Security Standard Compliance and Continuous Verification for Industrial IoT

Journal Title
XX(X):1–16

DOI: 10.1177/ToBeAssigned
www.sagepub.com/
SAGE

Ani Bicaku[1,2], Markus Tauber[1] and Jerker Delsing[2]

Abstract

Due to globalization and digitalization of industrial systems, standard compliance is gaining more attention. In order to stay competitive and remain in business, different sectors within industry are required to comply with multiple regulations. Compliance aims to fulfill regulations by including all measures imposed by laws and standards. Every device, application or service implements several technologies at many levels, and standards support interoperability across them. They help to create global markets for industries and enable networked development in order to be successful and sustainable. This work highlights the importance of standard compliance and continuous verification in Industrial IoT and implements an automatic monitoring and standard compliance verification framework.In this work, we focus on security, safety and organizational aspects of Industrial IoT. For each of them it is identified a representative number of standards, which are used to extract security, safety and organizational measurable indicator points. In addition, it is provided a metric model that forms the basis for the necessary information needed for compliance verification, including requirements, standards and metrics. Also, we present the prototype of the monitoring and standard compliance verification framework used to show the security compliance of an Industrial IoT use case.

Keywords

IIoT, IoT, Security, Safety, Organizational, Standard, Compliance, Monitoring, Digitalization, Industry

Introduction

Digitalization and hyper connectivity are already shaping and will shape our economy and society in an unpredicted way. The advances in technologies such as the Internet of Things (IoT), Cyber Physical Systems (CPS), embedded systems, cloud computing, Service-oriented Architecture (SOA), etc., provide all the enabling elements towards the fourth industrial revolution - Industry4.0, which is reshaping the industrial landscape. The application of the IoT to the manufacturing industry is called the Industrial Internet of Things (IIoT). IIoT will revolutionize the manufacturing by making possible to automatically and adaptively carry out processes that will interconnect and interact with each other (1), (2). Within IIoT, the information is monitored and synchronized between the physical cyber level by providing a digital representation of all devices, systems and processes, including large scale distributed systems, data and operations involved in the production of goods and services (3). In such environment, information security is one of the major concerns in all industries. Without proper security measures, intrusion attempts and non-authorized access will increase, resulting in higher costs, loss on sale, as well as leaks in critical data. Such data leaks can interrupt, modify or sabotage an operational process with intention to cause harm. In response, governments and standardization bodies have published several standards and regulations to help improving the security of industrial systems (4).

In industrial environments several devices are interconnecting with each other over IIoT platforms. Despite the significant benefits, this connectivity increases the possibility of security being compromised via malware, buffer overflow, and denial of service (DoS) attacks (5), (6), (7).

The latest reported attacks, such as the Ukraine's power grid attack by the Industroyer malware, which caused one hour collapse of systems responsible for serving Kiev with electricity (8); Dyn Cyberattack (9), involving multiple DDoS attacks targeting systems operated by the DNS provider Dyn; the Jeep Cherokee Hack (10), where hackers were able to remotely control the brakes and steering of the vehicle; Triton malware used to shutdown an industrial process by exploiting weaknesses in ICS, etc., are proof that the IIoT devices need a robust security framework in place to avoid any security issue. Non-authorized access into IIoT networks can lead to a loss in brand loyalty, reputation, major losses of revenue or market share, and more depending on the nature and severity of the attack.

Given the above scenarios, many industrial companies want to implement scalable security standards that can be easily assessed via measurable metrics. To understand their security exposure, they will need to improve their security process to fully incorporate standard compliance. Standardization assumes an important role in the digitalization of the industrial production since standards may affect the development, installation and runtime of industrial applications. For example, standardization can support the deployment of IIoT and particularly the smooth migration from the traditional

[1]University of Applied Sciences Burgenland - Austria
[2]Lulea University of Technology - Sweden
Email: ani.bicaku@fh-burgenlad.at, ani.bicaku@ltu.se,
markus.tauber@fh-burgenland.at, jerker.delsing@ltu.se

control systems to Industry4.0, by easily interfacing with existing legacy devices, plug-and-play systems, and algorithms, adapting their behaviour and interactions on-the-fly.

Nowadays, we use standards in our everyday life - healthcare, telecommunication, transport, food, energy, etc. These industries are governed by a large number of standards and regulations. Some of them have been around for a long time (e.g., weight and measure standards), others are worldwide recognized and they simplify our life, (e.g., Wi-Fi can be used everywhere in the world to navigate the internet).

Businesses, global economy and users have their benefits from these international standards. For businesses, standard compliance provides protection of interests, lower costs by avoiding redundancy, minimizing errors and reducing time to market. For the economy, standard compliance help services, devices and products to make sure that they can be produced in one specific country and used in another. For the user, standard compliance is important to provide safe and secure services, interconnection and interoperability with other services and systems worldwide (11). Due to digitalization and the increasing number of standards, a comprehensive compliance tool is needed to stay competitive and remain in business.

This paper examines the concept of IIoT and its enabling technologies with the main goal to highlight the importance of standard compliance as a way for increasing the accessibility, speed and comprehensiveness of information that supports the decision making process within an organization. It first evaluates existing standards and best practice guidelines from international standardization bodies, including recent developments (e.g., project that have already addressed this problem, IoT frameworks, tools, etc.). It then explains the usage of standards to extract Measurable Indicator Points (MIP), which are categorized in: (i) Measurable Security Indicators (MSI), (ii) Measurable Safety Indicators (MSFI) and (iii) Measurable Organizational Indicators (MOI). The MIPs are documented in a metric model, which is used to efficiently extract meaningful information for the Monitoring and Standard Compliance Verification framework (MSCV) based on a set of requirements. In our previous work (12), we have proposed the MSCV framework architecture and in here we evaluate it in an IIoT use case to show the functionality and how can be extended in the future. We also include an example usage of the metric model as input for the MSCV.

The reminder of this paper is organized as follows:

Section II reviews existing compliance standards, frameworks and tools including related research projects. Section III, presents the overall standard landscape based on the role of standardization bodies and the importance of standard compliance in different industry aspects. In Section IV is provided an evaluation of security, safety and organizational standards and their dependability. Section V presents the metric model based on the evaluated standards including requirements, standards and metrics. In Section VI is introduced the MSCV framework and its architecture, which is evaluated in Section VII in an IIoT use case. We conclude our work in Section VIII and a table for acronyms in the text is shown in Appendix A.

Related Work

Standard compliance frameworks and tools

- **Cobit-5** framework (13) addresses the governance and management of IT by integrating the organization IT into governance and covering all functions and processes within the organization. The framework includes five principles to build a governance and management framework such as: meeting stakeholder needs, end-to-end coverage, holistic approach, integrated framework and separation of governance from management. These principles are based on seven enablers: principles, policies and frameworks; processes; organizational structure; culture, ethics and behaviour; information; services, infrastructure and applications; and people, skills and competences. These enablers are generic and useful for all kind of organizations (commercial, non-profit or public). They provide three core publications: (i) Cobit 5 Framework, which describes the framework, including enablers (ii) Cobit 5 Enabling process, where are documented best practices used day-by-day and (iii) Cobit 5 Implementation, which provides the methodology for continuous improvement of IT governance.
- **COSO** framework (14) is a well accepted framework against which organizations measure the effectiveness of their systems of internal controls. The updated framework, based on the first release in 1992, helps organizations to effectively develop and maintain systems that are capable to adapt in changing environments. It consist of five components: (i) control environment, (ii) risk assessment, (iii) control activities, (iv) information and communication and (v) monitoring activities. The controls are defined as processes and the objective is to achieve efficiency of operations, reliability of financial report and compliance with laws and regulations. COSO provides a high-level view of the controls without any specification or detailed implementation.
- **OpenSCAP** framework (15) is based on the SCAP protocol (16) with specifications to support automated configuration, vulnerability, patch checking and security measurements. The OpenScap is an ecosystem of open-source tools implementing the SCAP standard, which consists of seven components: (i) XCCDF, a language used to describe the security checklist, (ii) OVAL, a language to make logical statement about the state of a system, (iii) DataStream, a format that packs the other components into a single file, (iv) ARF, known as the result data stream, (v) CPE, used to identify platforms and systems using unique defined names, (vi) CVE, a reference for already known vulnerabilities, and (vii) CWE, a list of software weaknesses to describe in detail known security weaknesses and flaws. The framework makes use of the National Vulnerability Database[1] by loading CVE feed, which are updated by the vendors of enterprise operating systems based on their new releases. OpenSCAP loads the CVE feed, which has data about the security vulnerabilities, and compare every item in the feed with system packages. This is an efficient way to

check the packages installed by an official source. OpenSCAP supports SCAP standard version 1.2 and is compatible with other SCAP versions. Also, it supports the OVAL language and the XCCDF in current versions. The framework consists of many security auditing tools and SCAP content used in vulnerability assessment and security compliance areas. Most important part of the ecosystem is the OpenSCAP shared library. On the top of the library is built the OpenSCAP scanner, which is a command line tool with plenty of features. OpenSCAP support online and offline evaluation. When local or remote machines are monitored, the online evaluation is used to do runtime checks. When containers and virtual machines are monitored, the offline evaluation is used, which means that the file system is evaluated in read-only mode. The disadvantage of this evaluation is that it is not possible to fix system issues in the read-only mode.

