

Security standard compliance and continuous verification for Industrial Internet of Things

Ani Bicaku^{1,2} , Markus Tauber¹ and Jerker Delsing²

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 Internet of Things and implements an automatic monitoring and standard compliance verification framework. In this work, we focus on security, safety, and organizational aspects of industrial Internet of Things. We identify a number of standards and best practice guidelines, which are used to extract security, safety, and organizational measurable indicator points. In addition, a metric model is provided 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 Internet of Things use case.

Keywords

Industrial Internet of things, Internet of things, security, safety, organizational, standard, compliance, monitoring, digitalization, Industry 4.0

Date received: 31 October 2019; accepted: 30 March 2020

Handling Editor: SookKyun Kim

Introduction

Digitalization and hyperconnectivity 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), cyberphysical systems (CPS), embedded systems, cloud computing, service-oriented architecture (SOA), and so on, provide all the enabling elements toward the fourth-industrial revolution—Industry4.0, which is reshaping the industrial landscape. The application of the IoT to manufacturing industry is called industrial Internet of Things (IIoT). IIoT makes 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. Without proper security measures,

¹University of Applied Sciences Burgenland, Eisenstadt, Austria

²Luleå University of Technology, Luleå, Sweden

Corresponding author:

Ani Bicaku, University of Applied Sciences Burgenland, Campus I, A-7000 Eisenstadt, Austria.

Emails: ani.bicaku@fh-burgenland.at; ani.bicaku@tu.se



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work

without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

intrusion attempts and non-authorized access will increase, resulting in higher costs, loss on sale, as well as leaks in critical data. Such leaks can interrupt, modify, or sabotage an operational process with the intention to cause harm. In response, governments and standardization bodies have published standards and regulations to help improving the security of industrial systems.⁴

In industrial environments, 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.^{5–7} The latest reported attacks, such as the Ukraine's power grid attack by the Industroyer malware, which caused 1 h collapse of systems responsible for serving Kiev with electricity;⁸ Dyn cyberattack,⁹ involving distributed denial-of-service (DDoS) attacks targeting systems operated by the domain name system (DNS) provider Dyn; the Jeep Cherokee Hack,¹⁰ where hackers were able to remotely control the brakes and steering of the vehicle; and Triton malware used to shut down an industrial process by exploiting weaknesses in industrial control system (ICS) are proof that the IIoT devices need a robust security to avoid any security issue. Non-authorized access into IIoT networks can lead to a loss in brand loyalty, reputation, revenue, or market share, and more depending on the nature and severity of the attack.

Given the above scenarios, many organizations want to implement scalable security standards that can be easily accessed 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 control systems to Industry4.0, by easily interfacing with existing legacy devices, plug-and-play systems, and algorithms, adapting their behavior and interactions on-the-fly.

Nowadays, we use standards in our everyday life—healthcare, telecommunication, transport, food, energy, and so on. 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 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 article 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 (MIPs), which are categorized as (a) measurable security indicators (MSIs), (b) measurable safety indicators (MSFIs), and (c) measurable organizational indicators (MOIs). The MIPs are documented in a metric model, which is used to efficiently extract meaningful information for the monitoring and standard compliance verification (MSCV) framework based on a set of requirements. In our previous work,¹² we have proposed the MSCV framework architecture and here we evaluate it in an IIoT use case to show the functionality and how it 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 article is organized as follows:

The section “Related Work” provides a review of existing standard compliance frameworks and tools including related research projects and scientific publications. In “Standardization Landscape” section, we present the overall standard landscape based on the role of standardization bodies and the importance of standard compliance in different industry aspects; next, in section “Standards and best practice guidelines evaluation” security, safety, organizational standards, and their dependability are evaluated. In section “Metric model,” we present the evaluated standards including requirements, standards, and metrics. In the section “MSCV framework—architecture” the MSCV framework and its architecture are introduced, which are evaluated in section “IIoT use case.” We conclude our work in section “Conclusion.”

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 and compliance to these standards. In the last years, several frameworks and tools have been published and a number of European projects addressing Industry 4.0 are funded.

Standard compliance frameworks and tools

The frameworks and tools presented in this section are selected based on their ability to be used in IIoT applications and lightweight capabilities (size and resource usage during execution). Another selection criterion is their ability to perform real-time assessment and artifacts collection about the monitored systems including documentation. The most popular tools and frameworks are listed as follows:

- Cobit-5** framework^{13,14} 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 behavior; 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: (1) Cobit 5 framework, which describes the framework, including enablers; (2) Cobit 5 enabling process, where best practices used day-by-day are documented; and (3) Cobit 5 implementation, which provides the methodology for continuous improvement of IT governance.
- Committee Sponsoring Organizations of Treadway (COSO)** framework^{15,16} is a 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 consists 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 but no specification or detailed implementation.
- OpenSCAP** framework¹⁷ is based on the security content automation protocol (SCAP)¹⁸ 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) extensible configuration checklist description format (XCCDF), a language used to describe the security checklist, (ii) open vulnerability and assessment language (OVAL), a language to make logical statement, (iii) DataStream that packs the other components into a single file, (iv) asset reporting format (ARF), known as the result data stream, (v) common platform evaluation (CPE), used to identify platforms and systems using unique defined names, (vi) common vulnerability and exposures (CVEs), a reference for known vulnerabilities, and (vii) common weakness enumeration (CWE), a list of software weaknesses to describe known security weaknesses and flaws. The framework makes use of the National Vulnerability Database by loading CVE feed, which are updated by the vendors of enterprise operating systems based on their new releases (<https://nvd.nist.gov/>). OpenSCAP loads the CVE feed and compares every item in the feed with system packages. This is an efficient way to check the packages installed by an official source. It supports SCAP standard version 1.2 and is compatible with other SCAP 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 shared library. On the top of the library, the OpenSCAP scanner is built, which is a command line tool with plenty of features. OpenSCAP supports online and offline evaluation. The disadvantage of this evaluation is that it is not possible to fix system issues in the read-only mode.
- Service Organization Control (SOC)** compliance,^{19,20} created by American Institute of Certified Public Accountants (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 control over financial statement and reporting. SOC 2 covers the controls of

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 trust criteria (security, availability, integrity, confidentiality, and privacy). SOC 2 includes two reports: (a) type 1 describing the system and suitability of the system design and (b) type 2 describing the system and operating effectiveness of the controls.

