Co-Engineering Gap Analysis of ANSI/ISA-62443-3-3

Petr Mlynek, Radek Fujdiak, Pavel Mrnustik, Bohuslav Krena, and Ludovic Apvrille

***Abstract*— Nowadays, software and system development is a more complex process than ever was and it faces challenges, where security became one of the most crucial. Based upon co-engineering in the AQUAS project, complex standards covering development processes regarding safety, but performance and security are missing. In the paper, the representative standard for Industrial Automation and Control Systems (IACS) is selected for gap analysis, both as examples of issues in co-engineering in security and performance, and possibly for evolution and extension in security standards. For IACS, the ANSI/ISA 62443 defines procedures for implementing security requirements. Based upon co-engineering in the AQUAS project and experience from the real implementation of security by TrustPort practitioners of this domain, the paper introduces the 62443 standard gaps analysis with the goal to identify the missing part. Based on this analysis, the possible recommendations for extending 62443-3-3 are proposed.**

***Keywords*—ANSI/ISA 62443, AQUAS, co-engineering, gap analysis, security, standard**

I. Introduction

A. Security for industrial automation and control systems Part 3-3: System security requirements and security levels

The ISA99 standard, part of the ISA-62443 series, provides detailed technical control System Requirements (SRs) associated with the seven Foundational Requirements (FRs) described in ISA-62443-1-1 (99.01.01) including definition of the requirements for control system capability security levels, SL-C (control system). These requirements are to be used by members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the System under Consideration (SuC) while developing the appropriate control system target SL, SL-T (control system), for a specific asset.

ISA-62443-1-1 (99.01.01) defines seven FRs:

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)

These seven requirements are the foundation for control system capability SLs, SL-C (control system). Defining security capability at the control system level is the goal and objective of this document as opposed to target SLs, SL-T, or achieved SLs, SL-A, which are out of scope.

This document expands the seven FRs defined in ISA 62443-1-1 (99.01.01) into a series of SRs. Each SR has a baseline requirement and zero or more Requirement Enhancements (REs) to strengthen security. To provide clarity to the reader, rationale and supplemental guidance is provided for each baseline requirement as well as notes for any associated REs as is deemed necessary. The baseline requirement and REs, if present, are then mapped to the control system capability security level, SL-C (FR, control system) 1 to 4.

All seven FRs have a defined set of four SLs. The control system capability level 0 for a particular FR is implicitly defined as no requirement. For example, the purpose statement for clause 8, FR 4 – Data confidentiality, is: “Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure”.

The associated four SLs are defined as:

- 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 individual SR and RE assignments are thus based on an incremental increase in overall control system security for that particular FR.

B. Goal

The goal of this gap analysis is to find possible missing parts of the ISA-62443-3-3 [18] based on application of this standard in two use cases of the AQUAS project (called

Manuscript received March 6, 2020, revised March 30, 2020.
The research leading to this paper has received funding from the AQUAS project (H2020-ECSEL JU grant agreement No 737475).

P. Mlynek and R. Fujdiak are with Brno University of Technology, Faculty of Electrical Enginnering and Communications, Brno; and TrustPort, a.s., Brno, Czech Republic (email: mlynek@feec.vutbr.cz).

Pavel Mrnustik is with TrustPort, a.s., Brno, Czech Republic (email: Pavel.Mrnustik@trustport.com).

Bohuslav Krena is with Brno University of Technology, Faculty of Informatics, Brno, Czech Republic (email: krena@fit.vutbr.cz).

Ludovic Apvrille is with LTCI, Telecom Paris, Institut Polytechnique de Paris, Sophia-Antipolis, France (email: ludovic.apvrille@telecom-paris.fr).

UC1 Air Traffic Management and UC4 Industrial Drive) [1]. Based on this analysis, several recommendations for extending 62443-3-3 were proposed.

II. State of the Art – Literature Review

The relation between SL from IEC 62443 and SIL from EN 50129 for safety systems was discussed in [2]. The results showed e.g. that there is no simple relationship between SL and SIL and for safety systems, so it is recommended to always take the requirements of SL 1 into account. From the point of view of the following gap analysis, SL 1 is not defined for many requirements and the relation between safety and security (SL and SIL) is defined only in a general way.

A common description of NIST 800-82 and IEC 62443 is given in [3].

Framework for Security in Engineering Projects, which supports requirements from 62443-2-4 and 62443-3-3, is described in [4].

The implications of functional safety for Industry 4.0 was explored in [5]. This work focused on SIL within SIL levels from IEC 61508 and SL from IEC 62443.

