Applicability of the IEC 62443 standard in Industry 4.0 / IIoT

Björn Leander
Mälardalen University
ABB Industrial Automation, Process Control Platform
Västerås, Sweden
bjorn.leander@se.abb.com

Aida Čaušević
Hans Hansson
Mälardalen University
Västerås, Sweden
aida.causevic@mdh.se
hans.hansson@mdh.se

ABSTRACT

Today's industrial automation systems are undergoing a digital transformation that implies a shift towards the Internet of Things (IoT), leading to the Industrial Internet of Things (IIoT) paradigm. Existing Industrial Automated Control Systems (IACS), enriched with a potentially large number of IoT devices are expected to make systems more efficient, flexible, provide intelligence, and ultimately enable autonomous control. In general, the majority of such systems come with high level of criticality that calls for well-established methods and approaches when achieving cybersecurity, preferably prescribed by a standard.

IEC 62443 is an industrial standard that provides procedures to manage risks related to cybersecurity threats in IACS. Given the new IIoT paradigm, it is likely that existing standards are not sufficiently aligned with the challenges related to developing and maintaining cybersecurity in such systems. In this paper we review the applicability of the IEC 62443 standard in IIoT contexts and discuss potential challenges the process owners might encounter.

Our analysis underlines that some areas within the standard could prove difficult to reach compliance with. In particular, handling of cross zone communication and software updates require additional guidance.

CCS CONCEPTS

• **Security and privacy → Systems security**.

ACM Reference Format:
Björn Leander, Aida Čaušević, and Hans Hansson. 2019. Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3339252.3341481

1 INTRODUCTION

Industrial Automation and Control Systems (IACS) are used for operating a wide range of industrial applications, including critical infrastructure. An emerging trend within IACS is the Industrial Internet of Things (IIoT), being driven by the fourth industrial revolution (Industry 4.0). According to Industrial Electrotechnical Commission (IEC) [6], a fundamental purpose of Industry 4.0 is to enable cooperation and collaboration between devices. More specifically, the aim of IIoT is to enable optimization, cost-savings, and new business opportunities in different domains. It is expected that IIoT will introduce significant advances in optimizing decision-making, operations and collaborations among a large number of increasingly autonomous control systems [8].

IEC 62443 [7] is an industry standard that describes ways to handle cybersecurity threats in IACS. The standard has been developed with the classical automation pyramid in mind. With the emergence of IIoT, this architecture is no longer the norm, and the development has accelerated an already ongoing convergence between Operation Technology (OT) and Information Technology (IT) that results in an increase of the attack surface of IACS. There is an apparent risk that the introduction of IIoT makes parts of the standards outdated.

The main purpose of this paper is to assess the IEC 62443 standard from an IIoT perspective, and discuss a number of issues that process owners will face when trying to keep compliance to the standard while adapting to the reality of an increasing number of IIoT devices being part of the system. To make the work more readable we include a rather simple description of an automation architecture in both a traditional IACS and an IIoT set up, to which we relate our findings.

The paper is organised as follows. Section 2 introduces necessary background and defines concepts used in this paper. In Section 3 the current state of the IEC 62443 standard is described together with the IACS reference model. Section 4 presents a simplified architecture for an IIoT system, and based on that we analyse the IEC 62443 standard, and provide a discussion on challenges when trying to reach compliance to the standard in such a system. The contributions of the work are recalled in Section 5, together with suggestions for the future research.

2 BACKGROUND

An IACS is defined as the system of hardware, software, personnel and policies involved in operation of an industrial process and that can affect its operation with regards to safety, security and reliability [7]. IACS are responsible for controlling and monitoring a wide range of different types of physical processes, ranging from chemical industries, power plants, manufacturing, etc. Many of these systems are of vital importance for supplying basic functionality to society, such as electricity and clean water. Failure of systems providing critical infrastructure services can have severe effects, both economical and environmental, and their protection is

ARES '19, August 26–29, 2019, Canterbury, United Kingdom

ACM ISBN 978-1-4503-7164-3/19/08…$15.00
https://doi.org/10.1145/3339252.3341481

therefore of great importance. For many industry segments there are laws regulating how this protection must be implemented. For example, plants delivering power to the North American power grid are required to fulfill the NERC CIP standard [17].

Cybersecurity is the protection of a computer system from unauthorized actors possibility to steal or alter information in the system, disrupt or alter behaviour of a function or perform an unauthorized action [11].

The IEC 62443 is the de facto standard for cybersecurity in industrial control systems, as the only one being applied internationally and cross-industry [12]. It is defined by the IEC in cooperation with International Society for Automation (ISA). IEC 62443 has parts being under development, but it is still widely used by industry, and also forms a base for certification, e.g. the Embedded Device Security Assurance (EDSA) certification [10]. An IACS owner can use the described methods to keep its system at a desired level of security, and also require that service providers and manufacturers of the components used in the IACS follow the principles and adheres to a certain security level for their delivery. In this way the IEC 62443 is a source of common understanding of cybersecurity related issues for IACS owners, component developers, and service providers.