- **Open process analyzer (OPA)**²¹ is a compliance framework, which checks process models against compliance rules based on modeling languages. Since business process management (BPM) does not check which processes are compliant and which are not, they introduce a compliance checking method including six steps: (i) model business processes using business process language (BPEL), (ii) business property specification language (BPSL) to specify compliance rules, (iii) transform the BPEL into representation process using π -calculus, (iv) BPSL compliance rules are transformed into linear temporal logic (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 constraints related to these processes.
- **Cloud Security Alliance - Cloud Control Matrix (CSA CCM)** framework^{22,23} provides fundamental security principles to guide cloud vendors and assist prospective cloud customers in determining the security risk of a cloud provider. It 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.

- **Governance, Risk, Compliance (GRC)** capability model^{24,25} developed by the Open Compliance and Ethics Group (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.

In Table 1, we show the comparison and evaluation of compliance frameworks and tools based on their abilities to address important features in an IIoT environment. They all consider real-time operations and need human intervention in order to read the results of the compliance, except OpenSCAP. All the evaluated frameworks/tools have significant documentation about the procedure during compliance check. All the evaluated frameworks and tools fail in providing metric classification and single component compliance, and also, not all of them are open-source and do not give the possibility to write own scripts. COSO, OpenSCAP, and CSA CCM are compliant to standards but only to specific standards, the user cannot add other standards.

European projects and standardization in IIoT

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

Table 1. Compliance frameworks and tools evaluation.

	Cobit 5	COSO	OpenSCAP	SOC	OPA	CSA CCM	GRC
Real-time support	+	+	—	+	+	+	+
Resource availability	—	—	+	—	+	—	—
Open-source	—	—	+	—	+	—	—
Standards	—	+	+	—	—	+	—
Human intervention	+	+	—	+	+	+	+
Metric classification	—	—	—	—	—	—	—
Component compliance	—	—	—	—	—	—	—
Documentation	+	+	+	+	+	+	+
Standard-based controls	+	—	+	—	—	+	—
Automatic compliance	—	—	+	—	—	—	—

COSO: Committee Sponsoring Organizations of Treadway; SOC: service organization control; OPA: open process analyzer; CSA: cloud security alliance; CCM: cloud control matrix; GRC: governance, risk, compliance.

projects based on their relation to IoT, digitalization, and Industry 4.0 application scenarios, and also for their impact in the industrial production to enhance transparency of data for overall efficiency.

COPRAS project had the scope to bring together and exchange information between research and information and communication technology (ICT) standards by encouraging projects to engage in standards activity to stimulate their dissemination and usage (<https://www.w3.org/2004/copras/>).

Arrowhead project had the objective to address the technical challenges associated with automation (<http://www.arrowhead.eu/>). The project has evaluated and used several security and safety standards with the aim to standardize the Arrowhead Framework, which is continued in the Productive4.0 project.

SECCRIT 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 (<http://secrit.eu/>). Several standards and frameworks are used (e.g. Cobit-5 and GRC). As a result, a cloud evaluation method is developed based on metrics extracted from these standards.

Semi40 project focuses on smart production and cyber physical production by providing tools and methodologies for system integration of smart device capabilities such as sensing, communication, knowledge management, decision-making, control, and actuation, resulting in smart maintenance and smart production execution (<http://www.semi40.eu/>). The project focuses on 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. CSA CCM framework is used to provide security metrics for the backend infrastructure.

Productive4.0 project aims to achieve significant improvement in digitalizing the European industry by means of electronics and ICT (<https://productive40.eu/>). 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—several compliance frameworks are evaluated within this project including the frameworks listed in this work.

Scientific publications

Existing works, such as Cheng et al.,²⁶ Ge et al.,²⁷ Racz et al.,²⁸ and Safa et al.,²⁹ outline the issues with manual compliance audits and the need for humans to interpret these documents.

- In Cheng et al.,²⁶ the authors group the compliance monitoring tools as (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, an enhanced compliance ontology for requirements based on natural language processing tools that are used to structure the information and populate the ontology is proposed. 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 using ontology definitions focusing on the concepts written in compliance documents.

- A framework for automating security analysis of the IoT is introduced in Ge et al.²⁷ 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,²⁸ where a process model for integrated IT GRC 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 work shows that IT GRC processes can be integrated based on their commonalities. However, the processes do not describe in detail how the integration will look like or which technologies are used.
- Safa et al.²⁹ 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 (SBT) 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 SBT, such as attachment, commitment, and personal norms. The aim is to check how information security compliance arises in organizations by showing how employees comply with organizational information policies. The results of the analysis confirmed that information security sharing has strong effects toward 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 International Standards Organization (ISO) 27002 is presented in Fenz and Neubauer.³⁰ 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 ISO 27002 standard. However, they considered only one standard and they do not check any dependency between security, safety, and organizational aspects.
- Susanto and Almunawar³¹ show the importance of standard compliance and propose the information security framework (ISF). The framework is a semi-automated tool developed to assist organizations to assess their compliance with ISO 27001. It has two major modules: e-assessment to assess the level of compliance and e-monitoring to monitor the activities.

Moreover, other approaches, such as Theoharidou et al.,³² Calder and Watkins,³³ and Vladimirov et al.,³⁴ concentrate on describing the importance and structure of a compliance framework, but fail, in general, to describe 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 straightforward, 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. To fill this gap, this article 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 all the MIPs of the standards have been implemented, 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 ICT 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.³⁵ This section describes the standardization bodies and the role of their standards in different domains.

Role of standardization bodies

The IoT community has a large number of standards and standardization bodies. We have listed below the most important organizations, which have the aim to produce standards in numerous application areas. In order to show the importance of standard compliance, it is important to know from which groups of interest they are drafted and published (Figure 1).

ISO 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 (TC), subcommittees (SC), and working groups (WCs) of experts appointed by ISO.

International Electrotechnical Commission (IEC) is a not-for-profit, quasi-governmental organization with

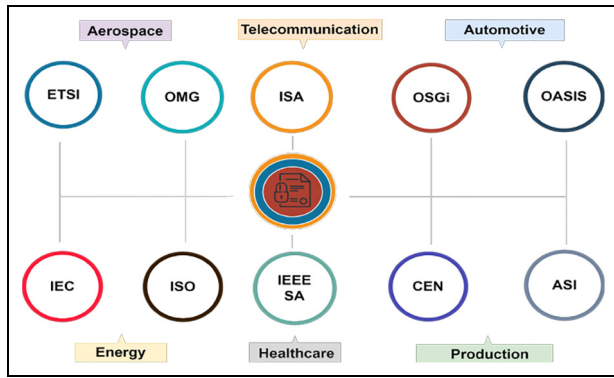


Figure 1. International standardization bodies.

