”Functional safety - Safety instrumented systems for the process industry sector”. Such a domain specific instantiation is mainly developed to consider peculiarities from a specific domain. For the industrial sectors both standards are relevant. Compliance to both standards was mostly evaluated during the design time [17], [18]. It was assumed that safety-critical systems are stable and compliance can be completely checked during design time. Due to Industry 4.0 and the goal of increased production flexibility there is an increasing need to check compliance also during run-time. Existing approaches utilize mainly concepts from contract-based development [19]. This assumes that the basic blocks of a safety-critical system will stay the same and are assessed during design-time. Contracts are then used to check the compliance of different system compositions based on pre-checked blocks [20]. While such approaches make it possible to shift a part of the safety assessment towards run-time, there is still the challenge that with flexible and configurable systems components need to be checked if they are still compliant with their respective safety standard.

Standards such as ISO 9001:2015, ISO/IEC/IEEE 15288, ISO 18404, ISO/IEC 29169, ISO IEC TS 33052, etc., are some of the standards considering business process management.

ISO 9001 [21] is an international standard that specifies requirements for a QMS and is used by organizations to

[1] https://www.enisa.europa.eu/topics/standards/standards
[2] https://www.etsi.org/
[3] https://www.iso.org/home.html
[4] https://www.iec.ch/

demonstrate the ability to consistently provide products and services that meet customer and regulatory requirements. Additionally, a process approach is suggested including the PDCA-Cycle and risk based thinking. The PDCA-cycle helps organizations to define processes, execute them, measure the outcome and analyse the results to set actions for further improvement.

ISO 18404 [22] provides tools for organizations to improve the capability of their business processes. This increase in performance and decrease in process variation leads to defect reduction and improvement in profits, employee morale, and quality of products or services. It focuses on clarifying competencies required for personnel and organizations in SixSigma, Lean and "Lean&SixSigma". Moreover, this standard constitutes general requirements from personnel (e.g. Black Belt) or organizations due to the numerous existing combinations of Lean and Six Sigma. Therefore, competencies for individual skill levels are described in details, such as Black Belt, Green Belt, Lean practitioners and their organizations. However, a specification and design for Six Sigma is excluded.

ISO/IEC TS 33052 [23] is used to describe the structure of a process reference model to support information security management. The PRM includes processes, derived from ISO/IEC 27001, which can already exist in the context of a management system of a service provider. This standard is used to deploy and control the execution and performance of operational and organizational processes by supporting the efficient, timely and quality day-to-day operations.

Although the produced guidelines and scientific work help users to address industrial requirements, more standard compliance measurements are needed.

There are various frameworks and platforms supporting monitoring of CPS and IoT. Several approaches and prototypes are presente, both in literature [24], [25], [26] and in the scope of research projects such as Cumulus, NGcert, SECCRIT etc. However, there is no generally accepted method that allows mapping the security, safety and organizational compliance. In this context, the proposed monitoring and standard compliance verification framework advances the state of the art by considering security, safety and organizational related aspects without compromising the underlying infrastructure.

III. Monitoring and Standard Compliance Verification Framework

Standard compliance is the adherence to a given set of security and safety requirements, represented by measurable metrics, on the use and configuration of systems or any other security, safety or legal mechanism. These measurable metrics should be imposed by standardized bodies to make each system, device or application comply with the standards.

To assure that the system is operating in a secure and standard compliant manner a monitoring module is needed, which is responsible for gathering all the required measurements. Thus, in this paper we present a monitoring and standard compliance verification framework, which has been designed to support different use cases and viewpoints that should be considered and researched in Industry 4.0.

The monitoring and standard compliance verification framework, illustrated in Figure 2, makes it possible to gather security, safety and organizational evidence from the target system in a structured way (e.g. MSI, MSFI, MOI). The architecture of the framework has a pluggable and expendable architecture allowing easy adaptation to constantly analyze and monitor the status of the system or components of the system. It is possible to monitor a large number of measurable metrics (as shown in Section IV B-D) for different CPPS components by aggregating, scheduling, storing, retrieving and analyzing the monitoring data to provide standard compliance verification.