- **SOC** compliance (17), created by AICPA, is designed for service providers storing data in the cloud. There exist three types of SOC reports: SOC 1, SOC 2 and SOC 3. Each of them has different focuses and purposes. SOC 1 - covers the organizations internal control over financial statement and reporting. SOC 2 - covers the controls of the systems used to process data, security and privacy of the data. SOC 3 - is a general use report. SOC 2 verifies if the organization comply with the requirements based on five trust criteria (security, availability, integrity, confidentiality and privacy). SOC 2 includes two reports: (i) type 1 - a report describing the system and suitability of the system design, (ii) type 2 - a report describing the system and operating effectiveness of the controls.
- **OPA** (18) is a compliance framework, which checks process models against compliance rules based on modeling languages. Since BPM does not check which processes are compliant and which not, they introduce a compliance checking method including six steps: (i) model business processes using BPEL, (ii) BPSL to specify compliance rules, (iii) transform the BPEL into representation process using pi-calculus, (iv) BPSL compliance rules are transformed into LTL, (v) model checking technology to verify if the business processes comply with the regulations and (vi) provide a counterexample to show how the compliance rules can be violated. However, this approach is limited to process modeling and does not include resources and data constrains related to these processes.
- **CSA CCM** framework (19), the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) provides fundamental security principles to guide cloud vendors and assist prospective cloud customers in determining the overall security risk of a cloud provider. The CSA CCM provides a control framework with a detailed explanation of security concepts and principles that are aligned to the CSA guidance in 13 domains. The CCM already provides a common interface to verify the security measures, but how to automatically provide the standard compliance is still under research.
- **GRC** - Governance, Risk, Compliance Capability Model (20), developed by the OCEG, consist of eight components (context, organize, assess, proact, detect, respond, measure and interact) and 33 elements, where each has a number of practices listed. This model is useful to understand the GRC activities, but it does not distinguish between operational and management processes. Furthermore the model does not provide any information on how it relates to existing standards.

	Real Time Support	Resources Availability	Open-Source	Standards	Human Intervention	Metric Classification	Component Compliance	Documentation
COBIT 5	+	-	-	-	+	-	-	+
COSO	+	-	-	+	+	-	-	+
OpenScap	-	+	+	+	-	-	-	+
SOC	+	-	-	-	+	-	-	+
OPA	+	+	+	-	+	-	-	+
CSA CCM	+	-	-	+	+	-	-	+
GRC	+	-	-	-	+	-	-	+

Table 1. Compliance Frameworks and Tools Evaluation

In table 1, we show the comparison of the evaluation of the frameworks and tools. They all consider real-time operations and have significant documentation about the procedure during compliance check. Most of them need the human intervention in order to read the results of the compliance. All the evaluated frameworks and tools fail in providing metric classification and single component compliance. Also, not all of them are open-source, and don't give the possibility to write own scripts. COSO, OpenScap and CSA CCM are compliant to standards but only to specific standards, the user can not add other standards.

Projects and publications in standard compliance

In spite of the importance of standard compliance, few research works have addressed the problem. However, there is a considerable number of research projects that identify the need of standards and their usage, but none of them considers automated compliance.

COPRAS[2] project had the scope to bring together and exchange information between research and ICT standards by encouraging projects to engage in standards activity to stimulate their dissemination and usage.

Arrowhead[3] project had the objective to address the technical challenges associated to automation. The project has evaluated and used several security and safety standards with the aim to standardize the Arrowhead Framework, work which is continued in the Productive4.0 project.

SECCRIT[4] project had the goal to analyze and evaluate cloud computing security in critical infrastructure IT by developing methodologies and best practices including risk assessment, policy specification and assurance evaluation.

Several standards are used and a cloud evaluation method is developed based on metrics extracted from these standards.

SemI40[5] project focuses on smart production and cyber physical production systems by providing tools and methodologies for system integration of smart device capabilities such as sensing, communication, knowledge management, decision-making, control, actuation, resulting in smart maintenance and smart production execution. The project focuses in semiconductor industry and has a work package dedicated to standardization with the goal to contribute in standardization bodies and ensure the long term technological impact.

Productive4.0[6] project aims to achieve significant improvement in digitalising the European industry by means of electronics and ICT. This project has a standardization work package with the objective to influence relevant standards in the industry. It provides an overview of involved standards in the industrial area including surveys, guidelines and identification of gaps in existing standards.

Existing works such as (21),(22), (23), and (24) outline the issues with manual compliance audits and the need for humans to interpret these documents. In (21) the authors group the compliance monitoring tools in: (i) compliance managers, (ii) vulnerability scanners, (iii) penetration testers, (iv) security events managers and (v) governance risk. Also, they highlight the overlaps among and between different compliance documents. To solve this problems, it is proposed an enhanced compliance ontology for requirements based on natural language processing tools that are used to structure the information and populate the ontology. In order to automate the approach, compliance requirements are linked to implementation verification scripts. However, the goal of this framework is to provide compliance monitoring for requirement documents by using ontology definitions focusing on the concepts written in compliance documents.

A framework for automating security analysis of the IoT is introduced in (22). The goal is to model and assess the security of IoT, which is used to build a graphical security model (based on Hierarchical Attack Representation Model(HARM)) and a security evaluator to provide automatic security analysis. The main goal of the framework is to identify attack paths in IoT, evaluate the security based on metrics and see the effectiveness of different defense strategies. The security metrics are classified in four levels (network, attack path, node and vulnerability). To see the functionality of the framework three example networks are evaluated and possible attack paths are computed. From the analysis, the system can decide to assess different defense mechanisms to protect the network. However, the security metrics are not extracted from security standards and the framework does not consider any compliance with existing standards.

In another study (23), where a process model for integrated IT governance, risk and compliance management is presented, the authors propose an integrated process model for high level IT GRC management. They consider models for three IT GRC disciplines (i) IT governance, (ii) IT risk management, and (iii) IT compliance and for each an adequate standard is evaluated. This works shows that IT governance, risk and compliance processes can be integrated based on their commonalities. However, the processes do not describe in details how the integration will look like or which technologies are used.

Safa et. al (24) provide the concept for a novel model to show the compliance with Information Security Organizational Policies and Procedures (ISOP) by literature review and two fundamental theories (Social Bond Theory and Involvement Theory). The proposed framework has two main parts: (i) the aspects of information security (knowledge sharing, collaboration, intervention and experience) and (ii) the main elements in the Social Bond Theory such as attachment, commitment and personal norms. The aim of this concept is to check how information security policy compliance arises in organizations by showing how employees comply with organizational information security policies. The results of the analysis confirmed that information security sharing has strong effects towards compliance with ISOP. However it does not provide any compliance procedure or how to assess ISOP compliance in organizations.

An ontology-based information security compliance based on ISO 27002 is presented in (25). The authors provide a method for formalizing information security controls and integrate them in decision support for risk and compliance management. The authors show how the research results can be used in a real-world scenario by implementing and validating the approach in an Austrian organization. Using the information collected during the evaluation, they were able to model the ongoing risks, identify the assets and determine the weakness of the system. A software tool is used to show the compliance level of the organization. The results showed that the generated decisions were in line with ISO27002 standard. However, they considered only one standard and they do not check any dependency between security, safety and organizational aspects.

The existing literature concentrates on describing the structure of a compliance framework, but fails in general, to describe in detail the process and the content for having a standard compliant system. Due to the lack of guidance, the compliance managers often use commercially available sources, or public and open source templates available in the Internet. The process of developing and implementing a compliance framework is not straight forward, since it is driven by multiple issues such as standardization bodies, complexity of new technologies, and external and internal threats. The existing literature highlights several compliance methods, but these methods do not include a comprehensive or detailed step-by-step process. Accordingly, this paper aims to provide a general compliance solution without compromising the underlying infrastructure. The MSCV framework provides the compliance for a single component/the entire system based on a single standard/multiple standards.