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 TC and SC and about 700 project teams carry out the standards work.

Institute of Electrical and Electronics Engineers Standard Association (IEEE-SA) 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 standard-related collaboration. Within more than 160 countries, they promote innovation, enable the creation and expansion of international markets, and help protect safety.

European Committee for Standardization (CEN) 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, and so on.

European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization in the telecommunication 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 standards or ICTs, including fixed, mobile, radio, broadcast, and Internet technologies.

Object Management Group (OMG) 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 (UML) and model driven architecture (MDA) to enable visual design, execution, and maintenance of software and other processes.

Instrument Society of America (ISA) 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.

Open service gateway initiative (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.

Organization for the Advancement of Structures Information Standards (OASIS) is a non-profit 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 5000 participants representing about 600 organizations and individual members in more than 65 countries.

Accellera Systems Initiative (ASI) 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 technologies that are balanced, open, and benefit the worldwide electronics industry. Leading companies and semiconductor manufacturers 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 technology development and are an

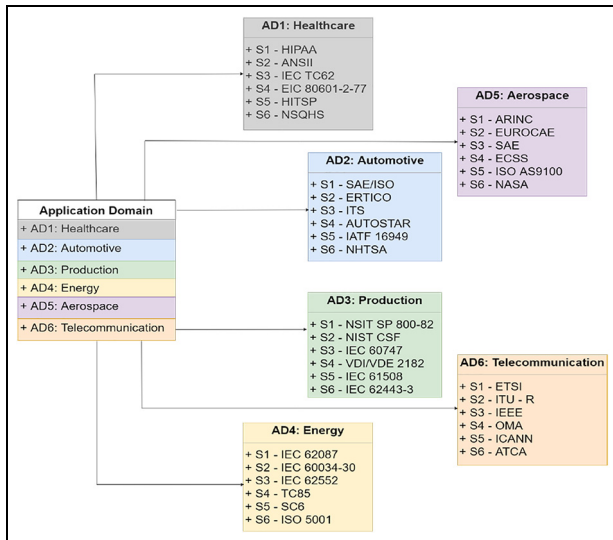


Figure 2. Standards in different application domains.

essential resource for researchers in different aspects.³⁶ 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 their importance. The importance of standard compliance for different industry domains is presented below.

Healthcare: Standard compliance in healthcare can cover a wide variety of practices and observe internal and external rules, but most healthcare compliance issues are related to patient safety, the privacy of patient information, and billing practices (e.g. health insurance portability and accountability act (HIPAA) and healthcare information technology standards panel (HITSP)).³⁷ 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 does not 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 and IEC 80601-2-77). 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. international automotive task force (IATF) 16949). Other important aspects are the safety and environmental regulations such as national highway traffic safety administration (NHTSA) standard. Automobile parts, such as tires, brakes, and gears, are subject to standardization in order to prevent accidents. In this industry, standards and regulations aim also to reduce the emission of CO₂, NO₂, noise, and 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 (unmanned aerial vehicle (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 European Organisation for Civil Aviation Equipment (EUROCAE) and ISO AS9100, can have several benefits for aerospace manufacturers and suppliers.³⁸ Another important aspect is the air traffic management,³⁹ used to maintain the distance between aircrafts, safety on ground, and to regulate the flow of the aircraft (e.g. aeronautical radio, incorporated (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 international telecommunication union radiocommunication (ITU-R), European Telecommunications Standards Institute (ETSI), and Internet Corporation for Assigned Names and Numbers (ICANN), allow systems to work locally and globally.⁴⁰ 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 and also to deny the sale of products that are less energy efficient than the minimum standard requirements.⁴¹ 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.⁴² 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, and so on.

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. 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.

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 are summarized.

Security standards

The evaluated security standards and best practice guidelines particularly focus on operational security and organizational aspects, as shown in Table 2.

Every standard has a specific focus, for example, if we consider ISO 270xx series of standards—if the scope is to use the framework for information security, the ISO 27001 standard is required; if the scope is to implement controls, ISO 27002 standard is required; if the scope is to have risk assessment, the ISO 27005 standard is required; and if it is needed to secure the information in cloud, the ISO 27017 standard is required. However, some of them also consider organizational and safety aspects.

Table 2. Security standards.

	NIST SP 800-82	NIST SP 800-184	NIST CSF	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27005	ISO/IEC 27017	ISO/IEC 15408	CCSC	NISPOM	CTP	CSA-ICS	NAMUS NA115	VDI/VDE 2182	IEC 62443-3-3
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

NIST: National Institute of Standards and Technology; SP: security publication; CSF: cybersecurity framework; ISO: International Standards Organization; IEC: International Electrotechnical Commission; NISPOM: National Industrial Security Program Operating Manual; CSA: cloud security alliance; ICS: industrial control system; CCSC: CIS critical security controls for effective cyber defense; CTP: cloud trust protocol; NAMUS-NA 115: user association of automation technology in process industries; VDI/VDE: verband der elektrotechnik, elektronik und informationstechnik.

Safety standards

Table 3 shows that safety standards and best practice guidelines, such as IEC 61508, IEC 61511, and American National Standards Institute (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.

Table 3. Safety standards.

	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

IEC: International Electrotechnical Commission; ANSI: American National Standards Institute; ISA: Instrument Society of America.

Process management standards

The process management standards mostly focus on organizational, but some consider other aspects (Table 4).

ISO/IEC TS 33052 uses ISO/IEC 27001 security requirements to define a process reference model (PRM) for the domain of information security. ISO/IEC/IEEE 15288 provides technical management processes, for example, risk management process.

Table 4. Process management standards.

	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

ISO: International Standards Organization; IEC: International Electrotechnical Commission; TS: technical specification; IEEE: Institute of Electrical and Electronics Engineers.

Discussion

This section provides a summary of the most relevant existing standards and best practice guidelines related to (a) security, (b) process management, and (c) safety. The purpose of this evaluation is to get a better overview of gaps and overlaps in the current state of the art related to security, organizational, and safety issues, and also to know what domain do they address in an IIoT end-to-

end communication—from the edge devices to the back-end infrastructure.

In Table 5, a summary of the evaluation of standards and best practice guidelines is presented. 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, programmable logic controller (PLC)), communication layer (e.g. data exchange, protocols, and gateways), and backend infrastructure (e.g. cloud services).