In the traditional IACS there used to be a clear separation between the OT network and the IT network. The OT network containing the devices and services directly concerned with controlling the physical process, was usually physically separated from the IT network, that contained e.g., the organization office network. There is an ongoing convergence between the IT and OT network, with the introduction of IT technology in the OT network, and a growing amount of interconnections between IT and OT networks, e.g., remote access from IT clients to OT functions and the usage of standard IT components in OT systems. This convergence of technologies implemented with different objectives with regards to security [12] is exposing IACS to potentially new cybersecurity threats. The attack on the Ukrainian power grid in December 2015, is one such an example, where attackers were able to compromise and disrupt power distribution [13], affecting approximately 250.000 Ukrainian citizens.

The Industrial Internet or Industry 4.0 is an ongoing trend in the world of industrial automation. Some of the promises of Industry 4.0 are:

- Autonomous collaboration between technical assets, minimizing the need for low level configuration.
- Advanced analysis of large amounts of data allowing better business decisions.
- Support for novel business models, such as Factory as a Service.

Internet technology is being applied in IACS systems, and specifically IoT devices and services being adopted to or developed specifically for use in industrial applications. IIoT has a multitude of definitions, but in this paper we will use the following definition, inspired by Boyes et al. [2]: an IIoT is assumed to be comprised of devices and services spread over a thing-to-cloud continuum, with each device able to be composed of several devices. Devices may have related information spread throughout several services, and for each device there may be multiple stakeholders both within and outside the IACS owner organisation. The objective of the IIoT is to optimise the overall value that the IACS deliver, including e.g., product or service quality, productivity, labour costs and resource allocations. In smart manufacturing, the product being manufactured is also part of the IIoT, directing the process-steps it flows through with actions that must be executed to complete its manufacturing process.

3 IEC 62443 - CURRENT STATE

IEC 62443 consist of a number of documents describing different aspects of implementing and maintaining security to a well defined level within an IACS. The standard is split into four main groups, with several documents in each group:

- IEC 62443-1-X General, contains documents for defining concepts, terminology, use cases, etc.
- IEC 62443-2-X Policies and procedures, contains e.g., secure patch management and security program requirements.
- IEC 62443-3-X System level requirements, system risk assessment, etc.
- IEC 62443-4-X Component level requirements, including component development requirements.

In this paper we will look at published documents of the standard available from the IEC library. At the time of writing this includes 1-1, 2-1, 2-3, 2-4, 3-1, 3-3, 4-1 and 4-2.

The IEC 62443 standard in general provides requirements that must be fulfilled, but does not suggest measures for evaluating implementation of these requirements. There is no clear guidelines in process of assuring that the requirements are met, which makes a lot of the work with assigning levels of security and assessing countermeasures into subjective tasks for the implementing organisation. This characteristic makes the standard useful also when new technologies are introduced, but partly impede the possibility of stating compliance without subjective judgement.

Risk tolerance level is one key aspect defining the risk an organisation can accept for a specific IACS. Several different response strategies can be applied to a risk:

- Change design to remove the risk;
- Reduce the risk;
- Accept the risk;
- Transfer the risk, e.g., insurances or outsourcing of function.

Cybersecurity Management Systems (CSMS) includes e.g., programs to continuously reassess risks. Security Levels are created to classify groups of assets, with regards to security zones. For each security zone a target security level $SL(target)$ is assigned. The $SL(target)$ is usually the outcome of a risk assessment of that zone. $SL(target)$ describes the effectiveness that applied countermeasures must reach to properly secure the zone. The achieved security level $SL(achieved)$ of a zone is a dynamic property that typically degrades with time, as emerging threats and evolving technologies make existing countermeasures relatively less secure, unless maintenance and upgrade procedures are followed. $SL(capability)$ is the security level a specific countermeasure or device/system can provide to a security zone.

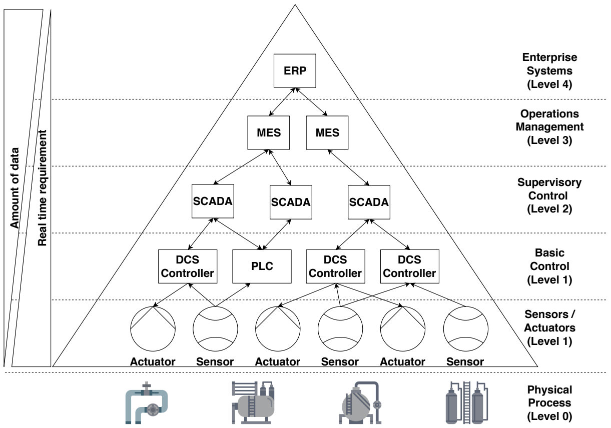

Figure 1: Traditional automation pyramid based on PERA

The goal is that for any given time $SL(acheived) \geq SL(target)$, for each security zone defined in the system. A security level life-cycle aims to continuously fulfill this goal, using recurring reassessments and specific assessments for security related system changes, e.g., process change, new vulnerability detected, software patch of devices.

