Seeking the Relation between Performance and Security in Modern Systems: Metrics and Measures

Radek Fujdiak[1,2], Petr Mlynek[1,2], Petr Blazek[1], Maros Barabas[1], and Pavel Mrnustik[2]
[1]Brno University of Technology, Technicka St. 12 Brno 61600, Czech Republic
[2]Trustport, Purkynova St. 2845/101 Brno 612 00, Czech republic
Email: {fujdiak, mlynek, blazek}@vutbr.cz, barabas@fit.vutbr.cz, pavel.mrnustik@trustport.com

***Abstract*—Nowadays, the security, safety and performance became a crucial part of the product life cycle (PLC) in which the requirements for these parameters are continuously growing. Therefore, it is a very challenging task to provide an efficient, well-balanced solution with fulfilling all these requirements. We are focused on the relations between security, safety and performance. This paper contains early-stage results and provides a summary of security requirements based on the selected current standards and recommendations such as IEC 62443 or NIST 800-57, and our best practices. Moreover, we introduce the relations between security and performance based on established requirements. We also provide examples of security impact on performance with using open data measurements. Last but not least, the results of this article might be used in the PLC, i.e., co-engineering, future system development or research on multi-parametric methods.**

***Keywords*—Security, System performance, Product life cycle, IEC 62443.**

I. Introduction

We are living in the digital era and the modern systems need to fulfill every-day higher requirements, i.e., from security, safety or performance. Therefore, the product life cycle (PLC) is becoming fast very complex as these requirements are often contradictory (i.e., the higher security negatively impacts the performance) [1]–[3]. This creates challenging task in finding the well-balance trinity of security, safety and performance [4]. We are aware the fact that security and safety are very close and some works threats them as same such as [5]–[10]. However, we see these parameters separately, because the secure system does not necessarily need to be safe, and vice versa (i.e., the security algorithm might add crucial delay to the system and make it unsafe, because the reaction time will be to slow [11]). The example of balancing this trinity of three main parameters with selected requirements (system reaction, threat persistence, and system robustness and complexity) is displayed in Fig. 1. Naturally, there are more than just the selected requirements, which must be included in the balancing process. Nevertheless, these requirements must be always brought into the context of a specific field such as space engineering; medicine and health; transportation; industrial control and management; or others. Therefore, there are always a specific needs for the system based on the selected field.

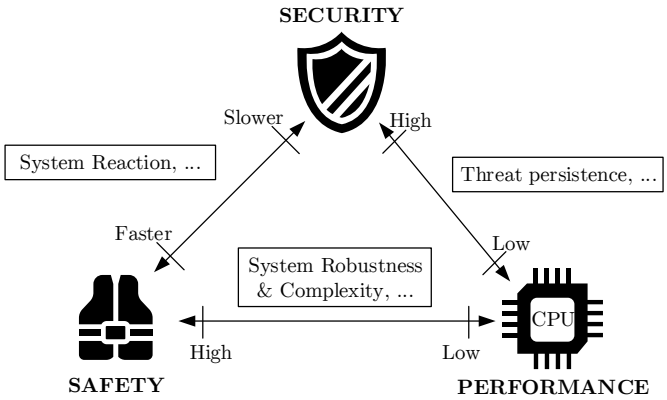

Fig. 1. An example of relations between security, safety and performance trinity with selected requirements.

Many current works are focusing on defining either security, safety or performance requirement [12]–[15] as same as the current standardization do [16]–[19]. However, the single parametric look is insufficient and it might cause variable issues in different parts of PLC, which markedly increase the research and development of the specific solution (product). This is the reason why we focus on the trinity of security, safety and performance as on the complex issue. Our research is divided for this area to two main parts: (i) establishment of main requirements from security, safety and performance; (ii) adding connections between security, safety and performance. This paper focused on methodology for the establishment of security requirements and adding their connections to the performance with clear metrics supported by results from experimental measurements.

The rest of the paper is organized as follows: Section II provides an executive summary of the current standardization as well as the norms and recommendations. Section III introduces the methodology for creating the metrics of security and performance. Further, the example is chosen in Section IV, where also relation between security and performance is provided. Finally, Section V summarizes our main contributions and conclusions.

This article has received funding within the National Sustainability Program under grant LO1401. Our research and the idea of the paper is coming from the research conducted and supported by research project Aggregated Quality Assurance for Systems (AQUAS H2020-EU.2.1.1.7 ID: 737475). For the research, the infrastructure of the SIX Center was used.

II. Executive summary of current security standards, norms and recommendations

There are many standards, norms, requirements or organizations, which define the security requirements such as [20]:

- ISO/IEC 27000, contains two main parts the 27001: Information technology - Security techniques - Information security management systems - Requirements; and 27002: best practice recommendations on information security management,
- Standard of Good Practice, it is provided by Information Security Forum as a comprehensive list of best practices for information security,
- NERC, The North American Electric Reliability Corporation, which created many standards such as NERC 1200 or NERC 1300),
- NIST, National Institute of Standards and Technology, which also creates many standards such as NIST 800-12, NIST 800-14, NIST 800-26, NIST 800-37, NIST 800-53, or NIST 800-82.
- ISO 15408, this is so called "common criteria" principally established for software applications,
- RFC 2196, which is a memorandum published for developing the security policies and procedures for information systems connected to the Internet,
- ISA/IEC-62443 (formerly ISA-99), it is a guidance that define procedures for implementing electronically secure Industrial Automation and Control Systems; and so called "IEC 62443: The Conformity Assessment Program", which is used to certify commercial off-the-shelf products and systems based on IEC 62443,
- IASME, which is similar to ISO 27001 with reduced complexity, cost, and administrative.