Security risk assessment methodology from [6] is taken from IEC 62443 and focused on Security Risk Assessment for Train Control and Monitoring Systems.

[7] is focused on Industrial Firewall Performance Issues in IACS. Experimental testbed reflects a typical recommended defense-indepth network security strategy in IACS following the IEC 62443 security standards. Evaluation of latency, jitter and packet loss introduced to communications by industrial firewalls at different locations when the industrial network is segmented via security levels, zones and conduits following the IEC 62443 security standards is reported.

Balancing between safety (ISO 12100, IEC 61508) and security (IEC 62443) in IACS systems was discussed in [8]. IEC 62443 is introduced the security point of view (IEC 62443 risk assessment for incidents).

[9] presents a comprehensive vulnerability assessment platform to evaluate the cyber security vulnerability of devices and networks in smart substation automation systems. The article refers to IEC 62443-3-3 and to FRs and their SRs.

The primary use case is a guidance on how to comply with IEC 62443-4-1 for agile architects following SAFe (Scaled Agile Framework). The article [10] refers to IEC 62443-4-1.

A proposed ILP (Integer Linear Programming) problem to accommodate traditional Industrial Control Systems (ICS) network design requirements and modern security recommendations outlined by the ISA-62443.03.02 standard can be found in [11].

[12] describes roles of the user, the system integrator and the product supplier in the security management, details of all aspects under the charge and management of each party in each process and concludes all aspects requiring attention in each security management process in IEC 62443. However, NIST SP 800-82 mainly analyses the current security loopholes and threats for ICS and describes how to implement security inspection and management against the security loopholes and threats.

In the paper [13] of our colleagues from AQUAS, the feasibility to define a development and co-certification life-cycle for functional safety and security was shown. In this paper, IEC 61508 (safety-related) and ISA 62443 (security-related) standards are analyzed. The results of this paper consist in commonalities, a mapping model, and a combined process in the context of safety and security co-engineering. In contrast, our paper focuses mainly on security issues and on the identification of missing parts in the standard based on co-engineering of tools and based on experiences obtained during real implementation of security by TrustPort practitioners in the security domain.

III. Methods

We are using an extensive Secure Software Development Life Cycle catalogue containing security requirements together with the advanced modelling framework TTool based on UML/SysML-Sec for performance analysis [14], see Fig. 1.

Also, we are using experience from the combined analysis of Security and Performance using SSDLC and TTool (https://ttool.telecom-paristech.fr/) applications for Interference Analysis in UC4 (Industrial drive, AQUAS project) [17].

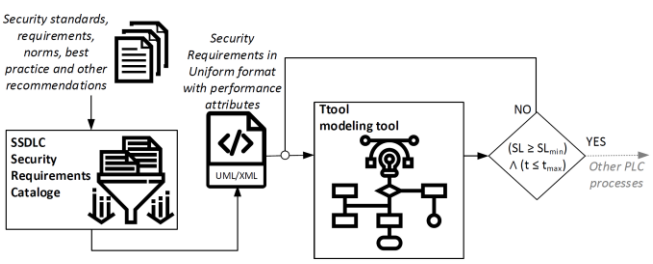

Fig. 1. The experimental environment – Combined analyses of security and performance to support the product life cycle using SSDLC and TTool.

IV. Results

The results are divided into four groups:

a) Gap analysis in Security level/ Security level vector.
b) Gap analysis in impact of security requirements on performance/safety/usability.
c) Gap analysis of verification methods of requirement implementations in 62443-3-3.
d) Proposal of new security requirements.

A. Gap analysis in Security level/ Security level vector

All seven FRs have a defined set of four SLs. The individual SR and RE assignments are thus based on an incremental increase in overall control system security for that particular FR.

1) Security levels – Definition

The following is an excerpt from ISA-62443-1-1 (99.01.01) that provides a good explanation of what SLs are and how they can be used.

"Security levels provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization. As more data becomes available and the mathematical representations of

risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of Security Levels (SL). It will have applicability to both end user companies, and vendors of IACS and security products. It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments."

In the first phase of the development, the ISA 62443 series of standards tend to use qualitative SLs, using terms such as "low", "medium", and "high". The asset owners will be required to come up with their own definition of what those classifications mean for their particular application. The long-term goal of the ISA-62443 series is to move as many of the security levels and requirements as possible to quantitative descriptions, requirements and metrics to establish repeatable applications of the standard across multiple companies and industries. Achieving this goal will take time, since more experience in applying the standards and data on industrial security systems will need to be acquired to justify the quantitative approach (means assigning measures on a ratio or interval scale).