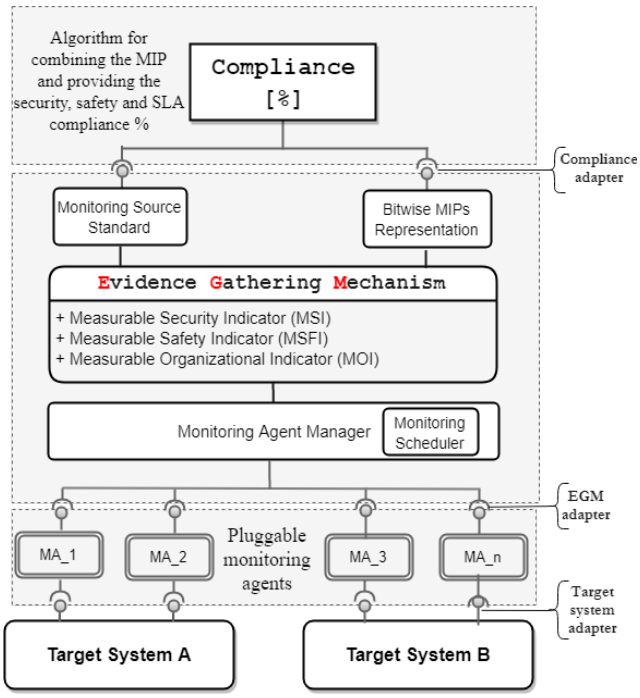

Fig. 2: Monitoring and standard compliance verification framework used to measure, aggregate, schedule, store, retrieve and analyze the monitoring data to provide standard compliance

The monitoring and standard compliance verification framework is composed of four main modules, including Monitoring Agents, Evidence Gathering Mechanism, Compliance and the Target System. The TS represents a system or component of a system that will be monitored by monitoring tool plugins or customized scripts.

A. Monitoring components

1) Monitoring Agents (MA): The MA module is used to gather data from the TS and should allow the integration of different pluggable monitoring agents (MA_i) from different monitoring tool plugins (e.g., Nagios plugin [27], Ceilometer plugin [28], Zabbix plugin [29], etc.) and customized scripts.

2) Evidence Gathering Mechanism (EGM): The EGM module is designed to acquire, store and analyze security, safety and legal related evidence [9]. It manages the incoming data from the monitoring agents and decides when/what data

to send to the Compliance module by using a writing buffer. It makes the mapping of the measurable metrics possible and their values with the standards to provide the necessary information for the compliance module. The EGM module consists of:

a) Monitoring Agent Manager: The Monitoring Agent Manager is the only contact point between the EGM module and the MA_i. It is responsible for organizing the MA_i based on the configurations and uses a Monitoring Scheduler to provide the run-time of each plugin in the corresponding component.

b) Monitoring Source Standard: The Monitoring Source Standard provides for each defined measurable metric the source from which standard/best practice guideline the metric is extracted. By mapping the MIPs to the specific standard, the compliance module can cross-check if the specific metric has been monitored in the target system.

c) Bitwise MIPs Representation: The Bitwise MIPs Representation module represents every MIP by a number, which can be converted to binary and operated on by a computer.

The EGM module gathers the monitoring data in a column structure based on the MIPs (MSI, MSFI, and MOI). For each MIP the following information is provided: (i) metric ID, (ii) value of the metric, which can be a binary value, true/false value, etc and (iii) the source based on the standard/best practice guideline from where the metric is extracted. A representative set of the information provided by the EGM module is shown in Figure 3. The information provided by

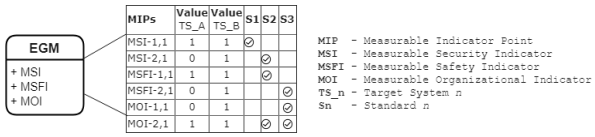

Fig. 3: A representative set of the information provided by the EGM module

the EGM module is used as input for the Compliance module for further analysis.

B. Standard Compliance Verification

In Industry 4.0 large monolithic organisations are moving towards multi-stakeholder cooperations, where cooperation is fostered by market requirements such as sustainable, flexible, efficient, competitive and customized production [1]. Despite the benefits, this brings new challenges in terms of security, safety and organizational related issues. Thus, it is of utmost importance to assure that independent entities inter-operate with each-other in a secure and standard compliant manner, without compromising the underlying infrastructure.