The IACS reference model used in the standard is 5-tier, influenced by the Purdue Enterprise Reference Architecture (PERA) [22], illustrated in Figure 1.

Layer 1-2 typically comprise the OT network, usually being split into several security zones based on criticality, layer 3-4 comprise the IT network. As can be seen the different layers directly interact only through hierarchy. Lower levels typically have real-time constraints, but the higher the level, the longer the cycles become. For Enterprise Resource Planning systems (ERP) reaction on data may be in terms of weeks or months. The amount of data being collected and concentrated per level is reversed, the higher the level, the more data is used for the processing logic.

3.1 Security program for IACS service provider and IACS owner

IEC 62443-2-1 Ed. 1 and 62443-2-4 contains guidance on the content and development for a CSMS for an organisation owning or providing service to an IACS. The standards mainly consist of policies and procedures, that shall be part of the CSMS, and suggestions on how these could be developed.

The elements of the CSMS with regards to IACS owner is divided into three main categories, the first one focusing on risk analysis, the second (and largest) one focusing on addressing risks, and the third one addresses fulfillment and continuous improvement of the CSMS.

The elements focusing on risk analysis provides requirements on e.g., that a risk assessment methodology must be selected, that a risk assessment using that methodology should be executed and documented by trained personnel and that there should be a strategy for reassessment.

The elements focusing on addressing risk contains requirements on policies, organization, selected security countermeasures, document management, incident handling, etc.

The elements focusing on fulfillment and improvement of the CSMS contains requirements on how to perform recurring audits of the organisation, and how to evaluate and introduce changes of the CSMS.

IACS service providers are separated into two categories: integration service providers and maintenance service providers. The requirements as defined for CSMS for IACS service providers are formulated slightly different compared to those of an IACS owner, as the focus is on what capability the service provider can deliver in relation to the IACS. The Capability Maturity Model Integration for services (CMMI-SVC) [4] is adapted to the standard as a measure for service provider maturity with regards to compliance with the standard.

3.2 Secure Patch Management

Secure patch management is an issue of great importance in an IACS, as software goes out of date, bugs are fixed, potentially functionality is added. At the same time, introduction of non-operable or malicious software poses a great threat to such a system.

IEC 62443-2-3 is the part of the standard that provides guidance on secure patch management. All assets must be monitored with regards to current versions and available patches, installed and verified in a test-system, create backups of original system before applying patch, and possibly halt operations while applying patch. Assets may reach a point in time when they are no longer supported by the product supplier, i.e., software/asset obsolescence. In such cases new patches for the asset will not be released regardless of any vulnerabilities or bugs discovered.

With the full patch management process both by the vendor and by the asset owner, a software patch has a life-cycle containing several states, including testing, approving and releasing from product supplier perspective to internal test, authorization and internal release by asset owner (i.e., 11 steps according to the standard).

The standard supplies a set of recommended requirements with regards to patch management for both the IACS owner and IACS product supplier. For the IACS owner the key issue is to keep an inventory of all updatable assets containing their current versions, latest available patch versions and status, regularly revise that list and apply patches after performing internal tests. For product supplier the requirements include supplying information on patch availability and applicability, warn customer in advance of "end-of-life" for product, etc.

The standard argues for any IACS owner and IACS product supplier to implement a patch management process to facilitate these requirements.

3.3 Security technologies for IACS

IEC 62443-3-1 provides an assessment of various cybersecurity tools, mitigation counter-measures, and technologies that can be used in IACS, followed by guidance on usage and known weaknesses of existing methods.

Authorization and authentication are two of the main areas being covered, discussing Role Based Acces Control (RBAC) as one useful, but not widely used method. The main weakness is that current RBAC systems in general are tied to specific technology stacks, such as COTS OS. IACS commonly include specialized devices that do not have this support by default, thus require development of interfaces against the (various) RBAC system(s). Furthermore, a centralized RBAC system would require any device to be covered to have access to a central server, making the operation of the IACS dependent on the health of the corporate network.

Network firewalls are discussed as an important tool for perimeter protection, including SW and HW firewalls, different filtering strategies, log monitoring, etc.

Symmetric Encryption is discussed, and noted not being commonly used in the IACS environment, as the control networks are seen as operating in physically secure zones. However, for traffic crossing unsecure networks, encryption of data is encouraged.

Public key (assymetric) encryption is seen as an important means of exchanging symmetric keys, but is in general too resource consuming to be used in time-critical devices. Man-in-the middle attacks can be successfully launched against public key encryption methods, unless authenticity of communicating parties are validated by certificates.

Audit log monitoring is described as being an important method of detecting intrusion attempts. Focus is mainly on servers e.g., windows server machines, for which there exist centralized audit log methods.