When mapping requirements to the different SLs, standard developers need some frame of reference describing what the different SLs mean and how they differ from each other.

2) Results for Gap analysis in Security level/ Security level vector

According to the gap analysis, it is possible to divide security requirements into three groups:

1) Security requirements with clear classifications of security levels and quantitative descriptions (at minimum two Requirement Enhancements from IEC 62443-3-3),
2) Security requirements with partial classifications of security levels (only one Requirement Enhancements),
3) Security requirements without classifications of security levels (no Requirement Enhancements).

Table I shows the security requirements from group 1 with clear classifications of security levels and quantitative descriptions. For example, the purpose statement for group 1 is SR 2.1 – Authorization enforcement. The requirements for the four SL levels that relate to SR 2.1 – Authorization enforcement is divided according to the incremental increase in overall control system security:

- SL 1: None.
- SL 2: Authorization enforcement for all users, Permission mapping to roles.
- SL 3: Authorization enforcement for all users, Permission mapping to roles, Supervisor override.
- SL 4: Authorization enforcement for all users, Permission mapping to roles, Supervisor override, Dual approval.

Table II shows the security requirements with partial classifications of security levels. There is only one requirement enhancements for four SL. SL 1 and SL 2 are mainly without requirements specification and SL3 and SL4 have the same requirements. A more detailed breakdown and division of requirements is missing. For example, SR 3.1 communication integrity could be divided according to key lengths: SHA-256, SHA-384 and SHA 512.

Table III shows the group of requirements without classification of security levels and without requirement enhancements. This group needs to be extended for future easy implementation. For example, SR 4.3 Using encryption could be divided according to key lengths: AES 128, AES 256, AES 512 and AES 1024.

B. Gap analysis in impact of security requirements on performance/safety/usability

There is a missing relation between performance/ safety/usability and security requirements according to literature review in Section II. This gap analysis of 62443-3-3 shows that this standard describes in general security/safety/performance of these security requirements:

SR 1.8 – Public key infrastructure (PKI) certificates

- *Description*: Any latency induced from the use of public key certificates should not degrade the operational performance of the control system.
- *Gap analysis result*: There could be an impact on performance in case of (extra) delay.

SR 2.1 – Authorization enforcement

- *Description*: Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the control system. The control system shall support dual approval for those actions that could results in serious impact on the industrial process.
- *Gap analysis result*: Possible impact on performance. Security requirement could have impact on performance and safety. For example, it may delay necessary work, and, in emergencies, inhibit a user's ability to respond in a timely manner, thus posing a safety hazard. The requirement may also impact usability. For example, if required often, it may become a nuisance to some users. Authorization enforcement is one example of a requirement that requires designers to extend their focus from a single system attribute: security, to the interaction between security, safety, performance, and usability [25].

SR 2.8 – Auditable events

- *Description*: Auditing activity can affect control system performance.
- *Gap analysis result*: Possible impact on performance.

SR 3.1 – Communication integrity

- *Description*: The use of cryptographic mechanisms to provide message authentication and integrity should be determined after careful consideration of the security needs and the potential ramifications on system performance and capability to recover from system failure.
- *Gap analysis result*: Too strong cryptographic mechanisms can impact performance (delay) and safety (e.g. failure rate of crypto accelerators).

SR 3.3 – Security functionality verification

- *Description*: Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations.
- *Gap analysis result*: Bad configured real-time testing can impact performance.

TABLE I.
SECURITY REQUIREMENT FROM GROUP 1 WITH CLEAR CLASSIFICATIONS OF SECURITY LEVELS (SLS) AND QUANTITATIVE DESCRIPTIONS