- “0” stands for the standard/best practice guideline that does not focus or does not address the specific layer at all.
- “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 National Institute of Standards and Technology (NIST) security publication (SP) 800-82, NIST cybersecurity framework (CSF), ISO/IEC 27001:2013, CC, National Industrial Security Program Operating Manual (NISPOM), CSA-ICS, NA115, and VDI/VDE 2182 consider the operational security of IIoT devices but in most of them a step-by-step guideline how to achieve the intended goals is missing. 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, and other standards, such as ISO/IEC 27017, european union agency for cybersecurity (ENISA), and cloud service level agreement standardization guideline (C-SIG), mainly focus on operational security issues in cloud platforms and cloud services.

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 back-end infrastructure. Therefore, based on this evaluation, we conclude that a set of measurable security, safety, and organizational metrics from different standards are needed 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 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.⁴³ Therefore, each industrial organization must understand the potential risks of a production environment, no longer isolated from the Internet and puts the system at a security risk.⁴⁴

Table 5. Standards and best practice guidelines evaluated based on security, organizational, and safety aspects in IIoT.

	NIST SP 800-82	NIST SP 800-184	NIST CSF	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27005	ISO/IEC 27017	ISO/IEC 15408	CCSC	NISPOM	CTP	CSA-ICS	NAMUS-NAI 15	VDE 2182	IEC 62443-3-3	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
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
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
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

NIST: National Institute of Standards and Technology; SP: security publication; CSF: cybersecurity framework; ISO: International Standards Organization; IEC: International Electrotechnical Commission; NISPOM: National Industrial Security Program Operating Manual; CSA: cloud security alliance; ICS: industrial control system; TS: technical specification; IEEE: Institute of Electrical and Electronics Engineers; ANSI: American National Standards Institute; ISA: Instrument Society of America; CTP: cloud trust protocol; NAMUS-NA I 15: user association of automation technology in process industries; VDI/VDE: Verband der elektrotechnik, elektronik und informationstechnik.

Toward addressing this challenge, in this article, a metric model is presented, as shown in Figure 3. The metric model is used as input for the MSCV framework (explained in the next 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, an ID, name, and sources from where this specific metrics is extracted are provided.

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.⁴⁵

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 as MSI, MSFI, and MOI, respectively.

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 addressing the access control requirement in the evaluated standards. In order to map the requirements, standards, and security metrics in the metric 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 six standards in total, two for each classification:

Security standards: ISO/IEC 27002 with 12 metrics and IEC 62443-3-3 with 15 metrics.

Safety standards: IEC 61508 with two metrics and IEC 61511 with six metrics.

Organizational standards: ISO/IEC-TS 33052 with 13 metrics and ISO/IEC/IEEE 15288 with four metrics. This is a simple representative example, which can be used as input for the MSCV framework. In the next section, we show the MSCV architecture and how the component of a system is checked for standard compliance verification. In the

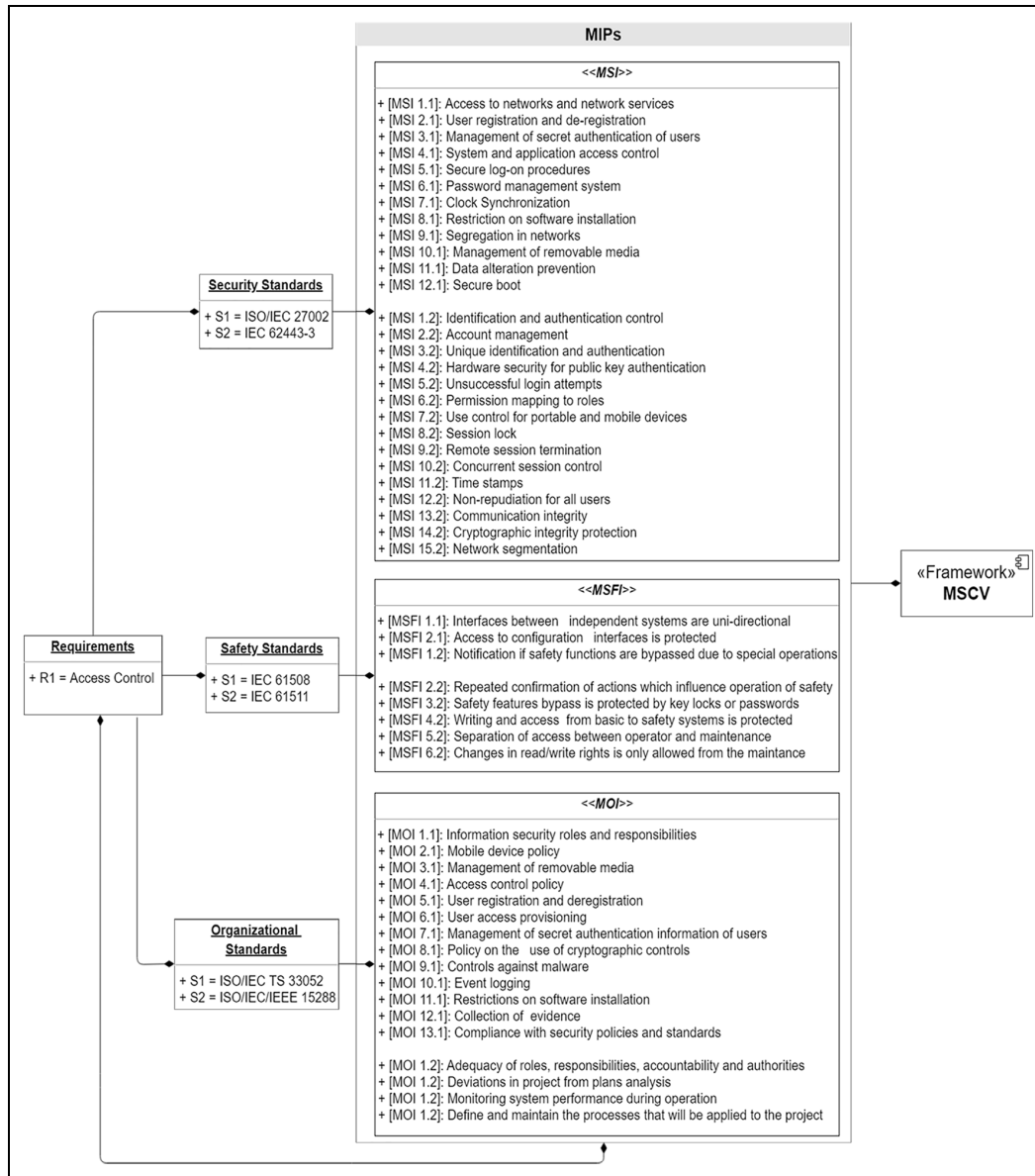


Figure 3. Example showing the usage of the metric model for security, safety, and organizational standards considering the access control requirement.

section “IIoT use case,” we show examples of the documentation of each metric with ID, name, source, definition, and monitoring possibility.