Intrusion Detection Systems (IDSs) come in two flavors: Network IDS (NIDS) and Host IDS (HIDS). NIDS is most commonly deployed as a separate device, e.g., connected to a mirroring port on a network router or integrated in a router or firewall. NIDS checks all network data for either known attack-patterns or unexpected behavior. HIDS is installed as software on a host and can check the logs, network traffic and file-system for indications of completed or ongoing intrusions. A special variant of IDS also prevents an intrusion attempt by, e.g., blocking network traffic related to a detected intrusion attempt. There are several drawbacks of IDS, mainly related to the cost of applying to all sub-nets and hosts, cost of monitoring and cost of handling false positives.

Vulnerability scanners provide means of hardening the system, and can be used to detect: security policy deviations, bad configurations and software flaws. Typically these kinds of scans should be performed when re-assessing $SL(acheived)$ for an IACS. However, the scan itself can have a negative impact on the performance of the IACS, implying that the scan should ideally be performed in a lab-environment first to assess that the impact of the scan will not interfere with regular operations. Alternatively a vulnerability scan could be performed during a planned maintenance halt of the process.

Host Configuration Management (HCM) tools can be used to remotely edit default host configurations with regards to available software, as well as user access. In IACS this is not widely used, due to the lack of standardization of such systems with regards to the diversity of hosts.

Operating Systems are discussed in the standard, especially real-time operating systems (RTOS) are mentioned as having limited possibilities and abilities to counter cybersecurity threats. As e.g., DCS controllers and PLCs, in general execute on RTOS, these devices by their nature cannot function without network connectivity that makes them one of the most vulnerable parts of an IACS. These systems monitor and control real physical processes. The recommendation is to keep them on truly isolated networks, e.g., keep time-critical application traffic on a separate network. This will probably be true in early adaptions to IIoT, with separation of real-time functionality for control and critical supervision from information collection with regards to analysis. In a longer perspective, IIoT devices could be part of an IACS as a real-time critical component, providing measurement feedback or process control.

3.4 System and Component security requirements and security levels

IEC 62243-3-3 and 4-2 describe system and component security requirements and security levels. It aims to provide requirements for the IACS, based on the seven foundation requirements (FR):

(1) Identification and authentication control (IAC);
(2) Use control (UC);
(3) System integrity (SI);
(4) Data confidentiality (DC);
(5) Restricted data flow (RDF);
(6) Timely response to events (TRE);
(7) Resource availability (RA).

Each foundation requirement has a purpose statement, and defines four security levels (i.e., SL 1-4), for example for the data confidentiality FR the levels are defined as follows:

SL 1 Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.

SL 2 Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.

SL 3 Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.

SL 4 Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

The higher the security level a control system reaches for a specific FR, the more persistent against an attack on that area the system should be. Typically SL 1 will protect against accidental leaks or low-motivation, low-resource attackers, whereas SL 4 will prevent attacks from a highly motivated and resourceful adversary. There is also an implicit SL 0, indicating no specific security protection necessary.

The FR are detailed in System Requirements (SR) and additional Requirement Enhancements (RE) which are related to the different security levels for the FR.

There is a special notion of essential functions, being required to maintain health, safety and environmental concerns. Essential functions cannot be negatively impacted by implementation of security requirements, e.g., accounts used for essential functions shall not be locked out, security functions shall not add significant delay on time-critical essential functions. This can lead to difficult trade-offs between availability and the other security objectives in the case of certain types of attacks and countermeasures.

In principal, when using these parts of the standard, the desired SL for a specific IACS or component is selected for each of the seven FR. This will lead to a number of SR and additional RE being applicable to the system. Each of these requirements must be fulfilled for the target SL to be reached. This also means that there is a (relatively) easy way to assess to which degree a certain SL is reached with regards to a specific FR.

In IEC62443-4-2 component requirements (CRs) are described, in a similar way as the system requirements. They are classified into four categories:

(1) Software Application Requirements (SAR);
(2) Embedded Device Requirements (EDR);
(3) Host Device Requirements (HDR);
(4) Network Device Requirements (NDR).

It is common that requirements are the same for all type of components, and therefore expressed only as general CRs.

(1) Software application - one or more programs/services that interacts with the process or control system and are executing on an embedded or host device;
(2) Embedded device - a specific purpose device with specialized hardware and firmware developed to fulfill that purpose. Typically the device is directly or indirectly involved into monitoring or controlling a physical process and has real-time requirements to fulfill;
(3) Host device - a general purpose device with capabilities of running several services, usually with an "open" OS, e.g., Windows or Linux;
(4) Network device - a device that facilitate (or limits) data flow between devices, but does not directly interact with the process.

Common component Security Constraints comprise a number of constraints applicable to the components that may restrict the implementation of some security functions. Some examples of constraints are: essential functionality must be sustained, least privilege shall be used when appropriate, etc.