In this paper we present an initial approach for standard compliance verification. The Compliance module is responsible for assuring that the system is operating in a secure and standard compliant manner driven by the input provided by the EGM module. The compliance depends on a set of MIPs, which are extracted from a number of widely used standards and best practice guidelines to address the target system specific requirements. Thus, in order to measure standard compliance one has to consider a set of MIPs and a set of standards, since a dynamic mix of new technologies, regulations and interactions of different organizations are involved. However, it is not easy to extract metrics for security, safety and organizational related issues [30], [31], since the indirect relationship and the dependability between them have to be considered as well. In the following section we present a representative set of MIPs for a specific target system and show how such a metric can be described.

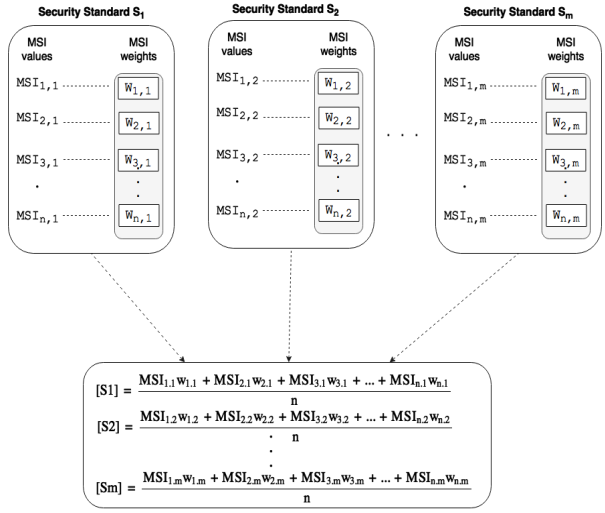

Fig. 4: Security standard compliance verification

To show the standard compliance verification approach, we have considered only MSIs. However, the same approach applies also for MSFIs and MOIs. Each MSI extracted from a standard is monitored using monitoring agents in the corresponding component of the target system. The monitoring data are than gathered by the EGM module, which is responsible for making them readable for the Compliance module. So, the EGM sends to the Compliance module for each MSI the source from which the metric is extracted and a binary value 1 or 0 that indicates if the metric is fulfilled or not. Depending on the specific target system requirements the Compliance module assigns to each MSI a weight value to indicate the importance in the range $[0, 1]$.

After gathering all the required evidence from the EGM module, the Compliance module first verifies the compliance $[\%]$ for a single standard as the ratio between the sum of each MSI measured value multiplied by its weight value and the total number of metrics per standard as shown in equation 1. It verifies the total compliance $[\%]$ as the ratio between the sum of each standard compliance and the total number of selected standards, as shown in equation 2.

$$MSI\_compliance_{(j)}[\%] = \frac{\sum_{i=1}^{n} MSI_{i,j}\omega_{i,j}}{n}100\% \quad (1)$$

$$MSI\_compliance[\%] = \frac{\sum_{j=1}^{m} compliance_{(j)}}{m}100\% \quad (2)$$

where:

n	total number of metrics per standard
m	total number of standards
$MSI_{i,j}$	measured value of "i" security metric from "j" standard
$\omega_{i,j}$	weight value of "i" security metric from the "j" standard

Introduction of Compliance Levels

In order to apply an appropriate level of security and safety standard compliance to a component or system depending on the requirements, four compliance levels [0-3] are arbitrarily defined:

Compliance Level	MIPs		
	MSI	MSFI	MOI
Level 0	basic	basic	basic
Level 1	basic	basic	high
	basic	high	basic
	high	basic	basic
Level 2	basic	high	high
	high	basic	high
	high	high	basic
Level 3	high	high	high

TABLE I: Arbitrary compliance levels based on MIPs

The compliance levels, shown in table I, depend on the standard compliance verification for MSIs, MSFIs and MOIs, whereas *basic* is defined as the compliance in the range $[0\%, 50\%]$ and *high* is defined as the compliance in the range $[50\%, 100\%]$.