Even if a provider claims that has implemented all the measurable indicator points of the standards, there is no way to verify this. To overcome this, the MSCV framework aims to automate the standard compliance. In order to automate such a process, we identify different standards (based on the requirements); classify them in security, safety and organizational; generate a set of MIPs; provide monitoring possibilities for each MIP via existing/customized plugins and provide the compliance for standard/set of standards.

Standardization Landscape

Industry 4.0 depends on a number of innovative technological developments including IIoT, which uses the information and communication technology to monitor and control industrial processes; communication; big data analysis and cloud computing. Standards are essential to ensure the understanding between these domains. A standard is the report used to set requirements and definitions for a specific component, system or service, which is approved by a recognized evaluation authority. They provide rules or guidelines including tests, methods, reference data, proof of concepts and analysis (26).

This section describes the standardization bodies and the role of their standards in different domains. Since our work is about compliance we choose a set of standards for each domain to describe the importance of standard compliance.

Role of Standardization Bodies

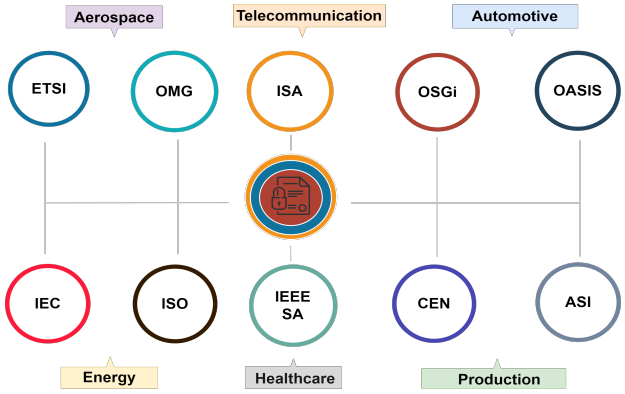

Figure 1. International standardization bodies

ISO (International Standards Organisation) is an independent, non-governmental international organization with a membership of 162 national standards bodies. They create documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. ISO has published 22.362 international standards for almost every sector, which are drafted by technical committees, subcommittees and working groups comprised of experts appointed by ISO.

IEC (International Electro-technical Commission) is a not-for-profit, quasi-governmental organization with 86 National Committees (one for each country). They are the world's leading organization that prepares and publishes international standards for all electrical, electronic and related technologies, known as "electrotechnology". These standards serve as a basis for national standardization and as references when drafting international tenders and contracts. They have published 1324 international standards. Over 170 technical committees and subcommittees, and about 700 project teams carry out the standards work of IEC.

IEEE-SA (Institute of Electrical and Electronics Engineers Standard Association) is not a body authorized by any government, but a community. It is an organization within IEEE that develops global standards and advances global technologies. They bring together individuals and organizations from a wide range of technical and geographic points of origin to facilitate standards development and standards related collaboration. Within more than 160 countries, they promote innovation, enable the creation and expansion of international markets and help protect health and public safety.

CEN (European Committee for Standardization) is an association with 34 European countries. CEN has been officially recognized by the European Union and by the European Free Trade Association as being responsible for developing and defining voluntary standards at European level. They support standardization activities in relation to a wide range of fields and sectors including air and space, chemicals, construction, consumer products, defense and security, energy, food and feed, health and safety, etc.

CENELEC (Comité Européen de Normalisation Electro-technique) is a non-profit organization with 33 member countries and 13 affiliate member countries for the European marketplace that works closely with the European Union but it is not an EU institution. It is responsible for standardization in the electrotechnical engineering field and prepares voluntary standards, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market.

ETSI (European Telecommunications Standards Institute) is an independent, not-for-profit, standardization organization in the telecommunications industry in Europe with more than 800 member organizations worldwide from 66 countries and five continents. Members are large and small companies, academia, government and public organizations. ETSI has produced over 30.000 international standards or information and communications technologies, including fixed, mobile, radio, converged, broadcast and internet technologies.

OMG (Object Management Group) is an international not-for-profit computer industry standard organization with more than 800 members for vendor-independent cross-system object-oriented programming. OMG standards include the Unified Modeling Language and Model Driven Architecture to enable visual design, execution and maintenance of software and other processes.

ISA (Instrument Society of America) is a non-profit professional association that sets the standards for those who apply engineering and technology to improve the management, safety and cyber security of modern automation and control systems used across industry and critical infrastructure. It has more than 40.000 members and 400.000 customers around the world. ISA has produced more than 150 standards documents where 4000+ automation professionals and 140 committees have been involved.

OSGi Alliance is a worldwide consortium of technology innovators that advances a proven and mature process to create open specifications that enable the modular assembly of software built with Java technology.

OASIS (Organization for the Advancement of Structures Information Standards) is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. They work on the development, convergence and adoption of open

standards for security, IoT, energy, content technologies, emergency management and other areas. The consortium has more than 5.000 participants representing about 600 organizations and individual members in more than 65 countries.

ASI (Accellera Systems Initiative) is a non-profit organization dedicated to create, support, promote, and advance system-level design, modeling and verification standards for use by the worldwide electronics industry. They have the goal to develop technology standards that are balanced, open and benefit the worldwide electronics industry. Leading companies and semiconductor manufacturers around the world are using these electronic design automation and intellectual property standards in a wide range of projects in numerous application areas to develop consumer, mobile, wireless, automotive and other smart electronic devices.

Importance of Standard Compliance

Standards are necessary in almost every business. Each device, application or service implements standardized technologies at many levels. They support interoperability across these technologies and help create global markets by enabling networked development on top of existing technology platforms. Standards embody a state of the art of technology development and are an essential resource for researchers in different aspects (27). We cannot cover all the standards in this article, but we provide an overview of the key standards in each industry as shown in figure 2 and the importance of standardization.

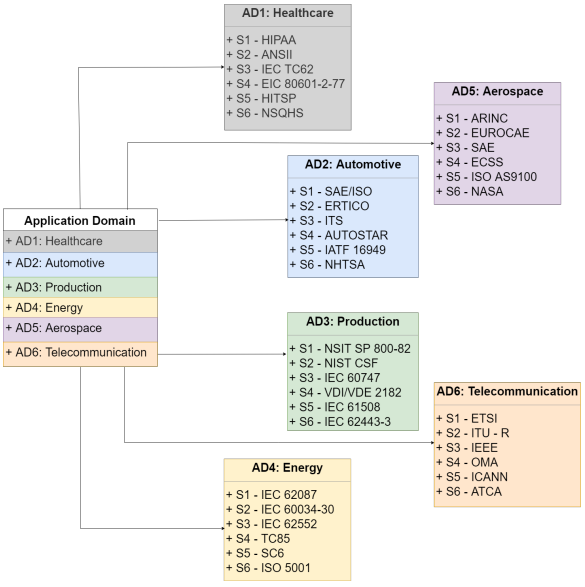

Figure 2. Standards in different application domains

Following is presented the importance of standard compliance for different industry domains.

Healthcare: Standard compliance in healthcare can cover a wide variety of practices and observe internal and external rules. But most healthcare compliance issues relate to patient safety, the privacy of patient information and billing practices (e.g., HIPAA, HITSP, etc) (28). Compliance keeps operations running smoothly and makes sure everyone follows proper procedures and understands expectations. Compliance in healthcare comes with even higher risks than in other industries. If a doctor or nurse doesn't follow proper procedure, they can end up injuring a patient or another staff member. Ultimately, healthcare compliance is about providing safe, high-quality patient care (e.g, IEC TC62, EIC 80601-2-77, etc). Complying with industry standards and regulations helps healthcare organizations continue to improve the quality of care. These organizations have to follow standards, regulations and laws from the federal and state level. Violations of these laws can result in lawsuits, fines or loss of licenses.

Automotive: Each region has its own automotive standards, meaning that companies should adapt their production standards in order to distribute their products in different countries around the world. Automotive industrial standards are important for improvement, maintenance prevention and cost reduction in the supply chain (e.g., IATF 16949). Other important aspects are the safety and environmental regulations such as NHTSA standard. Automobile parts such as tires, brakes, gears, etc., are subject to standardization in order to prevent accidents. In this industry, standards and regulations aim also to reduce the emission of CO_2, NO_2, noise, greenhouse gases used in mobile air-conditioning systems and fuel quality.