3.5 Secure development of IACS Components

IEC 62443-4-1 describes the best practices to follow when implementing IACS components. The standard is based partly on the Secure Development Life-cycle Assessment (SDLA) certification, as described by ISCI [9]. The document aims to support component suppliers. It is divided into eight main practices:

(1) Secure Management;
(2) Specification of security requirements;
(3) Secure by Design;
(4) Secure implementation;
(5) Secure validation and testing;
(6) Management of security related issues;
(7) Security update management;
(8) Security guidelines.

Each practice is described in detail, and divided into related requirements. The requirements are in the most cases described as a need for the development organization to have a process fulfilling specific goals, e.g., "Security requirements review (SR-5): A process shall be employed to ensure that security requirements are reviewed, updated as necessary and approved to ensure clarity, validity, alignment with the threat model, and their ability to be verified."

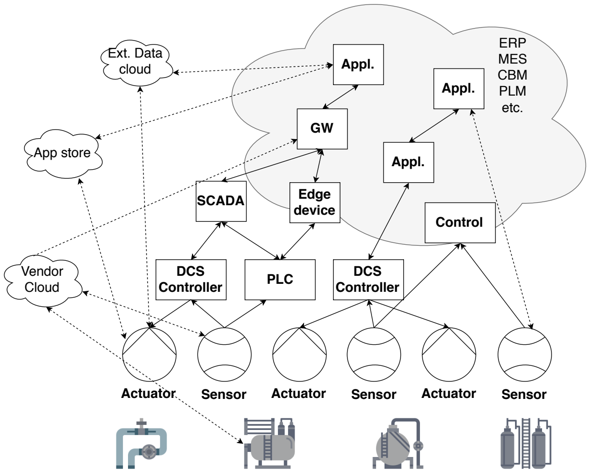

Figure 2: An example of an IIoT architecture [20]

If a product supplier is following these practices during the development life-cycle of an IACS component, the component will be able to comply to a specific SL over time, and will be secured by a defense in depth strategy.

Similarly as for the IACS service provider, the Capability Maturity Model Integration for development (CMMI-DEV) is used in the standard as a benchmark for a product supplier to indicate or self-assess to what degree the secure development processes for each practice are followed.

4 ASSESSMENT OF IEC 62443 IN RELATION TO IIOT

As IIoT devices and services are being increasingly adopted into IACS systems they increase the potential attack surface of the system, as they often live at the edge of the network, i.e., communicate over the zone boundaries.

To not deteriorate the security characteristics of an IACS, as IIoT technology is introduced, it would be desirable to use the IEC 62443 standard to reassess the system, as well as for initial assessments if greenfield IACS implementations utilizing IIoT are provided.

4.1 IIoT systems - an architectural view

An asset in IIoT can be seen as the sum of all devices and services containing functionality or data for that asset. The system for an asset could be comprised by different services for current and historical process data, such as current control set-point, historical data for power consumption, data from a connected vibration sensor, alarm and event-lists, and control logic. It also includes maintenance log and plans, software publisher services for the asset firmware and related services, graphical representation of asset as used in a control room, CAD drawings, asset vendor services, etc. At the high level it gathers analytics using data related to the asset to perform long term resource planning or process optimization. Therefore we can conclude that the whole IIoT system can be subsequently seen as a system of such systems.

In Figure 2, a simplified generic IIoT architecture is presented, the architecture is inspired by the one described by Schriegel et. al [20]. The architecture is based on the automation pyramid, extended with some of the concepts from a typical IIoT system. As can be seen from this simplified architecture, many of the functions traditionally kept in the IT network now can be realized in an on-site or remote cloud, with applications like Condition Based Monitoring (CBM), Product Life-cycle Management (PLM) and Manufacturing Execution Systems (MES). Data can be flowing directly from devices to cloud, or via edge nodes, allowing shorter analysis/decision cycles. There might be third party vendors collecting and possibly sharing information on assets (via Vendor Cloud). Different services/devices might be implemented with different cloud architectures in mind, requiring cross cloud integration (i.e., Ext. Data cloud). There might be local or remote software publishing services for patch management, adding functionality or enabling interoperability (i.e., App Store in the cloud). There might even be control logic being executed in a cloud or edge-device. Many of the characteristics of the traditional automation pyramid do no longer hold such as:

(1) No strict and predefined communication paths following the hierarchical levels.
(2) There might be real-time requirements at many levels.
(3) Possible mix of OT and IT functionalities at any level.

Based on these assumptions in an IIoT architecture we depict in Figure 2, we take a look at the standard and discuss the parts of the standard mostly impacted by this change.

4.2 Security zones and network segmentation in IIoT

The concept of security zones is central in IEC 62443. Given a heterogeneous IIoT system containing numerous interconnected devices and services that also utilize cloud technologies, one can raise the question whether the idea of zoning is still valid. Considering the brownfield scenario, where devices or services are introduced into one security zone, and those devices have network connectivity to other less protected zones, that will at least make the zone more susceptible to attacks. However, if components used for controlling a critical process are still isolated in a separate zone, and IIoT devices or services used for monitoring the critical process are kept in another network, the dividing into security zones clearly provide additional safety. In the Reference Architecture for Industry 4.0 (RAMI4.0) [6], it is suggested that there should be separate networks for direct process control.