- **Compliance Level 0** indicates that the compliance of all three MIP groups is basic
- **Compliance Level 1** indicates that at least the compliance of one MIP group is high
- **Compliance Level 2** indicates that at least the compliance of two MIP groups is high
- **Compliance Level 3** indicates that the compliance of all three MIP groups is high

IV. A REPRESENTATIVE SET OF MIPS FOR THE MONITORING AND STANDARD COMPLIANCE VERIFICATION FRAMEWORK

This section provides illustrative metrics that should be considered in an Industry 4.0 application scenario with the goal to address the requirements of access control systems for the production line. In that regard, the IEC 62443-3-3 (Industrial communication networks - Network and system security - System security requirements and security levels) [32] provides technical control system fundamentals requirements for industrial automation and control system capability, where we have selected three MSIs to show how each MSI is documented and monitored. The IEC 61508-3 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) [33], is the basic safety standard and intended as an umbrella standard by various industries to provide their own standards and guidelines, from which three MSFIs as representative examples are selected.

In contrast with security and safety standards, business management standards do not provide explicit technical measures. However, some standards provide a methodology on how to implement and execute assessments. ISO/IEC TS 33052 (Information Technology – Process reference model (PRM) for information security management) [23] provides process descriptions which relate to process purpose, process context, outcomes and traceable requirements. The traceable requirements give an indication which tasks and actives are relevant for certain processes and they are presented as actions that refer explicitly to ISO/IEC 27001 and relate to common tasks. It provides a process assessment model (PAM) from where we have selected three MOIs as representative examples.

A. Use Case

In order to extract MIPs, which can be used to evaluate the approach described in the previous section, we consider the use case depicted in Figure 5, from an ongoing research project addressing a secure end-to-end communication in CPPS [34].

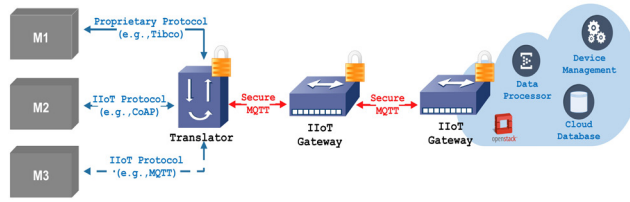

Fig. 5: CPPS end-to-end communication use case

To provide device management as a service, data is transmitted between devices (M1, M2, and M3), processed and sent to a private cloud for further processing and analysis. The communication protocol used between the edge devices, the IIoT components, and the cloud backend is the MQTT protocol, designed to be lightweight, flexible and simple to implement. In the production environment, the new industrial devices are already able to communicate using state of the art IIoT protocols, such as MQTT. However, this is not the case if a legacy device wants to establish a connection with the IIoT gateway. In this case, a translator system is needed to translate the device protocol into MQTT [35]. In such scenario, with different decentralized CPPS components, condition reports to the overall system are important. In order to observe the system behavior, several components can be monitored, including industrial devices, IIoT gateways and cloud services.

Once the requirements have been identified and the standards/best practice guidelines have been examined to see whether or not they address the specific requirement, the next step is to identify measurable indicator points. Based on this

use case and the access control requirements, we define a set of representative MSIs, MSFIs and MOIs extracted from security, safety and process management standards. For each MIP is provided: (i) an ID, (ii) the source and the definition based on the standards and best practice guidelines, (iii) possible monitoring solutions and (iv) a monitoring value are provided.

B. MSIs: Measurable Security Indicators

- **MSI-1.1**: Secure identification and authentication
  - *Source*: IEC 62443-3-3
  - *Definition*: The client and the server identify each other and assure their identities via secure log-on
  - *Monitoring Plugin*: Can be monitored with Nagios monitoring agent, which checks the configuration of the used protocol (or indeed any other client/server authentication method) to make sure that it uses a secure communication protocol.
  - *Monitoring Value*: True/False
- **MSI-2.1** : Strength of password-based authentication
  - *Source*: IEC 62443-3-3
  - *Definition*: The system shall be configurable by providing a degree of complexity such as minimum length, variety of characters and password rotation.
  - *Monitoring Plugin*: Can be implemented by performing checks on the PAM (Pluggable Authentication Module) to verify if a minimum length or complexity of passwords and password rotation is enabled.
  - *Monitoring Value*: True/False
- **MSI-3.1** : Concurrent session control
  - *Source*: IEC 62443-3-3
  - *Definition*: The system shall restrict the maximum number of concurrent sessions per system account or system type.
  - *Monitoring Plugin*: A script can be developed which checks *sshd_config* or *pam_limits* configuration.
  - *Monitoring Value*: True/False