ID	Title	SL1	SL2	SL3	SL4
SR 1.1	Human user identification and authentication	Passwords	Passwords, tokens, biometrics	Passwords, tokens, biometrics	Multifactor authentication
SR 1.7	Strength of password			For human users	For all users
SR 2.1	Authorization enforcement		Authorization enforcement for all users; Permission mapping to roles.	Authorization enforcement for all users; Permission mapping to roles; Supervisor override	Authorization enforcement for all users; Permission mapping to roles; Supervisor override; Dual approval.
SR 2.11	Timestamps			Internal time synchronization	Internal time synchronization; Protection of time source integrity
SR 3.2	Malicious code protection			Malicious code protection on entry and exit points	Malicious code protection on entry and exit points + Central management and reporting for malicious code protection
SR 3.3	Security functionality verification			Automated mechanisms for security functionality verification	Automated mechanisms for security functionality verification; Security functionality verification during normal operation
SR 3.8	Session integrity			Invalidation of session IDs after session termination; Unique session ID generation	Invalidation of session IDs after session termination; Unique session ID generation; Randomness of session IDs
SR 4.1	Confidentiality of information		Protection of confidentiality at rest or in transit via untrusted networks	Protection of confidentiality at rest or in transit via untrusted networks	Protection of confidentiality at rest or in transit via untrusted networks; Protection of confidentiality across zone boundaries; Protection of confidentiality on untrusted processors or memories.
SR 5.1	Network segmentation	Router	Router	Router, VLAN, proxy	Router, VLAN, proxy, VPN, firewall
SR 5.2	Zone boundary protection	Any boundary protection devices	Router, firewall	Router, firewall, backup - firewall	Router, firewall, backup - firewall
SR 7.1	DoS protection	Firewall, IPS	Firewall, IPS	Firewall, IPS	Firewall, IPS
SR 7.3	Control system backup	System backup	Verification	Verification, automation	Verification, automation

TABLE II.
SECURITY REQUIREMENT WITH PARTIAL CLASSIFICATIONS OF SECURITY LEVELS (ONLY ONE REQUIREMENT ENHANCEMENT)

ID	Title	SL1	SL2	SL3	SL4
SR 1.2	Identification and authentication of software processes and devices			Unique identification and authentication	Unique identification and authentication
SR 1.3	User account management			Unified account management	Unified account management
SR 1.5	Authenticator management			Hardware security for software process identity credentials	Hardware security for software process identity credentials
SR 1.6	Wireless access management			Unique identification and authentication	Unique identification and authentication
SR 1.9	Strength of public key authentication			Hardware security for public key authentication	Hardware security for public key authentication
SR 1.13	Access via untrusted networks		Explicit access request approval	Explicit access request approval	Explicit access request approval
SR 2.2	Wireless use control			Identify and report unauthorized wireless devices	Identify and report unauthorized wireless devices
SR 2.3	Use control for portable and mobile devices			Enforcement of security status of portable and mobile devices	Enforcement of security status of portable and mobile devices
SR 2.4	Mobile code			Mobile code integrity check	Mobile code integrity check
SR 2.12	Non-repudiation / authentication				Non-repudiation for all users

TABLE II.
SECURITY REQUIREMENT WITH PARTIAL CLASSIFICATIONS OF SECURITY LEVELS (ONLY ONE REQUIREMENT ENHANCEMENT) - CONTINUE

ID	Title	SL1	SL2	SL3	SL4
SR 3.1	Communication integrity			Cryptographic integrity protection	Cryptographic integrity protection
SR 3.4	Software and information integrity			Automated notification about integrity violations	Automated notification about integrity violations
SR 3.9	Protection of audit information				Audit records on write-once media
SR 4.2	Information persistence			Purging of shared memory resources	Purging of shared memory resources
SR 5.3	PtP communication restriction			Prohibit all general purpose person-to-person communications	Prohibit all general purpose person-to-person communications
SR 6.1	Audit log accessibility			Programmatic access to audit logs	Programmatic access to audit logs
SR 7.6	Network and security configuration settings			Machine-readable reporting of current security settings	Machine-readable reporting of current security settings

TABLE III.
SECURITY REQUIREMENT WITHOUT CLASSIFICATIONS OF SECURITY LEVELS (NO REQUIREMENT ENHANCEMENT)

ID	Title	SL1	SL2	SL3	SL4
SR 1.4	Identifier management				
SR 1.8	Public key infrastructure (PKI) certificates				
SR 1.10	Authenticator feedback				
SR 1.11	Unsuccessful login attempts				
SR 1.12	System use notification				
SR 2.5	Session blocking				
SR 2.6	Remote session termination				
SR 2.7	Concurrent session control				
SR 2.10	Response to audit processing failures				
SR 3.5	Input validation				
SR 3.6	Deterministic output				
SR 3.7	Error handling				
SR 4.3	Using encryption				
SR 5.4	Application partitioning				
SR 6.2	Continuous monitoring				
SR 7.2	Resource management				
SR 7.4	Control system recovery and reconstitution				
SR 7.5	Emergency power				
SR 7.7	Least functionality				
SR 7.8	Control system component inventory				

SR 3.5 – Input validation

- *Description*: The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.
- *Gap analysis result*: Security requirement could have impact on performance and safety.