Aerospace: The aerospace industry includes commercial aerospace, regional jet, general aviation, helicopter (civil or military), defense (UAV, fighter, etc.) and space. Standard compliance in aerospace covers a wide range of areas, such as product safety, management, material testing, maintenance support and much more. Becoming compliant to standards such as EUROCAE, ISO AS9100, etc., can have several benefits for aerospace manufacturers and suppliers (29). Another important aspect is the air traffic management (30), used to maintain the distance between aircrafts, safety on ground and to regulate the flow of the aircraft (e.g., ARINC standards).

Telecommunication: Telecommunication standards are fundamental to the operation of the ICT networks. Without them it is not possible to make a telephone call or surf the internet. For internet access, transport protocols, voice and video compression and other aspects of ICTs, several standards such as ITU-R, ETSI, ICANN, etc., allow systems to work locally and globally (31). These standards are important to facilitate the interoperability of technologies, promote the competition and hold down the prices by exchanging information over a significant distance.

Energy: Energy standards describe the energy performance of manufactured products, used also to deny the sale of products that are less energy efficient than the minimum standard requirements (32). These regulations usually have two aims: i) protocols used to have an accurate estimate of the energy performance of a product in the way it is typically used, or a ranking of its energy performance compared to other models such as ISO 5001; and ii) limits on energy performance (max/min efficiency) based on several tests such as IEC 62087.

Production: Standard compliance in production is the fulfillment of laws, regulations, guidelines and specifications. They can range from manufacturing-oriented (e.g., IEC 61508, VDI/VDE 2182, etc) to product-oriented (e.g., IEC 60747) and can be either domestic or international standards (33). The violation of these regulations will result in

legal sanctions, fines or even withdraw from the market. With the necessary compliance to standards, production organizations are able to operate and deliver safe, secure and quality products worldwide. The production industry has a need for globally accepted standards for design and materials in the manufacturing ecosystem. In support of these standards, several countries have their national initiatives: *Germany*-Industrie4.0, *USA*-Manufacturing USA, *China*-Made in China 2025, *Korea*-Manufacturing Innovation 3.0, *France*-Industrie du Futur, etc.

Standards and Best Practice Guidelines Evaluation

Based on the evaluation of different industry domains in the previous section, there are different types of standards. For the purpose of this work we have limited our discussion to the security, safety and organizational standards in the production environment (based on an IIoT use case, explained in section , and the requirements of industrial partners from the SemI40 project). In order to understand security compliance we also need to consider dependable aspects, such as safety and organizational. While security refers to the protection from threats and vulnerabilities based on a given set of requirements, safety is the condition of being protected from environmental damage, injury or loss of life and organizational aspects make sure to avoid redundancy and minimize errors.

Following are summarized the most relevant security, safety and organizational standards with the aim to identify if they consider the dependability between each other and what are the gaps that need to be considered to provide an improved overall security concept for IIoT.

Security Standards

	Security Standards and Best Practice Guidelines														
	NIST Special Publication 800-82	NIST Special Publication 800-184	NIST CSF	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27005	ISO/IEC 27017	ISO/IEC 15408 - CC	CCSC	NISPOM	CTP	CSA-ICS	NAMUS NA115	VDI/VDE 2182	IEC 62443-3
Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Organizational	0	1	1	1	0	1	1	0	0	1	0	0	0	0	0
Safety	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1

Table 2. Security Standards

The evaluated security standards and best practices particularly focus on operational security and organizational. Every standard has a specific focus, for example if we consider ISO270xx series of standards - if the scope is to use the framework for information security the ISO27001 standard is required, if the scope is to implement controls ISO27002 standard is required, if the scope is to have risk assessment the ISO27005 standard is required and if it is needed to secure the information in cloud the ISO27017 standard is required. However, some of them also consider organizational aspects and only four safety aspects.

Safety Standards

	Safety Standards and Best Practice Guidelines			
	IEC 61508	IEC 61511	ANSI/ISA-84.00.01	IEC 62061
Security	1	1	1	0
Organizational	0	0	0	0
Safety	**1**	**1**	**1**	**1**

Table 3. Safety Standards

The safety standards and best practice guidelines such as IEC 61508, IEC 61511 and ANSI/ISA-84.00.01 slightly consider security. Even though security is not the focus of these standards, the planned updates will justify an assessment with 1. As a result, the analysis of applicable standards for operational security, organizational and safety shows that no size fits it all - thus, to have a knowledge base and proof that the system is operating in a desirable state with respect to the above mentioned aspects, a combination of these standards has to be considered.

Process Management Standards

	Organizational Standards and Best Practice Guidelines				
	ISO 9001	ISO 18404	ISO/IEC TS 33052	ISO/IEC 29169	ISO/IEC/IEEE 15288
Security	0	0	1	0	1
Organizational	**1**	**1**	**1**	**1**	**1**
Safety	0	0	0	0	0

Table 4. Process Management Standards

The process management standards mostly focus on organizational aspects. However some of them also consider other aspects. For e.g., ISO/IEC TS 33052 focused on organizational aspects uses ISO/IEC 27001 security requirements to define a process reference model for the domain of information security. ISO/IEC/IEEE 15288 provides technical management processes for e.g., risk management process.

	Standards and Best Practices																									
	Security															Process Management					Safety					
	NIST Special Publication 800-82	NIST Special Publication 800-184	NIST CSF	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27005	ISO/IEC 27017	ISO/IEC 15408 - CC	CCSC	NISPOM	CTP	CSA-ICS	NAMUS NA115	VDI/VDE 2182	IEC 62443 -3	ISO 9001	ISO 18404	ISO/IEC TS 33052	ISO/IEC 29169	ISO/IEC/IEEE 15288	IEC 61508	IEC 61511	ANSI/ISA-84.00.01	IEC 62061	ISO 13849-1	Working Draft of WG20
Backend Infrastructure	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Communication Layer	1	1	1	1	1	1	0	1	1	0	1	1	1	0	1	0	0	0	0	0	1	1	1	1	0	1
Physical Devices	1	0	1	1	0	0	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 5. Standards and best practice guidelines evaluated based on security, organizational, and safety aspects in a cyber physical production system

Discussion

In Table 5 is presented a summary of the evaluation of standards and best practice guidelines. The selected standards and best practice guidelines are evaluated with respect to the topic that they address considering Industry 4.0 main enablers, such as physical devices (e.g., sensors, PLC), communication layer (e.g., data exchange, protocols, gateways) and backend infrastructure (e.g., cloud services).

- ”0” stands for the standard/best practice guideline that does not focus or does not address at all a specific layer
- ”1” stands for the standard/best practice guideline that clearly addresses the specific layer

Every standard is designed with a certain focus. Standards such as NIST SP 800-82, NIST CSF, ISO/IEC 27001:2013, CC, NISPOM, CSA-ICS, NA115 and VDI/VDE 2182 consider the operational security of IIoT devices but in most of them is missing a step-by-step guideline how to achieve the intended goals. While most of the standards (i.e., NIST SP 800-82, NIST SP 800-184, NIST CSF, ISO/IEC 27001, ISO/IEC 27002, CC, CCSC, CTP, CSA-ICS and NA115) address the security for data exchange or communication protocols, other standards such as ISO/IEC 27017, ENISA, and C-SIG mainly focus on operational security issues in cloud platforms. The outcome of our evaluation, clearly indicates that there is no single standard that address security for the whole IIoT environment, from the edge devices to the backend infrastructure. Therefore, based on this evaluation, we conclude that a set of measurable security, safety and organizational metrics from different standards are needed in order to cover the whole system. To address this problem we developed a metric model and show its usage in the next section.

Metric Model

The Industrial Control Systems (ICS) have been traditionally built as stand-alone systems, not connected to the outside world. The interconnection with the corporate network, wireless, mobile or cloud-based services make them potentially reachable from attacks (34). Therefore, each industrial organization must understand the potential risks of a production environment, which is no longer isolated from the Internet and puts the system at a security risk (35).

Towards addressing this challenge, in this paper is presented a metric model shown in Figure 3. The metric model is used as input for the MSCV framework (explained in section) in order to define if a target system is operating in a standard compliant manner. The model is a mapping between the set of requirements, standards/best practice guidelines and MIPs. For each extracted MIP is provided an ID, name of the metric and sources from where this specific metrics is extracted.

The identification of the standards is done based on a set of requirements provided in a research project by industrial partners in support of a secured IIoT use case, described in our previous work (36).

However, the same approach can be applied to several industrial use cases. Each standard is analyzed to derive security, safety and organizational metrics used to address a specific requirement. To simplify the assessment, these metrics are categorized respectively in MSI, MSFI and MOI.