C. MSFIs: Measurable Safety Indicators

- **MSFI-1.2** : Time-triggered architecture
  - *Source*: IEC 61508-3, Table A-2, Group 13
  - *Definition*: : Ensure that the system complies with the safety timing requirements
  - *Monitoring Plugin*: Can be checked via Nagios, send test packet to system and check if response time is inside allowed parameters. If Nagios is running on a separate system this achieves medium diagnostic coverage (based on IEC 61508-2). If the systems sends regular information about logical status high diagnostic coverage is achievable
  - *Monitoring Value*: Response time
- **MSFI-2.2** : Techniques and measures for error detection
  - *Source*: IEC 61508-3, Table A-18
  - *Definition*: Ensure that system modifications are protected against erroneous
  - *Monitoring Plugin*: Check that system modifications require a password
  - *Monitoring Value*: True/False
- **MSFI-3.2** : Control systematic operational failures
  - *Source*: IEC 61508-7
  - *Definition*: Ensure that all inputs via a safety-related system are echoed to the operator before being sent to the system. This should also consider abnormal human actions, e.g. speed of interaction
  - *Monitoring Plugin*: Can be monitored by a network module that checks the system behaviour
  - *Monitoring Value*: True/False

D. MOIs: Measurable Organizational Indicators

- **MOI-1.1**: Event Logging
  - *Source*: ISO/IEC TS 33052
  - *Definition*: The system shall forward event log information to a central security information and event management system
  - *Monitoring Plugin*: Can be monitored with a Nagios plugin checking syslog/event log configuration
  - *Monitoring Value*: True/False
- **MOI-2.1**: Restrictions on software installations
  - *Source*: ISO/IEC TS 33052
  - *Definition*: The system shall restrict software installation to approved products
  - *Monitoring Plugin*: Can be monitored with a custom Nagios plugin checking e.g. paket management (e.g. Linux) or other software management configuration
  - *Monitoring Value*: True/False
- **MOI-3.1** : Access to networks and network services
  - *Source*: ISO/IEC TS 33052
  - *Definition*: The system configuration must support access to mandatory networks and network services
  - *Monitoring Plugin*: : Can be monitored with a custom Nagios plugin checking network device and network service configuration (e.g., DNS, DHCP, Gateway, Netmask, NPS, 802.1x Cert etc.)
  - *Monitoring Value*: True/False

As illustrated in Figure 2, the monitoring agents defined for each MIP, will gather data from the target system (in this case the end-to-end communication use case) and will provide for the EGM the necessary information if the metric is fulfilled or not. The Compliance module maps the monitored metric with the corresponding standard and calculate the compliance [%] based on equation 2. The result will then be used to define the compliance level [0-3] of the system as shown in table I.

V. CONCLUSIONS

In this paper we have presented a monitoring and standard compliance verification framework for Industry 4.0 application scenarios with the aim to provide an automated standard compliance. The standard compliance is defined based on a set of MIPs extracted from existing standards and best practice guidelines. The MIPs are monitored in the target system using monitoring agents and the monitoring data are then used by the EGM to make them readable for the compliance module.

To give an example of how such an approach will work, we have extracted a representative set of MSIs, MSFIs and MOIs motivated by the requirements provided from an ongoing research project use case. We have provided the information on how the MSIs, MSFIs and MOIs can be measured by either existing monitoring tool plugins or customized scripts.

As part of our future work, we will implement and evaluate the monitoring and standard compliance verification framework and we will further analyze other security and safety standards that are relevant to the industrial environment.

Part of this analysis is also to determine other safety metrics that can be measured by the MSCV. Hardware based safety metrics like mean time between failures (MTBF) are difficult to monitor, and normally static. There are approaches to utilize contracts during run time to conduct safety assessment for systems which are composed during run time [36]. Other metrics which are oriented on hardware properties and need to be monitored, for example proof testing interval, can be monitored by setting a flag with time when the proof test is performed. We will also investigate how the information provided by the monitoring and standard compliance verification framework can be integrated in the Arrowhead Framework e.g., Arrowhed Test Tool (ATT) [37], which enables the possibility to test producer and consumer interfaces for the Arrowhead services.