In IEC 62443-3-1, the guidance (c. 6.2.7) states that only network traffic directed from the IACS towards the IT-network should be allowed. To make use of many of the advantages promised by IIoT, analytics will in many cases be performed in e.g., a cloud environment. Results from the analysis could be an updated configuration for a device to trim performance, including altering set-points. For this to work through such a firewall the communication protocol would need access to the device itself or a related service to regularly request the analytic engine for e.g., updated configurations.

Keeping network segmentation rules intact can be a challenge considering an increasing amount of the devices in the control system being IIoT devices with services distributed over the device-to-cloud continuum. Considering SR 5.2 - Zone boundary protection stating (at SL 2), network traffic crossing a zone boundary should be denied by default and allowed by exception only. Implementation of this will require a considerable amount of configuration efforts for every IIoT device added to the control system.

SR1.13 in IEC 62443-3-3 discusses access via an untrusted network, requesting the control system to monitor and control all access via such a network. In principle the guidance is that such communication paths should not exist, and if they exist, the control system should have capabilities to disable them. Both wireless and possibly untrusted networks will be a common interaction point for IIoT devices. SR1.6 and SR1.13 will in many ways be contradictory to allow some of the basic functionalities of an IIoT. These requirements could possibly be adapted so that communication over untrusted networks could be allowed, if the devices themselves fulfill specific requirements.

A novel network technology for an IIoT system with increasing popularity is Software Defined Networks (SDN), discussed in [1, 20, 21]. SDN is adopted from cloud computing technologies, and is characterized by dynamic configuration of the network by a central node, with the aim to optimize performance based on current application. This approach fits quite well with the dynamic nature of interconnections between devices and services in Industry 4.0, where applications may shift and communication paths may not be well known in advance. However, this technology seems to be in conflict with the physically or logically well defined and separated networks being protected by physical firewalls in strategic nodes as prescribed by the IEC 62443 standard.

Considering the IIoT paradigm where the communication paths are not confined within isolated networks, the need to use end-to-end security is apparent [8]. There are several cryptographical methods emerging that are relatively low-cost with regards to computational and bandwidth utilization, e.g. compressed versions of DTLS [18], which could enable using end-to-end security as a standard in IACS components. For some constrained devices, end-to-end security may still prove too costly with regards to resource consumption. In such cases specific edge nodes can be used to provide security functions for a collection of constrained devices.

4.3 Patch management in IIoT

The patch management guidelines, described in IEC 62443-2-3, seems to be infeasible in a number of situations when used in an IIoT system:

(1) The number of devices and services involved in IIoT substantially exceeds that of a typical IACS, making the work of monitoring and updating devices infeasible;
(2) A fair share of the IIoT devices will be Internet-facing or at least communicate using wireless technology, meaning that a postponed or deferred security-related update for a device could lead to an unacceptable risk of the device being compromised;

(3) For the devices or services not being directly involved in controlling the physical process, following these guidelines may be too strict.

Because of the high cost and effort compared to the risk of not applying a specific patch, decisions often weighs in favour of not applying the patch, or at least delaying it until a planned maintenance stop. As a consequence, many executing IACS are not being patched to the most recent software versions, both with regards to OS and application software, potentially resulting in:

- Decreasing *SL*(*achieved*) that increases the risk of the IACS being compromised;
- Incompatibilities between system parts;
- Degradation of system performance and reliability.

Secure patch management is of increasing importance in the IIoT system, but the suggested guidelines are both too strict in some sense and not strict enough in other. For an IIoT systems, there might be a need to classify devices and services based on criticality, and for the less critical components to allow, or even require, automatic patch management, e.g., based on TUF [3] or similar methodology that ensures update integrity. There are new guidelines, methods, and protocols being developed that address secure patch management. For example, the IETF Secure Update of IoT-devices (suit) work group is currently working on an architecture related to this [14].

There is an ongoing trend in software development towards DevOps [5], that most likely will affect the release cycles of some components in an IACS. DevOps is a result of combining agile software development methods with IT operations, shortening the development life-cylce and thereby the releases of a component will be more frequent and possibly without any specific periodicity. Typically a published code will push for an automatic build after which automatic tests are executed and the software is packaged. If test results are acceptable the update can be released, and possibly automatically pulled by the device instances running the software.

Another trend in software development gaining in interest in the last five years, that might impact how patch management will work in the future IACS, is the shift from classical virtualization using a hypervisor towards containerized services. Since a container execution environments provides some of the benefits from virtualization, without bringing in the overhead of emulating the OS, it could be useful as providing service execution at simpler host devices [19], e.g., the ABB Ability Edge relies on the Docker container environment.

Both DevOps and a container technology will push towards automatic patch management. For an IACS owner this will lead to increased simplicity for the technical work related to patch management, but will add a risk of less control over the system. Future version of IEC 62443-2-3 could include guidelines on how to maintain and monitor a system comprised of heterogeneous devices and services, as well as include a description on requirements for an automatic secure patch management method. Facilitating automated patch management could help in preserving the achieved security level for the system, as well as decreasing the amount of time a known bug prevails in a specific component.