Monitoring and standard compliance verification framework - MSCV architecture

Figure 4 shows the architecture of the MSCV framework, which is developed as a composition of different components gathered in three core parts: (a) monitoring agents, (b) evidence gathering mechanism (EGM), and (c) compliance module. The MSCV architecture is explained in our previous work.¹² In this article, we

provide a high-level view of the steps to check the compliance of a specific standard.

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 from different plugins (e.g. Nagios,⁴⁶ Ceilometer,⁴⁷ Zabbix,⁴⁸ etc.) customized scripts. The collected data are fed to the EGM.

The EGM is designed to acquire, store, and analyze the security, safety, and organizational related evidence.⁴⁹ 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, a monitoring

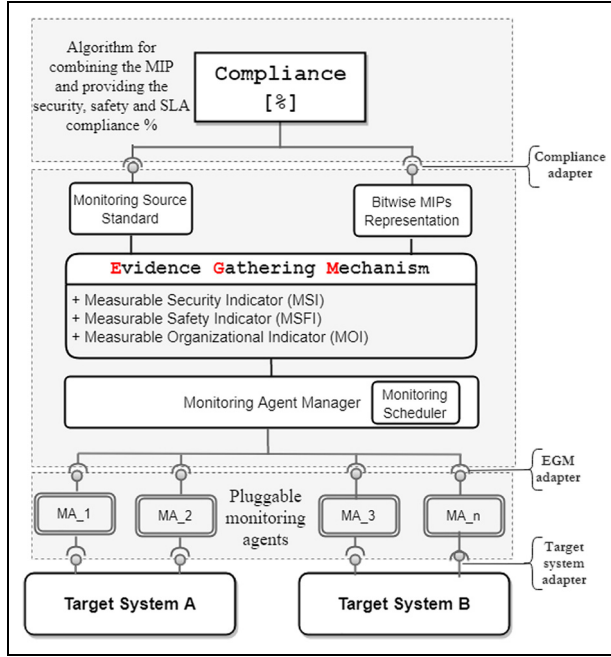


Figure 4. Monitoring and standard compliance verification framework used to measure, aggregate, schedule, store, retrieve, and analyze the monitoring data to provide standard compliance.

source standard to map the specific standard with each monitored metric and a bitwise MIP representation module that represent each metric by a binary number are included. This is the core part of the MSCV framework, where the knowledge regarding MIPs and standards lies. 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 EGM the source where 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 a weight value for each MSI to indicate the importance in range [0, 1] as shown in Figure 6.

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 is the number of metrics per standard, m is the number of standards, $MSI_{i,j}$ is the measured value of “ i ” security metric from “ j ” standard, and $\omega_{i,j}$ is the 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 7.⁵⁰ 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).

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 message queuing telemetry transport (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 translator⁵¹ to be able to communicate via IIoT protocols.

In such a scenario, with different IIoT components, condition reports to the overall system are important. In order to observe the system behavior, 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 the previous section, we have presented a metric model and a set of MSIs, MSFIs, and MOIs extracted

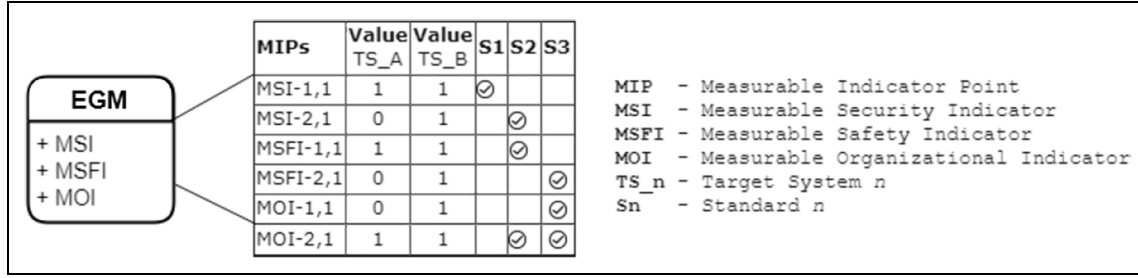


Figure 5. A representative set of the information provided by the EGM module.

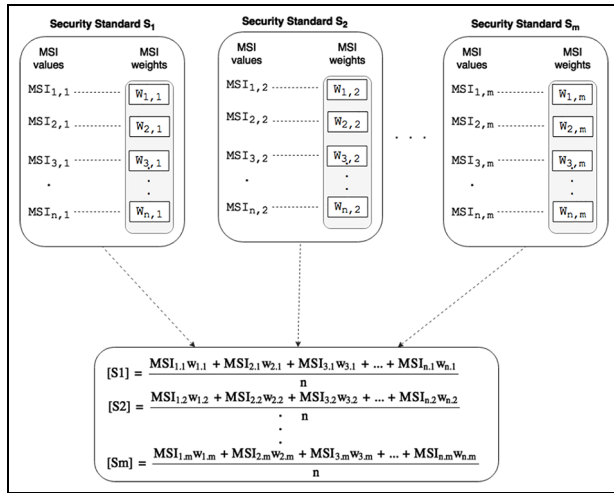


Figure 6. Security standard compliance verification.

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, and (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 62443-3-3 standards to check the security compliance. Taking these advantages in consideration, we have selected three MSIs from ISO 27002 and five MSIs from IEC 62443-3-3 to implement in our solution. For each MSI, the following information is provided: (i) ID, (ii) name, (iii) source, (iv) definition, and (v) monitoring solution.