SR 4.1 – Information confidentiality

- *Description*: It is crucial that the technique chosen considers the potential ramifications on control system performance and the capability to recover from system failure or attack.
- *Gap analysis result*: Possible impact on performance when incorrect protection technique was chosen.

SR 5.2 – Zone boundary protection

- *Description*: As part of a defense-in-depth protection strategy, higher impact control systems should be partitioned into separate zones utilizing conduits to restrict or prohibit network access.
- *Gap analysis result*: Bad zone partitioning could have impact on performance.

SR 6.2 – Continuous monitoring

- *Description*: The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.
- *Gap analysis result*: Performance monitoring does not impact performance but may have an impact if monitoring is not performed. Monitoring leads to better efficiency.

SR 7.1 – Denial of service protection

- *Description*: DoS event on the control system should not adversely impact any safety-related systems.
- *Gap analysis result*: Any DDoS filtration should not affect the rest of the system.

FR 6 – Timely response to events

- *Description*: The use of monitoring tools and techniques should not adversely affect the operational performance of the control system.
- *Gap analysis result*: Possible impact on performance when incorrect monitoring tools and techniques were chosen.

Gap analysis in impact of security requirements on performance/safety shows general description, e.g. possible impact on performance. There are missing trade-offs between security and safety/performance, methods of evaluation, quantitative descriptions, particular performance/safety indicators, metrics or repeatable methodology.

Another important relationship is that between security and usability. Security policies can be self-defeating if they reduce usability of the security mechanisms or of the systems they protect: they encourage users to circumvent them, to preserve performance and safety or simply convenience. For example, requiring complex passwords to improve security may cause users to respond by sharing passwords, having one password for many devices, keeping passwords written down next to the protected devices, reusing or recycling old passwords, etc. [14].

Thus attempts to improve security may actually harm it. Thus, requiring string security in these cases is self-defeating unless designers also ensure that users will comply, and that compliance will not dangerously harm safety and performance. Thus the U.S. National Institute of Standards and Technology and the U.K. National Cyber Security Centre recently reversed their long-standing advice on password policies, acknowledging that policies previously considered "most secure" (complex passwords, changed frequently) caused users to invent workarounds that undermined authentication [15] [25].

This gap is solved partially for particular requirements using Secure Software Development Life Cycle catalog, and containing security requirements together with the advanced modelling framework TTool based on UML/SysML-Sec. This approach [16][17] can help discovering interconnections between the security requirements (security) and its impact on the final system response (performance) during the development stage. Basically, SSDLC helps selecting security mechanisms that could answer to security requirements, see Fig 2. Then, in TTool/SysML-Sec (see Fig. 3), the complexity of these mechanisms is captured using complexity operators, both at cyphering/deciphering sides. Then, functions enhanced with security mechanisms are mapped into the system architecture. This includes the mapping of where crypto functions are executed (e.g. on general purpose processors or HW crypto accelerators) and the mapping of cryptographic material (e.g. keys). The mapping model is then simulated to evaluate the impact of added security mechanisms on performance. Performance is usually measured as the latency between two events, e.g. the reaction time to a given input until the corresponding response is produced.

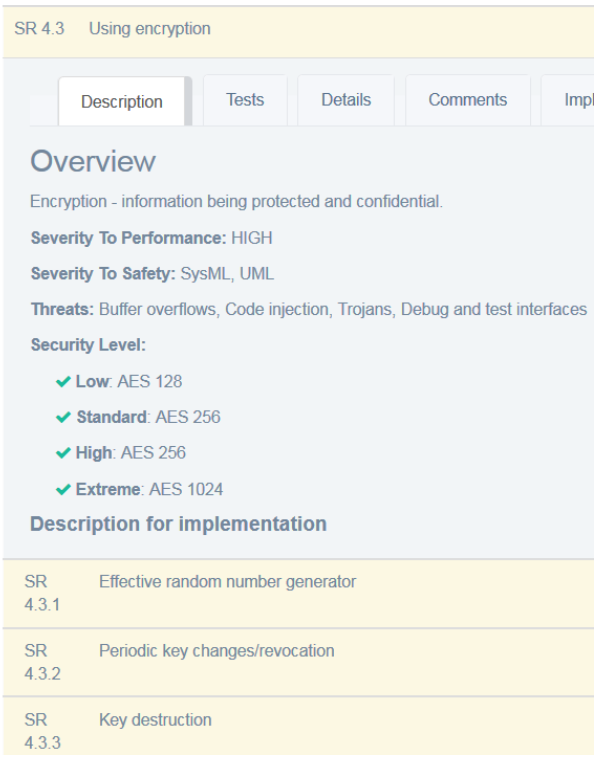

Fig. 2 SR 4.3 Using encryption – example from SSDLC.