Figure 3 shows a simple example on how such a metric model can be used, in which only one requirement (access control) is considered. The model provides a list of MIPs extracted from the security, safety and organizational standards, which should be considered in an industrial application scenario with the goal to address the requirement of access control for the production line. The metrics are intended to provide the policy and procedures required for the addressing the access control of the evaluated standards.

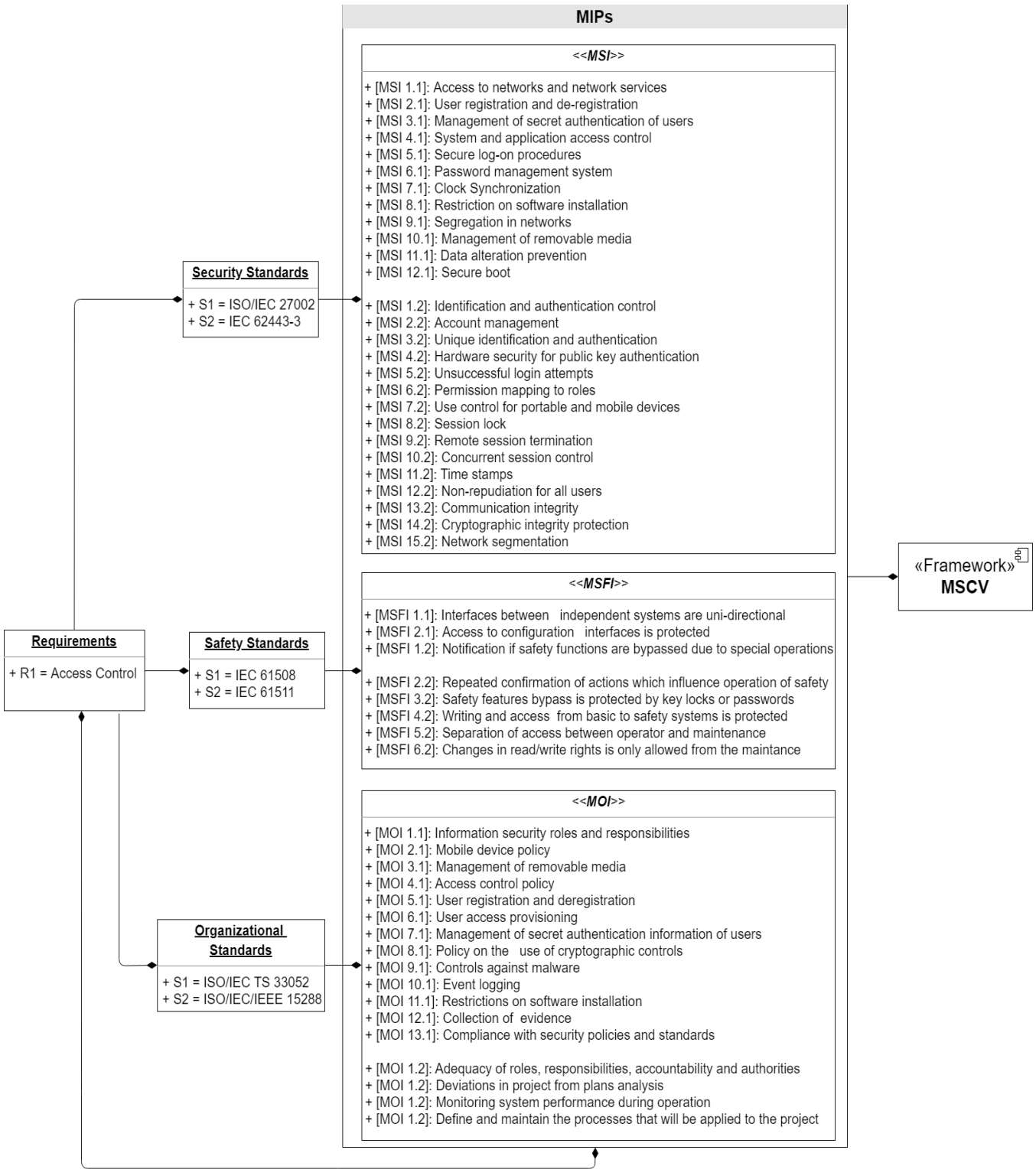

Figure 3. Example showing the usage of the metric model for security, safety and organizational standards considering the access control requirement

Following the model, the first step is to define a set of requirements related to a specific use case. After the requirements are defined (e.g. access control), the next step is to identify the standards addressing this requirement. From each standard, a set of metrics that can be used to address this requirement are extracted.

As an example, we present here only two standards for each classification:

- Security: ISO/IEC 27002[7] and IEC 62443-3[8]
- Safety: IEC 61508[9] and IEC 61511[10]
- Organizational: ISO/IEC-TS 33052[11] and ISO/IEC/IEEE 15288[12]

This is a simple representative example, which can be used as input for the MSCV framework.

Monitoring and Standard Compliance Verification Framework - Architecture

Figure 4 shows the architecture of the MSCV framework, which is developed as a composition of different components gathered in 3 core parts: (i) monitoring agents, (ii) Evidence Gathering Mechanism (EGM) and (iii) Compliance module.

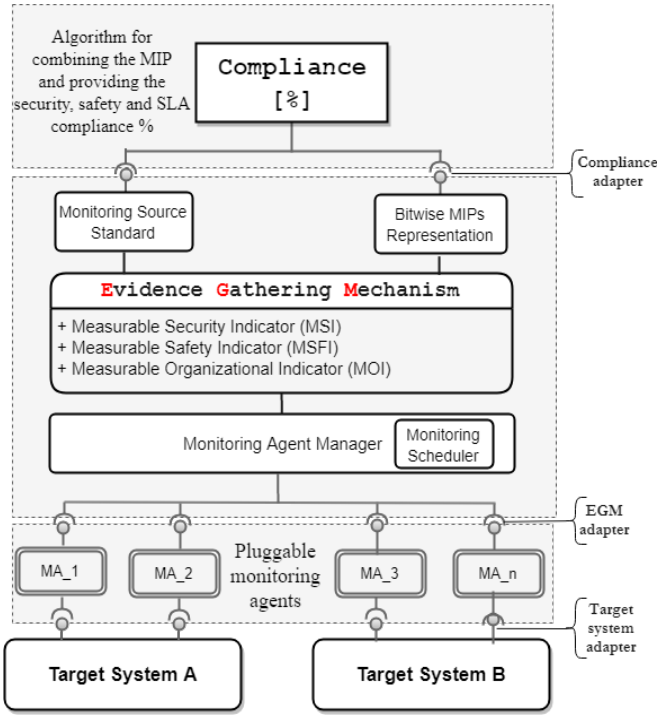

Figure 4. Monitoring and standard compliance verification framework used to measure, aggregate, schedule, store, retrieve and analyze the monitoring data to provide standard compliance

The first step to verify the compliance status against the requirements is to collect data effectively and efficiently. Therefore, as shown in Figure 4, the data are collected from the target system via pluggable monitoring agents (MA_n) that can be integrated from different plugins (e.g., Nagios (37), Ceilometer (38), Zabbix (39), etc.) and customized scripts. Then the collected data are fed to the EGM.

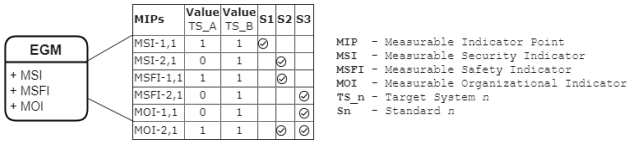

Figure 5. A representative set of the information provided by the EGM module

The EGM is designed to acquire, store and analyze security, safety and organizational related evidence (40). It categorizes the monitored data in MSI, MSFI and MOI and uses a monitoring scheduler to efficiently check the resources by deciding when to collect the data. Also, in the EGM module is included a monitoring source standard to map the specific standard with each monitored metric and a bitwise MIPs representation module that represent each metric by a binary number. This is the core part of the MSCV framework, where all the knowledge regarding MIPs and standards lies in. The information provided by the EGM is used as an input for the compliance module for further analysis. A representative set of the information provided by the EGM is shown in Figure 5.

The Compliance module receives from the EGM the source from which the metric is extracted and a binary value 1 or 0, which 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 $[0, 1]$ as shown in figure 6.