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, for example, 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 (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 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

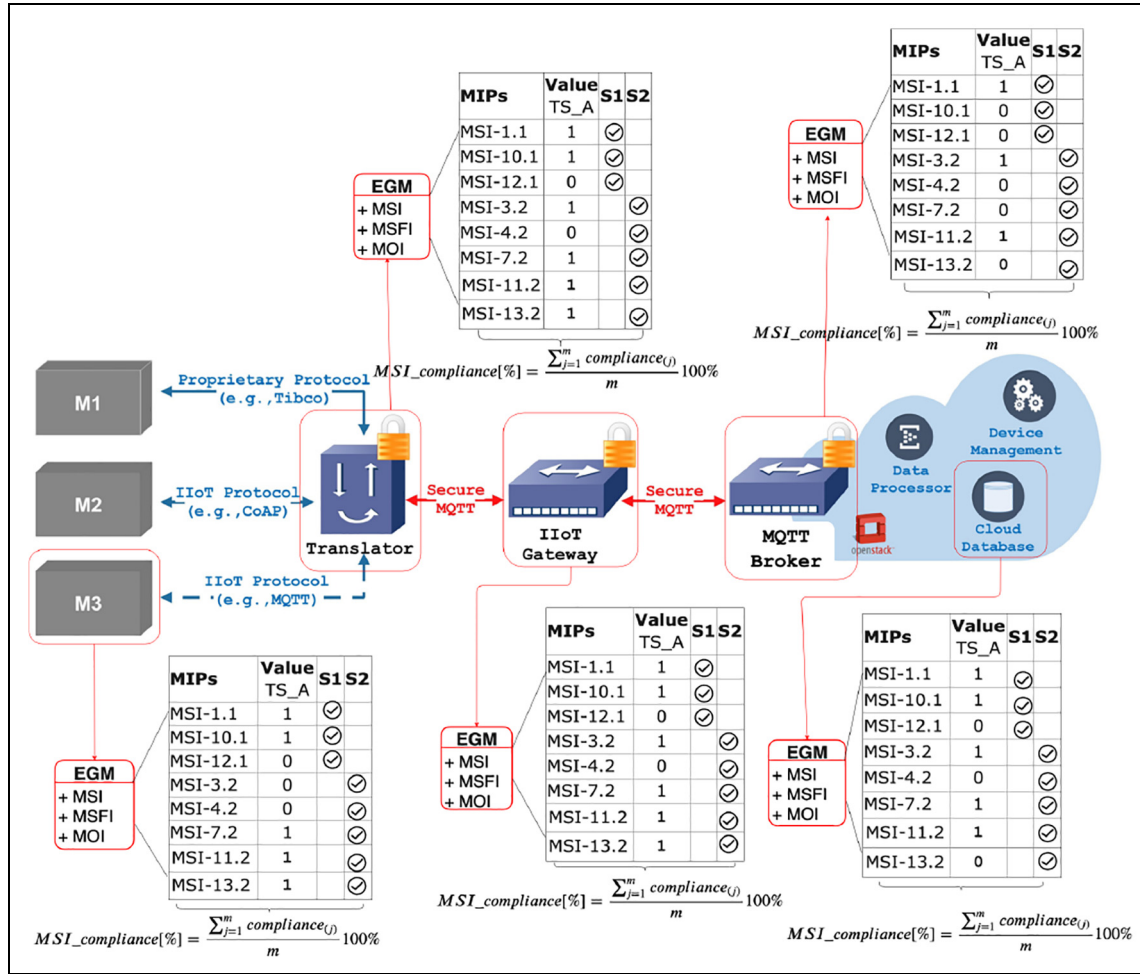


Figure 7. The end-to-end communication use case used to check the overall compliance of the system based on five components and two security standards.

bootstrap code executed at power on) and unified extensible firmware interface (UEFI) or U-Boot bootloaders for multi-stage boot may be performed using public key cryptography standards (PKCS) 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 UEFI.

Unique identification and authentication

- **[ID]** MSI 3.2.
- **[Name]** Unique identification and authentication.
- **[Source]** IEC 62443-3-3.
- **[Definition]** The control system shall provide the capability to uniquely identify and authenticate all users (humans, software, 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 62443-3-3.
- **[Definition]** The control system shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security standards and recommendations (e.g. trusted platform module (TPM)).
- **[Monitoring Solution]** The plugin checks if the system/device is using TPM or security controller to store the keys.

Use control for portable devices

- **[ID]** MSI 7.2.

- **[Name]** Use control for portable devices.
- **[Source]** IEC 62443-3-3.
- **[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 62443-3-3.
- **[Definition]** Timestamps (date and time) of records should be generated using internal system clocks.
- **[Monitoring Solution]** The plugin checks if the network time protocol (NTP) is enabled including internal time synchronization and protection of time source integrity.

Communication integrity

- **[ID]** MSI 13.2
- **[Name]** Communication integrity.
- **[Source]** IEC 62443-3-3.
- **[Definition]** The control system shall provide the capability to protect the integrity of transmitted information. Depending on the context (e.g. 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 transport layer security (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 ISO 27002 and IEC 62443-3-3 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 then 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 where the metric is extracted, for example, for [MSI-1.1], the source is S1—ISO 27002, 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 the previous section. Then, it verifies the total compliance [%] based in equation (2).

For the presented use case, we consider two scenarios.

Scenario I. The first scenario considers (a) five main components of the use case, (b) two standards, and (c) 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 ISO 27002 and IEC 62443-3-3.

Scenario II. The second scenario considers (a) five main components of the use case, (b) two standards, and (c) 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 ISO 27002 and IEC 62443-3-3.

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.