APPENDIX A
ACRONYMS

Acronym	Reference Abbreviation
ATT	Arrowhead Test Tool
CPPS	Cyber Physical Production System
CC	Common Criteria
CSCG	Cyber Security Coordination Group
CPS	Cyber Physical Systems
Cumulus	Certification Infrastructure for Multi-Layer Cloud Services
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
EGM	Evidence Gathering Mechanism
ENISA	European Network and Information Security
ETSI	European Telecommunications Standards Institute
EAL	Evaluation Assurance Levels
IoT	Internet of Things
ISO	International Organization for Standardization
IEC	International Electrotechnical Commision
ISMS	Information Security Management System
IIoT	Industrial Internet of Things
MIP	Measurable Indicator Point
MSI	Measurable Security Indicator
MSFI	Measurable Safety Indicator
MOI	Measurable Organizational Indicator
MA	Monitoring Agent
MA_i	Nr. of Monitoring Agents
MQTT	Message Queuing Telemetry Transport
NGcert	Next Generation Certification
PDCA	Plan-Do-Check-Act
PRMM	Process Reference Model
PRM	Process Reference Model
PAM	Pluggable Authentication Module
PP	Protection Profile
QMS	Quality Management System
SoS	System of Systems
SOA	Service Oriented Architecture
ST	Security Target
SECCRIT	Secure Cloud Computing for Critical Infrastructure IT
TOE	Target of Evaluation
TS	Target System

ACKNOWLEDGEMENT

The work has been performed in the project Power Semiconductor and Electronics Manufacturing 4.0 (SemI40), grant agreement n°692466. The project is co-funded by grants from Austria, Germany, Italy, France, Portugal and-Electronic Component Systems for European Leadership Joint Undertaking.

REFERENCES

[1] J. Delsing, "Iot automation: Arrowhead framework," 2017.
[2] A. W. Colombo, T. Bangemann, and S. Karnouskos, "Imc-aesop outcomes: Paving the way to collaborative manufacturing systems," in *12th IEEE International Conference on Industrial Informatics*, 2014.
[3] C. Schmittner, Z. Ma, and E. Schoitsch, "Combined safety and security development lifecylce," in *Industrial Informatics (INDIN), 2015 IEEE 13th International Conference on*. IEEE, 2015, pp. 1408–1415.
[4] M. Gaitanides, R. Scholz, and A. Vrohlings, "Prozeßmanagement-grundlagen und zielsetzungen," *Gaitanides, M., Scholz, R., Vrohlings, A., Raster, M.(Hrsg.)*, pp. 1–20, 1994.
[5] E. Jonsson, "Towards an integrated conceptual model of security and dependability," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*. IEEE, 2006, pp. 8–pp.
[6] D. Basin, F. Klaedtke, and S. Müller, "Monitoring security policies with metric first-order temporal logic," in *Proceedings of the 15th ACM symposium on Access control models and technologies*. ACM, 2010.
[7] L. Hayden, *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*. McGraw-Hill Education Group, 2010.
[8] A. Bicaku, C. Schmittner, M. Tauber, and J. Delsing, "Monitoring industry 4.0 applications for security and safety standard compliance," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018, pp. 749–754.
[9] A. Bicaku, S. Balaban, M. G. Tauber, A. Hudic, A. Mauthe, and D. Hutchison, "Harmonized monitoring for high assurance clouds," in *Cloud Engineering Workshop (IC2EW), 2016 IEEE International Conference on*. IEEE, 2016, pp. 118–123.
[10] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," *Journal of Information Security*, vol. 4, p. 92, 2013.
[11] C. C. Consortium *et al.*, "Common criteria (aka cc) for information technology security evaluation (iso/iec 15408), 2013."
[12] R. Atoui, J. Bennett, S. Cook, P. Galwas, P. Gupta, J. Haine, H. Trevor, C. Hills, R. Marshall, M. John, K. Munro, I. Philips, D. Purves, C. Robbins, D. Rogers, C. Shaw, R. Shepherd, and C. Shire, "Iot security compliance framework," *IoT Security Foundation*, 2016.
[13] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.
[14] K. Julisch, "Security compliance: the next frontier in security research," in *Proceedings of the 2008 workshop on New security paradigms*. ACM, 2009, pp. 71–74.
[15] D. J. Smith and K. G. Simpson, *Safety Critical Systems Handbook: A Straight forward Guide to Functional Safety, IEC 61508 (2010 EDITION) and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849*. Elsevier, 2010.
[16] K. Bond, "Iec 61511-functional safety: Safety instrumented systems for the process industry sector," in *Annual Symposium on Instrumentation for the Process Industries*, vol. 57, 2002, pp. 33–40.
[17] M. Lloyd and P. Reeve, "Iec 61508 and iec 61511 assessments-some lessons learned," 2009.
[18] R. K. Panesar-Walawege, M. Sabetzadeh, L. Briand, and T. Coq, "Characterizing the chain of evidence for software safety cases: A conceptual model based on the iec 61508 standard," in *Software Testing, Verification and Validation (ICST), 2010 Third International Conference on*. IEEE, 2010, pp. 335–344.
[19] A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone, "Taming dr. frankenstein: Contract-based design for cyber-physical systems," *European journal of control*, vol. 18, no. 3, pp. 217–238, 2012.
[20] D. Schneider and M. Trapp, "Conditional safety certificates in open systems," in *Proceedings of the 1st workshop on critical automotive applications: robustness & safety*. ACM, 2010, pp. 57–60.
[21] E. ISO, "9001: 2015 quality managem5ent systems," *Requirements (ISO 9001: 2015), European Committee for Standardization, Brussels*, 2015.
[22] "Iso 18404:2015 - quantitative methods in process improvement – six sigma – competencies for key personnel and their organizations in relation to six sigma and lean implementation," https://www.iso.org/standard/62405.html.