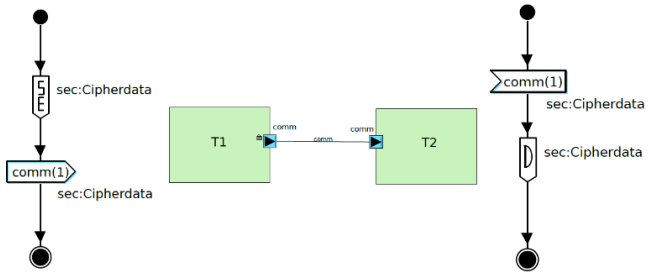

Fig. 3. Encryption/decryption model in TTool framework. Two tasks T1 and T2 communicate in a confidential way through a data channel link. The activity of T1 (left part of figure) models a ciphering scheme followed by the sending of one data sample (or packet) into the data channel. In the left part of the Figure, T2 first receives one data sample before deciphering it with the same scheme (i.e. with the same key and algorithm).

C. Gap analysis of verification methods of requirement implementations in 62443-3-3

The adequate compensating countermeasures to meet particular requirements are defined, that means should be provided. But the way how to provide them is missing.

For example, ENCS and E.DSO provide the first set of harmonised smart meter security requirements [19]. This document provides a deep description of evaluation and countermeasures of particular requirements.

1) Proposal of 62443-3-3 extension – sub requirements

The list of security requirements (SeR) based on ISA/IEC-62443 could be extended by the requirements from NIST 800-82, IEC 27001 and COBIT to obtain complex security recommendations (requirements), see Table IV.

The example of one particular requirement is shown in Table IV. The requirement "Using encryption" also contains the necessary sub-requirements to fulfil complex security aspects.

Other aspects for covering all aspects of implementing the security in the product life cycle (PLC) were also defined in SSDLC. For example, security levels, methods for verification and potential threats or attack are defined.

TABLE IV.
SECURITY REQUIREMENT – SR 4.3 USING ENCRYPTION WITH SUBREQUIREMENTS

SR 4.3	Using encryption	Encryption - information being protected and confidential.	Algorithms for Symmetric Ciphers (e.g. AES, 3DES)
SR 4.3.1	Effective RNG	Key generation needs to be performed using an effective random number generator.	RNG Validation List from NIST
SR 4.3.2	Periodic key changes/revocation	Key lifetime or the validity period is limited.	30 days, 1 year, 2 years
SR 4.3.3	Key destruction	Purging of shared memory resources - SR 4.2 – Information persistence.	
SR 4.3.4	Key backup	Recovery in case of failure or outage.	Storage and recovery according to ISO.
SR 4.3.5	Key distribution	Methods for establishing cryptographic keys.	i.e., Elliptic-curve Diffie–Hellman (ECDH)
SR 4.3.6	Key length/size	Encryption algorithm security level based on the FIPS certification	ECRYPT, NIST, BSI, ANSSI

2) Proposal of 62443-3-3 extension – countermeasures/verification

For example, the description for implementation for SR 7.1 DoS protection was proposed in the standard 62443-3-3 (firewall and IPS), but verification methods (e.g. attacks) of particular requirements are missing.

Based on co-engineering in AQUAS project, the methods for verification (attacks) were described for particular requirements in SSDLC. There are as follows:

a) Valid message during flood attack

1. The evaluator performs flood attacks containing only valid messages targeted to data inputs. The maximum power is given by the maximum capacity of the connected interface.
2. The evaluator performs a flood attack for 50 % of the input capacity and verifies the system functionality by sending a valid message.
3. The evaluator performs a flood attack for 75 % of the input capacity and verifies the system functionality by sending a valid message.
4. The evaluator performs a flood attack for 100 % of the input capacity and verifies the system functionality by sending a valid message.

b) System functionality during flood attack

1. The evaluator performs a flood attack for at least 100 % of the primary interface capacity with valid messages. The evaluator verifies that the system does not interrupt the functionality (e.g. energy measurement) during the attack.
2. The evaluator performs a flood attack for at least 100 % of the primary interface capacity with non-valid messages (TCP SYN, UDP). The evaluator verifies that the system does not interrupt the functionality (e.g. energy measurement) during the attack.