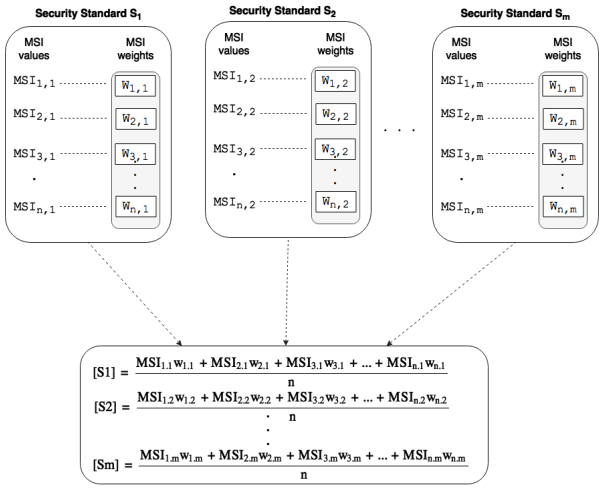

Figure 6. Security standard compliance verification

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. The total compliance $[\%]$ is defined as the ratio between the sum of each standard compliance (defined in equation 1) 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

The MSCV framework, illustrated in Figure 4, allows to gather security, safety and organizational evidence from the target system into a structured way. The architecture of the framework has a pluggable and extendable architecture allowing easy adaptation to constantly analyze and monitor the status of the system or components of the system. It is able to monitor a large number of measurable metrics for different CPS components by aggregating, scheduling, storing, retrieving and analyzing the monitoring data to provide standard compliance verification.

IIoT Use Case

To show the functionality of the MSCV framework we consider an IIoT use case, shown in figure 7 (41). The MSCV framework will be used to: (i) check the compliance of each component based on the use case requirements and a set of metrics extracted from international standards, and (ii) to provide the overall compliance of the system based on equation 2.

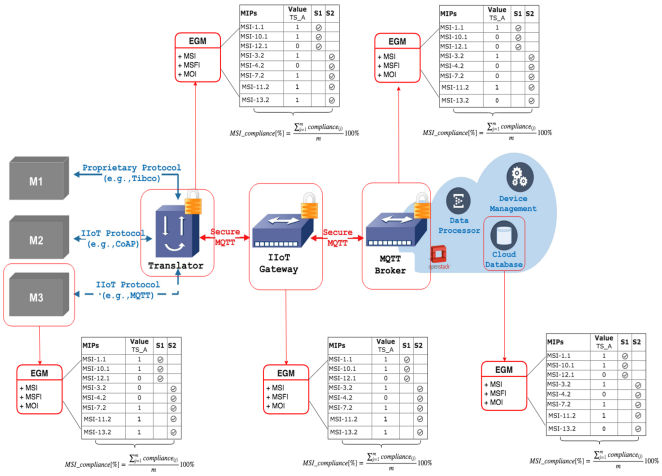

Figure 7. The end-to-end communication use case used to check the overall compliance of the system based on five components and two security standards

To provide an application service (e.g., device management as a service), data are transmitted between devices, processed throughout the network, 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 system is the MQTT protocol. MQTT is a lightweight protocol widely used to accommodate the IoT devices with low power and bandwidth requirements. In the production environment, new industrial devices are already able to communicate using state of the art IIoT protocols, such as MQTT, but legacy devices will need a translator (42) to be able to communicate via IIoT protocols.

In such a scenario, with different decentralized IIoT components, condition reports to the overall system are important. In order to observe the system behaviour, several components are monitored (an industrial device (M3), the translator, the IIoT gateway, the MQTT broker and the cloud database) using the MSCV framework.

Standard evaluation to extract MSIs

In section we have presented the metric model and a set of MSIs, MSFIs and MOIs extracted from security, safety and organizational standards based on the access control requirement (see Figure 3). For our research work, in order to build a prototype of the MSCV framework we have used several open-source components and software: (i) the OpenStack cloud platform, which works with open-source technologies and makes it ideal for building, testing and investigating the use case and the MSCV framework; (ii) check_mk, as a comprehensive monitoring tool for configuring the platform independently of the monitoring core, (iii) Nagios plugins, which offer several ways to monitor MSIs in the target system and are compatible with check_mk.

Several standards are analyzed, as shown in Table 5. After a comparison based on the layer that they address in IIoT environments and the metric description, we have selected the ISO 27002 and IEC 62443-3 standards to check the security compliance. Taking these advantages in consideration, we have selected three MSIs from ISO 27002 and five MSIs from IEC 62443-3 to implement in our solution.

For each MSI is provided the following information:

Access to Networks and Network Services

- [**ID**] MSI 1.1
- [**Name**] Access to networks and network services
- [**Source**] ISO/IEC 27002
- [**Definition**] Users should only be provided with access to the network and network services that they have been specifically authorized to use. Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's information security management and control
- [**Monitoring Solution**] The plugin checks if there are established procedures/configuration for determining the access to specific network and network services

Management of Removable Media

- [**ID**] MSI 10.1
- [**Name**] Management of removable media
- [**Source**] ISO/IEC 27002
- [**Definition**] The control system shall provide the capability to automatically enforce configurable usage restrictions that include: (i) preventing the use of portable and mobile devices, (ii) requiring context specific authorization (iii) restricting code and data transfer to/from portable and mobile devices
- [**Monitoring Solution**] The plugin checks if transfer to/from portable devices (e.g., USB) are disabled

Secure Boot

- [**ID**] MSI 12.1
- [**Name**] Secure boot
- [**Source**] ISO/IEC 27002
- [**Definition**] Secure boot attestation of the firmware (immutable or cryptographically protected bootstrap code executed at power on) and UEFI or U-Boot bootloaders for multi-stage boot may be performed using PKCS standards based cryptographic key hashes. This extends the platform-level attestation from bootstrap to OS startup, and assists in the prevention of unauthorized firmware, bootloader or boot image updates over-the-air or over-the-network
- [**Monitoring Solution**] The plugin checks probes if the system uses Unified Extensible Firmware Interface.

Unique Identification and Authentication

- [**ID**] MSI 3.2
- [**Name**] Unique identification and authentication
- [**Source**] IEC 62443-3
- [**Definition**] The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices)
- [**Monitoring Solution**] The plugin checks if each account has a unique username and is protected via a password

Hardware Security for Public Key Authentication

- [**ID**] MSI 4.2
- [**Name**] Hardware security for public key authentication
- [**Source**] IEC 62443-3
- [**Definition**] The control system shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations (e.g. TPM)
- [**Monitoring Solution**] The plugin checks if the system/device is using Trusted Platform Module or security controller to store the keys

Use Control for Portable Devices

- [**ID**] MSI 7.2
- [**Name**] Use control for portable devices
- [**Source**] IEC 62443-3
- [**Definition**] The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices
- [**Monitoring Solution**] The plugin checks if removable media such as USB are disabled

Time Stamps

- [**ID**] MSI 11.2
- [**Name**] Time stamps
- [**Source**] IEC 62443-3
- [**Definition**] Timestamps (including date and time) of records should be generated using internal system clocks
- [**Monitoring Solution**] The plugin checks if the NTP is enabled including internal time synchronization and protection of time source integrity

Communication Integrity

- [**ID**] MSI 13.2
- [**Name**] Communication integrity
- [**Source**] IEC 62443-3
- [**Definition**]The control system shall provide the capability to protect the integrity of transmitted information. Depending on the context (for example transmission within a local network versus transmission via untrusted networks) and the network type used in the transmission feasible and appropriate mechanisms will vary
- [**Monitoring Solution**] The plugin checks if the system is using TLS for secure communication

Security Standard Compliance Verification

In order to understand the security compliance, it is important to first show the difference with security. Security is the mechanism to protect devices and systems against unauthorized access and manipulation. Security compliance refers to the fulfillment of requirements and measurable indicators, defined in security standards or best practice guidelines. To show the functionality of the MSCV framework we investigate the compliance of the proposed use case considering ISO27002 and IEC 62443-3 based on the access control requirement and a set of MSIs.

Each MSI extracted from the standards 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. Therefore, the EGM sends to the compliance module for each MSI the source from which the metric is extracted, e.g., for [MSI-1.1] the source is S1 - ISO27002, a binary value ”1” or ”0” that indicates if the metric is fulfilled or not, in this case ”1” for monitoring value ”OK” or ”0” for monitoring value ”CRITICAL”.

As illustrated in Figure 6, after gathering all the required evidence from the EGM module, the compliance module first verifies the compliance [%] for a single standard based on equation 1 in section . Than it verifies the total compliance [%] based in equation 2 at section .