[23] "Iso/iec ts 33052:2016 - information technology – process reference model (prm) for information security management," https://www.iso.org/standard/55142.html.
[24] M. T. Lazarescu, "Design of a wsn platform for long-term environmental monitoring for iot applications," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 45–54, 2013.
[25] Y. Liu, Y. Yang, X. Lv, and L. Wang, "A self-learning sensor fault detection framework for industry monitoring iot," *Mathematical problems in engineering*, vol. 2013, 2013.
[26] S. Tennina, M. Bouroche, P. Braga, R. Gomes, M. Alves, F. Mirza, V. Ciriello, G. Carrozza, P. Oliveira, and V. Cahill, "Emmon: A wsn system architecture for large scale and dense real-time embedded monitoring," in *Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on*. IEEE, 2011, pp. 150–157.
[27] N. Enterprises, "Nagios," https://exchange.nagios.org/directory, 2017.
[28] OpenStack-Wiki, "Ceilometer," 2017.
[29] R. Olups, *Zabbix 1.8 network monitoring*. Packt Publishing Ltd, 2010.
[30] S. Pfleeger and R. Cunningham, "Why measuring security is hard," *IEEE Security & Privacy*, vol. 8, no. 4, pp. 46–54, 2010.
[31] W. Jansen, "Research directions in security metrics," *Journal of Information System Security*, vol. 7, no. 1, pp. 3–22, 2011.
[32] T. Phinney, "Iec 62443: Industrial network and system security," *Last accessed July*, vol. 29, 2013.
[33] I. IEC, "61508 functional safety of electrical/electronic/programmable electronic safety-related systems," *International electrotechnical commission*, 1998.
[34] S. Maksuti, A. Bicaku, M. Tauber, S. Palkovits-Rauter, S. Haas, and J. Delsing, "Towards flexible and secure end-to-endcommunication in industry 4.0," in *IEEE 15th International Conference of Industrial Informatics INDIN'2017*, 2017.
[35] A. Bicaku, S. Maksuti, S. Palkovits-Rauter, M. Tauber, R. Matischek, C. Schmittner, G. Mantas, M. Thron, and J. Delsing, "Towards trustworthy end-to-end communication in industry 4.0," in *IEEE 15TH International Conference of Industrial Informatics INDIN'2017*, 2017.
[36] D. Schneider and M. Trapp, "Conditional safety certification of open adaptive systems," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 8, no. 2, p. 8, 2013.
[37] F. Blomstedt, "Arrowhead test tool," https://forge.soa4d.org/plugins/scmgit/cgi-bin/gitweb.cgi?p=arrowhead-f/arrowhead-f.git;a=blob;f=5_Compliance/1_Testtool/Arrowhead_SysD_Compliance+Test+Tool.pdf;h=f36e1b1cf63c5a05c79307a10d506739f15d9f4c;hb=HEAD.