D. Proposal of new security requirements

The vendor of an equipment has to meet the requirements for lifetime expectancy, which ranges from 5 to 30 years.

ENISA in [20] defines the challenge no. 5: Amortization of ICS investments. This challenge proposed that security staff will have to deal with ICS with little or no security capabilities for the next 10 – 15 years, and this will have to be taken into account when designing security plans.

ENISA in [21] defines vulnerability Remote Processor operations. This vulnerability focused on computation power and memory resources of the processors for future security upgrades.

NIST defines in [22] the use of algorithms and key lengths specified in Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs). In this document NIST required the security strength of at least 112 bits, but for example, if the data to be encrypted have the security life of 15 years, then protection at the security strength of 112 bits will not be sufficient, since the 15-year period extends beyond 2030.

Table V shows the recommendation for key length strength according to ENISA and ECRYPT-CSA [23], [24]. In IACS and ICS, the device lifecycle of 15-years should be considered, therefore the security strength must be designed for security strength beyond 2028 or could to be changed

e.g. via firmware update during the device lifecycle.

TABLE V.
ECRYPT-CSA RECOMMENDATIONS ON KEY LENGTH

Protection	Symmetric	Factoring Modulus	Discrete Logarithm Key Group		Elliptic Curve	Hash
Legacy standard level *Should not be used in new systems*	80	1024	160	1024	160	160
Near term protection *Security for at least ten years (2019-2028)*	128	3072	256	3072	256	256
Long-term protection *Security for thirty to fifty years (2019-2068)*	256	15360	512	15360	512	512

Co-engineering in AQUAS project shows trade-offs between security and performance/safety. In some IACS and ICS systems or devices, it could be hard to implement the key length for long term protection, therefore we propose new security requirements focusing on future updates in the device's lifetime:

1) The system or device shall allow remote updates for cryptographic algorithms, credentials and key lengths.
2) The device shall have sufficient memory and computation power to allow the updates of cryptographic algorithms and key lengths.

We propose to add these new requirements in foundational requirement Resource availability (RA), for example in the following way:

SR 7.9 Future updates during lifetime

Requirement

The system or device shall allow remote updates for cryptographic algorithms, credentials and key lengths during system lifetime.

On the other hand, if this requirement is not feasible and doable (e.g. if the computation power of MCUs are not sufficient to implement new algorithms and longer key length), the new interaction between security and performance have to be solved (for example according to approach using SSDLC and TTool).

Rationale and supplemental guidance

The evaluator shall perform remote update (e.g. using FW update) of the security functionalities, cryptographic primitives and parameters.

Requirement enhancements

(1) Cryptographic algorithms (for encryption, key establishment mechanisms and integrity).
(2) Key lengths (for symmetric, factoring, modulus, discrete logarithm, elliptic curve and hash).
(3) Random Number Generators.
(4) Add roles and users.
(5) Change role authorization.
(6) Adding new security events.

Security levels

The requirements for the four SL levels that relate to SR 7.9 – Future updates during lifetime are:

- SL-C(RA, control system) 1: SR 7.9 (4)
- SL-C(RA, control system) 2: SR 7.9 (4) (5) (6)
- SL-C(RA, control system) 3: SR 7.9 (2) (3) (4) (5) (6)
- SL-C(RA, control system) 4: SR 7.9 (1) (2) (3) (4) (5) (6)

V. CONCLUSION

The paper introduced the 62443 standard gaps analysis with the goal to identify the missing parts and to propose the possible extensions. Based on this analysis the possible recommendations for extending 62443-3-3 were proposed.

REFERENCES

[1] EU Publication Office, "Aggregated quality assurance for systems: Aquas h2020 project official website," https://cordis.europa.eu/project/ rcn/210527 en.html, 2017, (H2020-EU.2.1.1.7, ID: 737475). Accessed: 2019-06-08.