For the presented use case we consider two scenarios:

Scenario I
The first scenario considers: (i) five main components of the use case, (ii) two standards and (iii) a set of representative MSIs to calculate the standard compliance of the target system (IIoT use case). As shown in figure 8, the MQTT broker fulfill only [MSI 1.1], [MSI 10.1], [MSI 3.2], [MSI 7.2], [MSI 11.2] and [MSI 13.2]. Based on the fulfilled metrics the compliance of this component is 75% and the overall security compliance of the use case is 63% based on the monitored metrics of ISO27002 and IEC 62443-3.

Scenario II
The second scenario considers:(i) five main components of the use case, (ii) two standards and (iii) a set of representative MSIs to calculate the standard compliance of the target system (IIoT use case). As shown in figure 8, the MQTT broker does not fulfill any of the identified MSIs. Based on these metrics the compliance of this component is 0% and the overall security compliance of the use case is 48% based on the monitored metrics of ISO27002 and IEC62443-3.

In the above scenarios, components such as the industrial device and the cloud database need more security controls integrated, whereas the IIoT gateway has already in place most of the required security controls extracted from the standards. Thus, it is possible not only to verify the current standard compliance of the system but also to identify the components, which need more security controls integrated in order to improve the overall compliance of the target system. The same approach applies also for safety with MSFIs and organizational standards with MOIs.

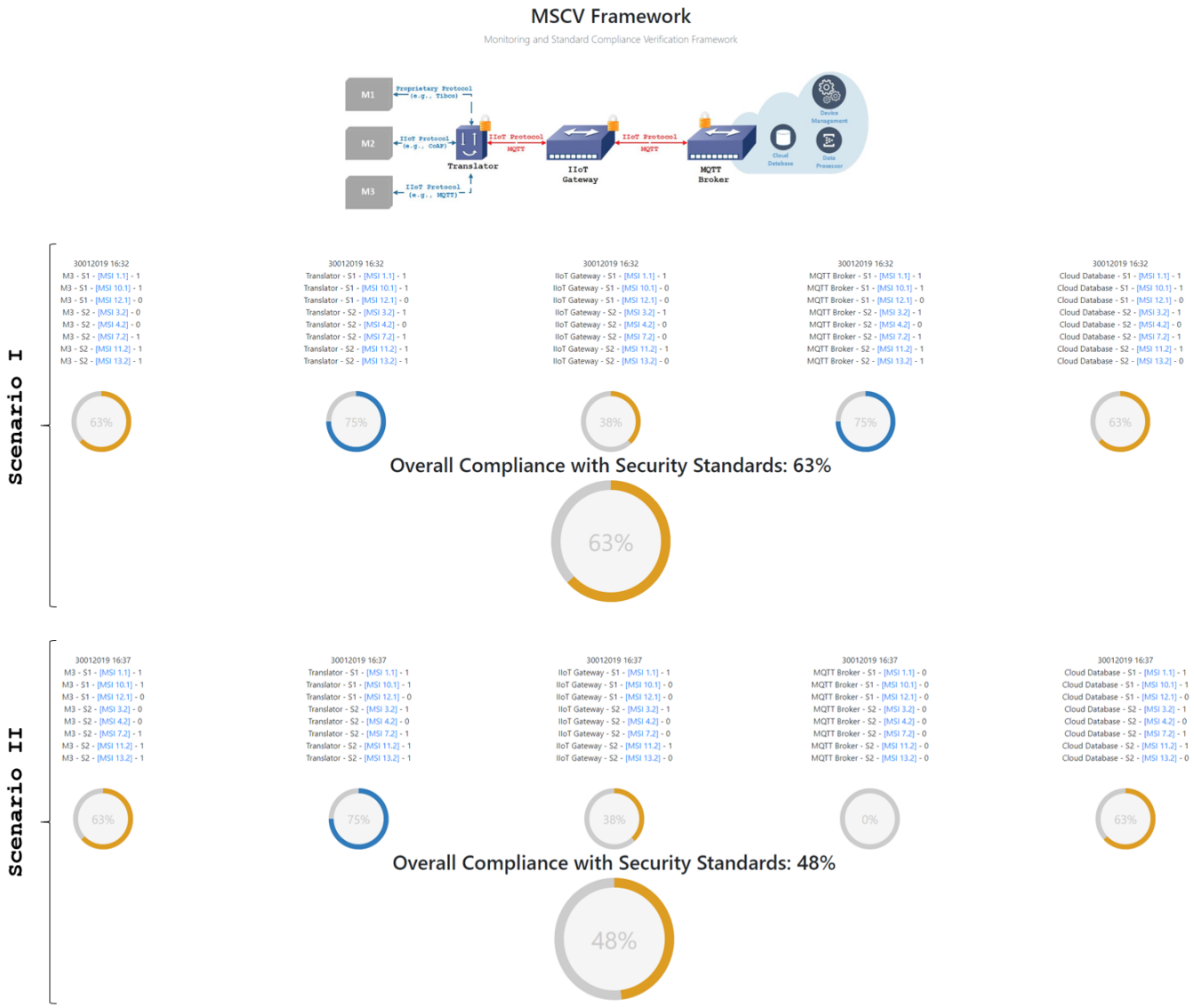

Figure 8. The component/overall compliance check for the end-to-end communication use case based on a set of metrics extracted from the security standards

Conclusion

The digitalization of industrial production will bring new challenges to the existing manufacturing systems. Despite this evolution, security, safety and organizational aspects, especially compliance to existing standards, remain an issue for large scale adoption in the production environment.

In this paper we have presented a MSCV framework. Initially, a high level description of the approach and architecture is provided, where are identified three main components in order to build an automated compliance framework: (i) monitoring agents, (ii) EGM module and (iii) compliance module. After identifying the components, we implement them to develop the MSCV framework in an OpenStack cloud platform, using check_mk, existing plugins, and customized scripts for the monitoring agents. We have also described a metric model used to identify requirements, standards and extract MIPs. The MIPs are classified in MSIs, MSFIs and MOIs and the information is used as an input for the MSCV framework. The framework provides a component or system compliance based on the evaluated standards and the extracted MIPs. The framework shows the compliance of an IIoT use case based on the access control requirement. To show the security compliance are evaluated ISO 27002 and IEC 62443-3 standards and a representative set of MSIs is extracted. The MSIs are monitored in five components of the use case and the overall compliance of the target system is shown in two scenarios: (i) one of the components fulfill most of the MSIs and (ii) the component does not fulfill any of the MSIs. As part of our future work, we will evaluate the MSCV framework for other standards to extract more MIPs that are relevant for the production environment and we will investigate if the metrics are machine readable. We will also investigate the integration of the MSCV in the Arrowhead Framework (1), which is a SoA framework addressing the move from large monolithic organizations towards multi-stakeholder cooperations with the aim to enable sustainability, flexibility, efficiency and competitiveness. The MSCV will be used by Arrowhead to check standard compliance of new devices, systems and services that interact with the Arrowhead framework.

Acronyms

Acronym	Reference Abbreviation
AICPA	American Institute of Certified Public Accountants
ARF	Asset Reporting Format
ATT	Arrowhead Test Tool
BPM	Business Process Management
BPEL	Business Process Language
BPSL	Business Property Specification Language
CCM	Cloud Control Matrix
CEN	European Committee for Standardization
COSO	Committee Sponsoring Organizations of Treadway
COPRAS	Cooperation Platform for Research And Standards
CPE	Common Platform Evaluation
CSA	Cloud Security Alliance
CVE	Common Vulnerability and Exposures
CWE	Common Weakness Enumeration
DDoS	Distributed Denial-of-Service
EGM	Evidence Gathering Mechanism
ETSI	European Telecommunication Standards Institute
GRC	Governance, Risk, Compliance
HARM	Hierarchical Attack Representation Model
HIISP	Healthcare Information Technology Standards Panel
ICS	Industrial Control System
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IIoT	Industrial Internet of Things
ISO	International Standards Organization
ISA	Instrument Society of America
ISOP	Information Security Organizational Policies
LTL	Linear Temporal Logic
MDA	Model Driven Architecture
MEA	Monitor Evaluate and Assess
MIP	Measurable Indicator Points
MOI	Measurable Organizational Indicator
MQTT	Message Queuing Telemetry Transport
MSI	Measurable Security Indicator
MSCV	Monitoring and Standards Compliance Verification
MSFI	Measurable Safety Indicator
MTBF	Mean Time Between Failures
NSQHS	National Safety and Quality Health Service
OCEG	Open Compliance and Ethics Group
OMG	Object Management Group
OPA	Open Process Analyzer
OVAL	Open Vulnerability and Assessment Language
PKCS	Public Key Cryptography Standards
PLC	Programmable Logic Controller
PRM	Process Reference Model
SBT	Social Bond Theory
SCAP	Security Content Automation Protocol
SC	Subcommittees
SoA	Service Oriented Architecture
SOC	Service Organization Control
TC	Technical Committees
UCF	Unified Compliance Framework
UEFI	Unified Extensible
UNL	Unified Modelling Language
XCCDF	Extensible Configuration Checklist Description
WG	Working Group

Acknowledgements

Research leading to these results has received funding from the EU ECSEL Joint Undertaking under grant agreement No 737459 - Productive4.0 project and grant agreement No 826452 - Arrowhead Tools project.