Ani Bicaku is a PhD student at Luleå University of Technology and works as a researcher at the University of Applied Sciences Burgenland in the research field "Cloud and Cyber Physical Systems Security". Recently, he was working at the Austrian Institute of Technology in the AIT's ICT-Security Program and was responsible for evaluating data security, data privacy and high assurance in cloud computing. Also part of his duty was to build an OpenStack Cloud System testbed used for monitoring high assurance of critical infrastructure cloud services. He received the Dipl -Ing. degree in Communication Engineering from the Carinthia University of Applied Sciences, Klagenfurt - Austria and his B.Sc. degree in Telecommunication Engineering from the Polytechnic University of Tirana, Tirana - Albania.

Christoph Schmittner received his M.Sc. in System and Software Engineering at the University of Applied Sciences Regensburg in 2013. His main research area is safety and security co-engineering.
He works on safety, security analysis and coanalysis methods, connected and safety critical / fault & intrusion tolerant system architectures, functional safety and cybersecurity standards and interdepen-dence of safety and security in critical systems.
He is member of the Austrian mirror committees for ISO/TC 22 Road vehicles and IEC TC 56 Dependability and designated Austrian expert in corresponding international standardization groups (IEC 61508, IEC 62443 ISO 26262 and ISO/SAE 21434), member of TC65/WG20 "Industrial-process measurement, control and automation – Framework to bridge the requirements for safety and security", TC65/AHG2 "Reliability of Automation Devices and Systems" and TC65/AHG3 "Smart Manufacturing Framework and System Architecture" and coordinating the Austrian contribution to the development of ISO/SAE 21434 "road vehicles – cybersecurity engineering".

Patrick Rottmann recently finished his Master's thesis on "Monitoring and Standards Compliant Measurements in Industry 4.0" at the university of Applied Sciences Burgenland, in the Master program Cloud Computing Engineering. Prior to that he completed his BSc at the University of Applied Sciences Burgenland in the BSc Program IT Infrastructure Management. In parallel to his studies he was working as IT Engineer at the Umweltbundesamt GmbH where he still leads and coordinates IT Infrastructure projects.

Markus Tauber works as FH-Professor for the University of Applied Sciences Burgenland, where he holds the position: director of the MSc program "Cloud Computing Engineering" and leads the research center "Cloud and Cyber-Physical Systems Security". Between 2012 until 2015 he coordinated the research topic "High Assurance Cloud" at the Austrian Institute of Technology (AIT) part of AIT's ICT-Security Program. Amongst other activities he was the coordinator of the FP7 Project "Secure Cloud computing for CRitical infrastructure IT" - (www.seccrit.eu) and involved in the ARTEMIS Project Arrowhead. From 2004 to 2012 he was working at the University of St Andrews (UK) where he worked as researcher on various topics in the area networks and distributed systems and was awarded a PhD in Computer Science for which he was working on "Autonomic Management in Distributed Storage Systems".

Prof. Jerker Delsing received the M.Sc. in Engineering Physics at Lund Institute of Technology, Sweden 1982. In 1988 he received the PhD. degree in Electrical Measurement at the Lund University. During 1985 - 1988 he worked part time at Alfa-Laval - SattControl (now ABB) with development of sensors and measurement technology. In 1994 he was promoted to associate professor in Heat and Power Engineering at Lund University. Early 1995 he was appointed full professor in Industrial Electronics at Lulea University of Technology where he currently is the scientific head of EISLAB, http://www.ltu.se/eislab. His present research profile can be entitled IoT and SoS Automation, with applications to automation in large and complex industry and society systems.
Prof. Delsing and his EISLAB group has been a partner of several large EU projects in the field, e.g. Socrades, IMC-AESOP, Arrowhead, FAR-EDGE, Productive4.0 and Arrowhead Tools. Delsing is a board member of ARTEMIS, ProcessIT.EU and ProcessIT Innovations.