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

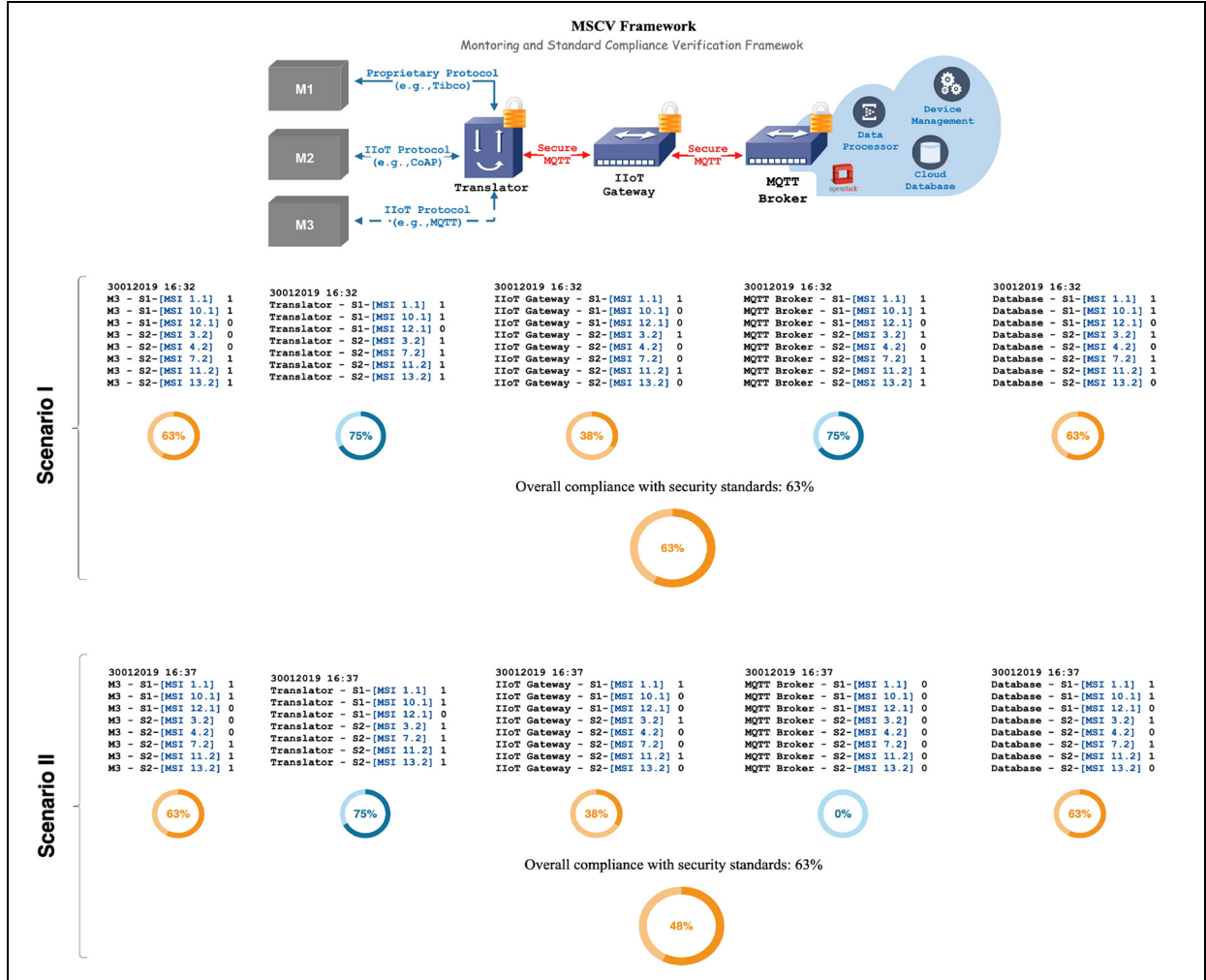


Figure 8. The component/overall compliance check for the end-to-end communication use case based on a set of metrics extracted from the security standards.

standards remains an issue for large scale adoption in the production environment.

In this article, we have presented a MSCV framework. Initially, a high level description of the approach and architecture is provided, where three main components in order to build an automated compliance framework: (a) monitoring agents, (b) EGM module, and (c) compliance module are identified. 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, ISO 27002 and IEC 62443-3-3 standards are evaluated, 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: (a) one of the components fulfill most of the MSIs and (b) 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 movement from large monolithic organizations toward multi-stakeholder cooperations with the aim to enable sustainability, flexibility, efficiency, and competitiveness.

The MSCV will be used to check standard compliance of devices, systems, and services that interact with the Arrowhead Framework during onboarding.⁵²


Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: 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).

ORCID iD

Ani Bicaku  <https://orcid.org/0000-0003-2477-3692>

References

1. Delsing J. *IoT automation: arrowhead framework*. Boca Raton, FL: 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: *Proceedings of the IECON 2012-38th annual conference on IEEE industrial electronics society*, Montreal, QC, Canada, 25–28 October 2012, pp.5766–5772. New York: IEEE.
3. Boyes H, Hallaq B, Cunningham J, et al. The industrial internet of things (IIoT): an analysis framework. *Comput Ind* 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 (IIoT): a text mining approach. *IEEE Intell Syst* 2018; 33: 63–73.
6. Wurm J, Hoang K, Arias O, et al. Security analysis on consumer and industrial IIoT devices. In: *Proceedings of the 2016 21st Asia and South Pacific design automation conference (ASP-DAC)*, Macau, China, 25–28 January 2016, pp.519–524. New York: IEEE.
7. Falco G, Caldera C and Shrobe H. IIoT cybersecurity risk modeling for SCADA systems. *IEEE Internet Things J* 2018; 5: 4486–4495.
8. Kshetri N and Voas J. Hacking power grids: a current problem. *IEEE Comput Soc Press* 2017; 50: 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: *Proceedings of the 2018 international conference on computer science, electronics and communication engineering (CSECE 2018)*. Atlantis Press, <https://www.atlantis-press.com/proceedings/csece-18/25893360>
10. Yeh E, Choi J, Prelcic N, et al. Security in automotive radar and vehicular networks, 2016, http://www.ce.utexas.edu/prof/bhat/ABSTRACTS/SecurityOverview_mmWave_V2X.pdf
11. TETRA and Critical Communications Association (TCCA). Importance of standard compliance in telecommunication. In: TCCA (ed.) *Standards white paper v1.0*. Ely: Critical Communications Broadband Group, TCCA.
12. Bicaku A, Schmittner C, Tauber M, et al. Monitoring Industry 4.0 applications for security and safety standard compliance. In: *Proceedings of the 2018 IEEE industrial cyber-physical systems (ICPS)*, St. Petersburg, 15–18 May 2018, pp.749–754. New York: IEEE.
13. De Haes S, Van Grembergen W and Debreceeny RS. COBIT 5 and enterprise governance of information technology: building blocks and research opportunities. *J InformSyst* 2013; 27: 307–324.
14. Pasquini A and Galie E. COBIT 5 and the process capability model. Improvements provided for IT governance process. In: *Proceedings of the FIKUSZ'13 symposium for young researchers*, pp.67–76, https://kgk.uni-obuda.hu/sites/default/files/06_Pasquini_Galie.pdf
15. Janvrin DJ, Payne EA, Byrnes P, et al. The updated COSO internal control—integrated framework: recommendations and opportunities for future research. *J Inform Syst* 2012; 26: 189–213.
16. Graham L. *Internal control audit and compliance: documentation and testing under the new COSO framework*. Hoboken, NJ: John Wiley & Sons, 2015.
17. Lubell J. Using DITA to create security configuration checklists. In: *Proceedings of the Balisage: the markup conference*, <http://www.balisage.net/Proceedings/vol19/html/Lubell01/BalisageVol19-Lubell01.html>
18. Waltermire D, Quinn S, Scarfone K, et al. The technical specification for the security content automation protocol (SCAP): SCAP version 1.2. *NIST Spec Publ* 2011; 800: 126.
19. Gapinski A. Cloud computing: information security standards, compliance and attestation. In: *Proceedings of international conference on engineering and technologies (LACCEI)*, Santo Domingo, Dominican Republic, www.laccei.org
20. Choe V, Taylor D and Brizhik A. SOC 2 breakdown. A five-part guide to understanding the service organization controls 2 report and its benefits. *Intern Audit* 2012; 69: 54–59.
21. Liu Y, Muller S and Xu K. A static compliance-checking framework for business process models. *IBM Syst J* 2007; 46: 335–361.
22. 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*, Seville, 18–21 July 2011. New York: IEEE.
23. Ravi T and Sankar S. Measuring the security compliance using cloud control matrix. *Mid East J Sci Res* 2015; 23: 1797–1803.
24. Mitchell S and Switzer CS. *GRC capability model (red book 2.0)*. Phoenix, AZ: Open Compliance & Ethics Group (OCEG), 2009.
25. Vicente P and da Silva MM. A conceptual model for integrated governance, risk and compliance. In: *Proceedings*