4.4 System/component requirements and security technologies in IIoT

When assessing the requirements in detail, the majority remains applicable in an IIoT perspective, as well. Some might however need to be revised within the new context.

The standard only briefly mentions the need for service authorization, stating that this is usually not implemented and/or used in IACS. For IIoT, this will be of great importance, as most of the interactions will be machine-to-machine.

Host firewalls are also discussed as being not commonly used in the IACS environment, as IACS product vendor typically do not allow it, along with any other third party SW, since it might affect the operability of the IACS. In IIoT systems, it would be natural at least to require that devices with direct Internet connectivity deploy micro-firewalls for added protection. Intrusion detection and prevention systems could also form an important line of defense, however, for these systems to work effectively in an IIoT environment, the cost must be lowered and the monitoring must be highly automated. The IDS and firewalls will also face an increasing amount of encrypted traffic, making state-full packet inspection more difficult when employed at intermediate network nodes, possibly deterring their effectiveness in e.g., attack-pattern recognition.

In the perspective of IIoT, both symmetric and public key encryption will be needed for some of the data-flows, especially for sensitive information that must be transferred to cloud storage for e.g., Big Data analysis. However, in traditional IACS, encryption is rarely used. Using encryption mechanisms comes with a cost both on bandwidth and CPU utilization - especially with regards to asymmetric cryptography. It is therefore of importance to assess the required protection level for specific sets of data, so that the appropriate algorithm is chosen. In the guidance from IEC 62443-3-1 with regards to encryption, it is acknowledged that encryption technologies will be of growing importance in the future, increasingly connected IACS, but the guidance currently only covers symmetric cryptography. It is suggested that any devices utilizing cryptography should be certified according to some well known security standard, e.g., FIPS 140-2 [16], to provide probability that the cryptographic algorithms used are implemented according to the state of the art. This may be a good guidance, but it will possibly prove difficult to follow for any device and service developer. It could be argued that compliance to SDLA, or evidence of using an industry standard approved cryptographic libraries can be used to strengthen trustworthiness of IACS components using cryptography.

Audit logs for user activities are discussed, e.g., access control events, however, for devices or services activities, audit logs are not discussed in depth, but should be of increasing importance from an IIoT perspective. Especially regarding automatic collection and analysis of audit logs combined with an automatic counter-act system for detected anomalies. This should be useful in a scenario with a large number of access points. Exactly what information should be logged regarding machine-to-machine communication could be elaborated. The guidance states that security related data e.g., user account creation or failed logins should be logged, but for the IIoT scenario there might be additional information that are of interest, e.g., device discovery and disconnect, protocol handshakes resulting in a protocol version degradation, etc.

A vulnerability scanning for IIoT-devices could be a useful way of assessing the device security characteristics. To enable a vulnerability scanner in an IIoT system, the information needed to understand how to perform a scan and classify vulnerabilities with regards to a wide range of devices with widely different execution environments should exist. In the guidance, vulnerability scanners are suggested to be used mainly on hosts running standard operating systems.

Host Configuration Management (HCM) tools for centrally managing resources and user accounts are discussed in the standard as not being widely used in IACS. Due to the heterogeneous nature of an IACS system, current HCM tools are not adequate as they typically target only one kind of operating system. For an IIoT system, the diversity of devices will be even a bigger issue, at the same time as the need for efficient and centralized management is of great importance. Possibly parts of this management will be automatically executed in an IIoT system.

5 CONCLUSIONS

IEC 62443 is a well known and widely used standard within industrial automation. It describes requirements and the best practice for development, integration and assessments of components and systems related to an IACS with regards to cybersecurity. The emergence of the IIoT paradigm adds a new dimension to be considered compared to traditional IACS. Given the expected complexity of such systems, our aim was to perform an analysis of the IEC 62443 standards and asses its applicability with regards to IIoT. We have noticed that several parts of IEC 62443 are already well suited for use in the context of IIoT systems. However, a number of concepts as described in the standard may prove difficult to comply with, specifically including

1. Security zone boundaries will be more difficult to withhold due to the dynamic characteristics of an IIoT system.
2. Communication over zone boundaries will be a requirement for many IIoT devices and services in order to provide any value, something which is currently discouraged by the standard.
3. For software updates, a significant level of automation of updates will be needed for IIoT devices and services. It is currently not described in the standard if and how such automation can be supported.

Apart from additional guidance on these challenges, there is also a need for technology that might not yet be available, e.g., microfirewalls for IIoT devices, vulnerability scanners for IIoT systems, HCM tools spanning IIoT devices and services.