References

[1] Delsing J. *Iot automation: Arrowhead framework*. CRC Press, 2017.

[2] Karnouskos S, Colombo AW, Bangemann T et al. A soa-based architecture for empowering future collaborative cloud-based industrial automation. In *IECON 2012-38th Annual Conference on IEEE Industrial Electronics Society*. IEEE, pp. 5766–5772.

[3] Boyes H, Hallaq B, Cunningham J et al. The industrial internet of things (iiot): An analysis framework. *Computers in Industry* 2018; 101: 1–12.

[4] Ding D, Han QL, Xiang Y et al. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* 2018; 275: 1674–1683.

[5] Samtani S, Yu S, Zhu H et al. Identifying supervisory control and data acquisition (scada) devices and their vulnerabilities on the internet of things (iot): a text mining approach. *IEEE Intelligent Systems* 2018; .

[6] Wurm J, Hoang K, Arias O et al. Security analysis on consumer and industrial iot devices. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, pp. 519–524.

[7] Falco G, Caldera C and Shrobe H. Iiot cybersecurity risk modeling for scada systems. *IEEE Internet of Things Journal* 2018; 5(6): 4486–4495.

[8] Kshetri N and Voas J. Hacking power grids: a current problem. *Computer* 2017; 50(12): 91–95.

[9] Liu Y, Wang Z and Li N. Characterizing the impact of ddos attack on inter-domain routing system: A case study of the dyn cyberattack. In *2018 International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)*. Atlantis Press.

[10] Yeh E, Choi J, Prelcic N et al. Security in automotive radar and vehicular networks. *submitted to Microwave Journal* 2016; .

[11] TCCA. Importance of standard compliance in telecommunication. In *Standards White Paper v1.0*. TETRA and Critical Communications Association Critical Communications Broadband Group.

[12] Bicaku A, Schmittner C, Tauber M et al. Monitoring industry 4.0 applications for security and safety standard compliance. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, pp. 749–754.

[13] De Haes S, Van Grembergen W and Debreceny RS. Cobit 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems* 2013; 27(1): 307–324.

[14] Janvrin DJ, Payne EA, Byrnes P et al. The updated coso internal control integrated framework recommendations and opportunities for future research. *Journal of Information Systems* 2012; 26(2): 189–213.

[15] Lubell J. Using dita to create security configuration checklists. In *Balisage: The Markup Conference*.

[16] Waltermire D, Quinn S, Scarfone K et al. The technical specification for the security content automation protocol (scap): Scap version 1.2. *NIST Special Publication* 2011; 800: 126.

[17] Gapinski A. Cloud computing: Information security standards, compliance and attestation. In *Proceedings of International Conference on Engineering and Technologies (LACCEI). Santo Domingo. Retrieved from www. laccei. org*.

[18] Liu Y, Muller S and Xu K. A static compliance-checking framework for business process models. *IBM Systems Journal* 2007; 46(2): 335–361.

[19] Luna J, Ghani H, Germanus D et al. A security metrics framework for the cloud. In *Proceedings of the International Conference on Security and Cryptography*. IEEE, pp. 245–250.

[20] Mitchell S and Switzer CS. Grc capability model" red book" 2.0. *Open Compliance & Ethics Group, OCEG (April 2009)* 2009; .

[21] Cheng D, Villamarin J, Cu G et al. Towards end-to-end continuous monitoring of compliance status across multiple requirements. *International Journal of Advanced Computer Science and Applications* 2018; 9(12): 456–466.

[22] Ge M, Hong JB, Guttmann W et al. A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications* 2017; 83: 12–27.

[23] Racz N, Weippl E and Seufert A. A process model for integrated it governance, risk, and compliance management. In *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)*. Citeseer, pp. 155–170.

[24] Safa NS, Von Solms R and Furnell S. Information security policy compliance model in organizations. *Computers & Security* 2016; 56: 70–82.

[25] Fenz S and Neubauer T. Ontology-based information security compliance determination and control selection on the example of iso 27002. *Information & Computer Security* 2018; 26(5): 551–567.

[26] Wang L, Törngren M and Onori M. Current status and advancement of cyber-physical systems in manufacturing. *Journal of Manufacturing Systems* 2015; 37: 517–527.

[27] Bandyopadhyay D and Sen J. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications* 2011; 58(1): 49–69.

[28] Eichelberg M, Aden T, Riesmeier J et al. A survey and analysis of electronic healthcare record standards. *Acm Computing Surveys (Csur)* 2005; 37(4): 277–315.

[29] Blackford RW. Aerospace coating and treatment standards. *Metal finishing* 2003; 101(3): 14–24.

[30] Pelton JN. Future space safety technology, standards, and regulations. In *Space Safety Regulations and Standards*. Elsevier, 2010. pp. 397–406.

[31] Costa-Pérez X, Festag A, Kolbe HJ et al. Latest trends in telecommunication standards. *ACM SIGCOMM Computer Communication Review* 2013; 43(2): 64–71.

[32] Dodoo A, Gustavsson L and Sathre R. Building energy-efficiency standards in a life cycle primary energy perspective. *Energy and Buildings* 2011; 43(7): 1589–1597.

[33] Pigosso D, Ferraz M, Teixeira C et al. The deployment of product-related environmental legislation into product requirements. *Sustainability* 2016; 8(4): 332.

[34] Morris TH and Gao W. Industrial control system cyber attacks. In *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research*. pp. 22–29.

[35] Jang-Jaccard J and Nepal S. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences* 2014; 80(5): 973–993.

[36] Bicaku A, Maksuti S, Palkovits-Rauter S et al. Towards trustworthy end-to-end communication in industry 4.0. In *Industrial Informatics (INDIN), 2017 IEEE 15th International Conference on*. IEEE, pp. 889–896.

[37] Enterprises N. Nagios. https://exchange.nagios.org/directory, 2019.

[38] OpenStack-Wiki. Ceilometer, 2019.

[39] Olups R. *Zabbix 1.8 network monitoring*. Packt Publishing Ltd, 2010.

[40] Bicaku A, Balaban S, Tauber MG et al. Harmonized monitoring for high assurance clouds. In *Cloud Engineering Workshop (IC2EW), 2016 IEEE International Conference on*. IEEE, pp. 118–123.

[41] Maksuti S, Bicaku A, Tauber M et al. Towards flexible and secure end-to-end communication in industry 4.0. In *Industrial Informatics (INDIN), 2017 IEEE 15th International Conference on*. IEEE, pp. 883–888.

[42] Derhamy H, Eliasson J and Delsing J. Iot interoperability on demand and low latency transparent multiprotocol translator. *IEEE Internet of Things Journal* 2017; 4(5): 1754–1763.

[43] Bicaku A, Maksuti S, Hegedűs C et al. Interacting with the arrowhead local cloud: On-boarding procedure. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, pp. 743–748.

Notes

1. https://nvd.nist.gov/
2. https://www.w3.org/2004/copras/
3. http://www.arrowhead.eu/
4. http://seccrit.eu/
5. http://www.semi40.eu/
6. https://productive40.eu/
7. https://www.iso.org/standard/54533.html
8. https://webstore.iec.ch/publication/7033
9. https://www.iec.ch/functionalsafety/explained/
10. https://webstore.iec.ch/publication/24241
11. https://www.iso.org/standard/55142.html
12. https://www.iso.org/standard/63711.html

Author Biographies

Dipl-Ing 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 (AIT) 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 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 - Albania. Bicaku is a member of Austrian Electrotechnical Committee (OEK) of the Austrian Electrotechnical Association (OVE) at IEC and CENELEC standardization bodies within TC65-WG10 ”Security for industrial process measurement and control - Network and System Security”. He has been part of several EU projects, e.g., SECCRIT, SEMI40, PRODUCTIVE4.0, ArrowheadTools and Comp4Drones.

Prof.(FH) Dr. 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” 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.