[2] Jens Braband. What's Security Level got to do with Safety Integrity Level?. *8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)*, Jan 2016, TOULOUSE, France. ⟨hal-01289437⟩

[3] R. S. H. Piggin, "Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security," *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*, Birmingham, 2013, pp. 1-6. doi: 10.1049/cp.2013.0001

[4] M. Maidl, D. Kröselberg, J. Christ and K. Beckers, "A Comprehensive Framework for Security in Engineering Projects - Based on IEC 62443," *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Memphis, TN, 2018, pp. 42-47. doi: 10.1109/ISSREW.2018.00-33

[5] T. Meany, "Functional safety and Industry 4.0," *2017 28th Irish Signals and Systems Conference (ISSC)*, Killarney, 2017, pp. 1-7. doi: 10.1109/ISSC.2017.7983633

[6] M. Rekik, C. Gransart and M. Berbineau, "Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems," *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, 2018, pp. 1-9. doi: 10.1109/CNS.2018.8433201

[7] D. Zvabva, P. Zavarsky, S. Butakov and J. Luswata, "Evaluation of Industrial Firewall Performance Issues in Automation and Control Networks," *2018 29th Biennial Symposium on Communications (BSC)*, Toronto, ON, 2018, pp. 1-5. doi: 10.1109/BSC.2018.8494696

[8] H. Kanamaru, "Bridging functional safety and cyber security of SIS/SCS," *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, Kanazawa, 2017, pp. 279-284. doi: 10.23919/SICE.2017.8105699

[9] Chai Jiwen and Liu Shanmei, "Cyber security vulnerability assessment for Smart substations," *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Xi'an, 2016, pp. 1368-1373. doi: 10.1109/APPEEC.2016.7779741

[10] F. Moyon, K. Beckers, S. Klepper, P. Lachberger and B. Bruegge, "Towards Continuous Security Compliance in Agile Software Development at Scale," *2018 IEEE/ACM 4th International Workshop on Rapid Continuous Software Engineering (RCoSE)*, Gothenburg, Sweden, 2018, pp. 31-34.

[11] B. Genge, P. Haller and I. Kiss, "Cyber-Security-Aware Network Design of Industrial Control Systems," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1373-1384, Sept. 2017. doi: 10.1109/JSYST.2015.2462715

[12] X. Hao, F. Zhou and X. Chen, "Analysis on security standards for industrial control system and enlightenment on relevant Chinese standards," *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, Hefei, 2016, pp. 1967-1971. doi: 10.1109/ICIEA.2016.7603911.

[13] A. Ruiz, J. Puelles, J. Martinez, T. Gruber, M. Matschnig, B. Fischer, "Preliminary Safety and Security Co-engineering Process in the Industrial Automation Sector," *10th European Congress on Embedded Real Time Systems (ERTS 2020)*, Toulouse, France, 2020.

[14] L. Zhang-Kennedy, S. Chiasson, and P. van Oorschot, "Revisiting password rules: facilitating human management of passwords," *2016 APWG symposium on electronic crime research (eCrime)*, IEEE, June 2016.

[15] P. A. Grassi, R. A. Perlner, E. M. Newton, A. R. Regenscheid, W. E. Burr, J. P. Richer, and M. F. Theofanos, *Digital Identity Guidelines:*

Authentication and Lifecycle Management [including updates as of 12-01-2017] (No. Special Publication (NIST SP)-800-63B), 2017.

[16] R. Fujdiak et al., "Managing the Secure Software Development," *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, CANARY ISLANDS, Spain, 2019, pp. 1-4. doi: 10.1109/NTMS.2019.8763845

[17] R. Fujdiak et al., "Modeling the Trade-off Between Security and Performance to Support the Product Life Cycle," *2019 8th Mediterranean Conference on Embedded Computing (MECO)*, Budva, Montenegro, 2019, pp. 1-6. doi: 10.1109/MECO.2019.8760043

[18] ANSI/ISA-62443-3-3 (99.03.03)-2013. Security for industrial automation and control systems Part 3-3: System security requirements and security levels. Approved 12 August 2013.

[19] Security requirements for procuring smart meters and data concentrators. ENCS. 2019. Online: https://mailchi.mp/1ea0fd33e29d/encs-and-edso-provide-first-set-of-harmonised-smart-meter-security-requirements?e=017ad05f5d.

[20] Protecting Industrial Control Systems. Recommendations for Europe and Member States [Deliverable – 2011-12-09]. December 14, 2011. ENISA.

[21] Communication network dependencies for ICS/SCADA Systems, DECEMBER 2016. ENISA

[22] Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A Revision 2. Online: https://doi.org/10.6028/NIST.SP.800-131Ar2

[23] Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018.

[24] Cryptographic Key Length Recommendation, BlueKrypt - v 31.0 - June 10, 2018. Online: https://www.keylength.com/en/

[25] L. Strigini, and M. Gadala. "Human Factors Standards and the Hard Human Factor Problems: Observations on Medical Usability Standards," *Proceedings of the 13th International Joint Conference on Biomedical Engineering Systems and Technologies*. SCITEPRESS, 2020