As future work, it may additionally be useful to take a look at related standards and recommendations, compare and potentially get inspiration for complementing IEC 62443. Examples of relevant related standards include the NIST Framework for Improving Critical Infrastructure Cybersecurity [15] and the suit architecture for secure updates of IoT devices [14]. Additionally, Industrial Internet Consortium has developed a security framework as a part of its reference architecture (IIC IIRA G4) [8].

ACKNOWLEDGMENTS

This work is supported by the industrial postgraduate school Automation Region Research Academy (ARRAY), and the SAFSEC-CPS project, both funded by The Knowledge Foundation. In addition, ABB has provided funding. The authors would like to acknowledge Judith Rossebø and Tomas Lindström for their feedback.

REFERENCES

[1] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan. 2019. Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency. *IEEE Internet of Things Journal* 6, 1 (Feb 2019), 267–277. https://doi.org/10.1109/JIOT.2017.2734903

[2] Hugh Boyes, Bil Hallaq, Joe Cunningham, and Tim Watson. 2018. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry* 101, June (2018), 1–12. https://doi.org/10.1016/j.compind.2018.04.015

[3] Cappos, Justin et. al. 2019. The Update Framework. Retrieved May 13, 2019 from https://theupdateframework.github.io/

[4] CMMI Institute 2019. CMMI Services. Retrieved May 14, 2019 from https://cmmiinstitute.com/cmmi/svc

[5] C. Ebert, G. Gallardo, J. Hernantes, and N. Serrano. 2016. DevOps. *IEEE Software* 33, 3 (May 2016), 94–100. https://doi.org/10.1109/MS.2016.68

[6] IEC. 2016. *Smart Manufacturing - Reference Architecture Module Industry 4.0 (RAMI4.0).* Technical Report. Internation Electrotechnical Commission. 1–35 pages.

[7] IEC 62443 2009-2018. *IEC 62443 Security for Industrial Automation and Control Systems.* Standard. Internation Electrotechnical Commission, Geneva, CH.

[8] Industrial Internet Consortium. 2016. *Industrial Internet of Things Volume G4 : Security Framework.* Technical Report IIC:PUB:G4:V1.0:PB:20160919. 1–173 pages. https://doi.org/10.13140/RG.2.2.28143.23201

[9] ISA Security Compliance Institute. 2014. *Security Development Life-cycle Assurance - Certification Requirement, rev 1.3.* Technical Report SDLA-300.

[10] ISASecure 2019. IEC 62443-4-2 - EDSA Certification. Retrieved May 2, 2019 from http://www.isasecure.org/en-US/Certification/IEC-62443-Edsa-Certification

[11] Richard Kissel. 2013. *Glossary of key information security terms, Revision 2.* U.S. Dept. of Commerce, National Institute of Standards and Technology.

[12] William Knowles, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, and Kevin Jones. 2015. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection* 9 (2015), 52 – 80. https://doi.org/10.1016/j.ijcip.2015.02.002

[13] Robert M Lee, Michael J Assante, and Tim Conway. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Technical Report. SANS.

[14] Brendan Moran, Milosch Meriac, Hannes Tschofenig, and David Brown. 2019. *A Firmware Update Architecture for Internet of Things Devices.* Internet-Draft draft-ietf-suit-architecture-05. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-ietf-suit-architecture-05 Work in Progress.

[15] NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity.* Technical Report. 1–55 pages. https://doi.org/10.6028/NIST.CSWP.04162018

[16] NIST. 2019. *Security Requirements for Cryptographic Modules.* Technical Report. 1–11 pages. https://doi.org/10.6028/NIST.FIPS.140-3

[17] North American Electric Reliability Corporation 2019. CIP Standards. Retrieved May 9, 2019 from http://www.nerc.com/pa/Stand/pages/cipstandards.aspx

[18] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt. 2013. Lithe: Lightweight Secure CoAP for the Internet of Things. *IEEE Sensors Journal* 13, 10 (Oct 2013), 3711–3720. https://doi.org/10.1109/JSEN.2013.2277656

[19] Joao Rufino, Muhammad Alam, Joaquim Ferreira, Abdur Rehman, and Kim Fung Tsang. 2017. Orchestration of containerized microservices for IIoT using Docker. In *Proceedings of the IEEE International Conference on Industrial Technology.* IEEE, 1532–1536. https://doi.org/10.1109/ICIT.2017.7915594

[20] Sebastian Schriegel, Thomas Kobzan, and Jurgen Jasperneite. 2018. Investigation on a distributed SDN control plane architecture for heterogeneous time sensitive networks. *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS* 2018-June (2018), 1–10. https://doi.org/10.1109/WFCS.2018.8402356

[21] J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, and A. V. Vasilakos. 2016. Software-Defined Industrial Internet of Things in the Context of Industry 4.0. *IEEE Sensors Journal* 16, 20 (Oct 2016), 7373–7380. https://doi.org/10.1109/JSEN.2016.2565621

[22] Theodore J. Williams. 1994. The Purdue enterprise reference architecture. *Computers in Industry* 24, 2 (1994), 141 – 158. https://doi.org/10.1016/0166-3615(94)90017-5