- of the international conference on advanced information systems engineering, pp.199–213. Springer, https://link.springer.com/content/pdf/10.1007%2F978-3-642-21640-4_16.pdf
26. Cheng D, Villamarin J, Cu G, et al. Towards end-to-end continuous monitoring of compliance status across multiple requirements. *Int J Adv Comput Sci Appl* 2018; 9: 456–466.
 27. Ge M, Hong JB, Guttman W, et al. A framework for automating security analysis of the internet of things. *J Netw Comput Appl* 2017; 83: 12–27.
 28. Racz N, Weippl E and Seufert A. A process model for integrated it governance, risk, and compliance management. In: *Proceedings of the 9th Baltic conference on databases and information systems*, pp.155–170, <https://pdfs.semanticscholar.org/d28d/185b7609674e7bf782db812bcd1c48753718.pdf>
 29. Safa NS, Von Solms R and Furnell S. Information security policy compliance model in organizations. *Comput Secur* 2016; 56: 70–82.
 30. Fenz S and Neubauer T. Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Inform Comput Secur* 2018; 26: 551–567.
 31. Susanto H and Almunawar MN. *Information security management systems: a novel framework and software as a tool for compliance with information security standard*. Boca Raton, FL: CRC Press, 2018.
 32. Theoharidou M, Kokolakis S, Karyda M, et al. The insider threat to information systems and the effectiveness of ISO17799. *Comput Secur* 2005; 24: 472–484.
 33. Calder A and Watkins S. *IT governance: an international guide to data security and ISO27001/ISO27002*. London: Kogan Page Publishers, 2012.
 34. Vladimirov AA, Gavrilenko KV and Michajlowski AA. *Assessing information security: strategies, tactics, logic and framework*. Ely: IT Governance Ltd., 2010.
 35. Wang L, Törngren M and Onori M. Current status and advancement of cyber-physical systems in manufacturing. *J Manuf Syst* 2015; 37: 517–527.
 36. Bandyopadhyay D and Sen J. Internet of things: applications and challenges in technology and standardization. *Wirel Pers Commun* 2011; 58: 49–69.
 37. Eichelberg M, Aden T, Riesmeier J, et al. A survey and analysis of electronic healthcare record standards. *ACM Comput Surv* 2005; 37: 277–315.
 38. Blackford RW. Aerospace coating and treatment standards. *Met Finish* 2003; 101: 14–24.
 39. Pelton JN. Future space safety technology, standards, and regulations. In: Pelton JN and Jakhu R. (eds) *Space safety regulations and standards*. Burlington, VT: Elsevier, 2010, pp.397–406.
 40. Costa-Pérez X, Festag A, Kolbe HJ, et al. Latest trends in telecommunication standards. *ACM SIGCOMM Comput Commun Rev* 2013; 43: 64–71.
 41. Dodoo A, Gustavsson L and Sathre R. Building energy-efficiency standards in a life cycle primary energy perspective. *Energ Build* 2011; 43: 1589–1597.
 42. Pigosso D, Ferraz M, Teixeira C, et al. The deployment of product-related environmental legislation into product requirements. *Sustainability* 2016; 8: 332.
 43. 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, <https://dl.acm.org/doi/10.5555/2735338.2735341>
 44. Jang-Jaccard J and Nepal S. A survey of emerging threats in cybersecurity. *J Comput Syst Sci* 2014; 80: 973–993.
 45. Bicaku A, Maksuti S, Palkovits-Rauter S, et al. Towards trustworthy end-to-end communication in Industry 4.0. In: *Proceedings of the 2017 IEEE 15th international conference on industrial informatics (INDIN)*, Emden, 24–26 July 2017, pp.889–896. New York: IEEE.
 46. Nagios Enterprises. Nagios, 2019, <https://exchange.nagios.org/directory>
 47. OpenStack. Ceilometer, 2019, <https://docs.openstack.org/ceilometer>
 48. Olups R. *Zabbix 1.8 network monitoring*. Birmingham: Packt Publishing Ltd., 2010.
 49. Bicaku A, Balaban S, Tauber MG, et al. Harmonized monitoring for high assurance clouds. In: *Proceedings of the 2016 IEEE international conference on cloud engineering workshop (IC2EW)*, Berlin, 4–8 April 2016, pp.118–123. New York: IEEE.
 50. Maksuti S, Bicaku A, Tauber M, et al. Towards flexible and secure end-to-end communication in Industry 4.0. In: *Proceedings of the 2017 IEEE 15th international conference on industrial informatics (INDIN)*, Emden, 24–26 July 2017, pp.883–888. New York: IEEE.
 51. Derhamy H, Eliasson J and Delsing J. IoT interoperability—on-demand and low latency transparent multiprotocol translator. *IEEE Internet Things J* 2017; 4: 1754–1763.
 52. Bicaku A, Maksuti S, Hegedüs C, et al. Interacting with the arrowhead local cloud: on-boarding procedure. In: *Proceedings of the IEEE industrial cyber-physical systems*, St. Petersburg, 15–18 May 2018, pp.743–748. New York: IEEE.