These are just the main items dealing with cyber-security, but there are many others, which focus for example on specific parts of the cyber-security or specific fields. However, if we look on the whole PLC, there are two main general sources for the security requirements: IEC 62443 and NIST 800-82 [21]. Moreover, the IEC 62443 and NIST 800-82 are correlate [22]. The security requirements will be define on base of these two general standards as a clear example.

A. IEC 62344

The IEC stands for International Electrotechnical Commission Standard which is an international standards organization focused on all electrical, electronic and related technologies [23]. Further, the IEC 62443 is standard, which were originally referred to ANSI/ISA-99 or ISA99 standard and renumbered in 2010 to ANSI/ISA-62443 series [24]. The original intention of the ISA-99 was to have broad standard. However, the ISA standards are mostly only US-centric without international reach. Therefore, the IEC 62443 was created as a product of collaboration with an international impact [25]. The IEC 62443 is a collection of norms, technical reports and another related information, which define procedures for the implementation in IACS (Industrial Automation and Control Systems). The instructions presented in this standards are aimed at the end user, designing, implementation, control of industrial automation and control systems and other element associated with IACS. The standard is divided into four main sections (groups), which are divided into different parts as shown in Tab. I.

TABLE I. Individual parts of the IEC 62443 standard [26].

Group	Part	Content
General	IEC 62443-**1-1**	Terminology, concepts and models
	IEC 62443-**1-2**	Master glossary of terms and abbreviations
	IEC 62443-**1-3**	System security compliance metrics
	IEC 62443-**1-4**	IACS security lifecycle and use-case
Policies & Procedures	IEC 62443-**2-1**	Requirements for an IACS security management system
	IEC 62443-**2-2**	Implementation guidance for an IACS security management system
	IEC 62443-**2-3**	Patch management in the IACS environment
	IEC 62443-**2-4**	Installation and maintenance requirements for IACS suppliers
System	IEC 62443-**3-1**	Security technologies for IACS
	IEC 62443-**3-2**	Security levels for zones and conduits
	IEC 62443-**3-3**	System security requirements and security levels
Component	IEC 62443-**4-1**	Product development requirements
	IEC 62443-**4-2**	Technical security requirements for IACS components

The first group IEC 62443 is *General*, which contains basic and general information such as terminology, concepts, and models. This section also includes security metrics and IACS cycles. The second group with title *Policies & Procedures* includes a description of how to create and maintain an effective IACS security program. The third group, the *System*, is focused on system design and requirements for secure integration of control systems. This part is crucial as it specifies the cryptographic minimum for the control system. However, the key length and types of cryptographic algorithms in the standard are not directly defines, but there are references to the standard NIST 800-57. The last main part of IEC 62443 is called *Components* and is focused on products. This part is very similar to previous section *System* with describing the product developments and technical requirements of the system to control products. In the case of cryptographic requirements, this part of the standard refers again to the NIST 800-57 as in the previous section [26].

B. NIST 800-82

The NIST is US National Institute of Standards and Technology (NIST) have produced the ICS guide similarly focused, as the other good practice already mentioned at SCADA, DCS and PLCs [16]. The purpose of the institute is a promotion of innovation in the industry, improving scientific measurement, standards, and technology with regard to economic security and quality of life. Further, the "NIST 800-82 - Guide to Industrial Control Systems (ICS) Security" standard is an an import part of NIST family of standards, which focuses on ICS (Industrial Control Systems) and has five main parts:

- Overview of ICS including a comparison between ICS and IT systems.

- Discussion of ICS risk management and assessment.
- Overview of the development and deployment of an ICS security program to mitigate the risk of the vulnerabilities.
- Recommendations for integrating security into network architectures typically found in ICS, with an emphasis on network segregation practices.
- Summary of the management, operational, and technical controls identified in "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations", and provides initial guidance on how these security controls apply to ICS [27].

Moreover, there are defined special consideration for security in ICS:

- Timeless and Performance Requirements, discusses the acceptable level of delay and jitter dictated by individual installation.
- Availability Requirements, discusses the reliability and availability based on network redundancy and self-healing.
- Risk Management Requirements, discusses both security and safety in context of fault tolerance, losses (economical, life, intellectual), damage and information.
- Physical Effects, discusses the control of physical processes and its consequences in the ICS domain.
- System Operation, discusses differences between ICS operating system and control system (CS).
- Resource Constraints, discusses the ICS system resources.
- Communications, discuss all form of communication.
- Change Management, focuses on integrity of IT and CS.
- Managed Support,
- Component Lifetime,
- Component Location.

Further, the standard 800-82 is mapping also the other NIST security standards:

- NIST 800-28 which provides guidance on active content and mobile code [28],
- NIST 800-52 which provides guidance on Transport Layer Security (TLS) implementations [29],
- NIST 800-56 which provides guidance on cryptographic key establishment [30],
- NIST 800-57 which provides guidance on cryptographic key management [31],
- NIST 800-58 which provides guidance on security considerations for VoIP technologies [32],
- NIST 800-63 which provides guidance on remote electronic authentication [33],
- NIST 800-77 which provides guidance for IPSEC VPNs [34].
- and many others.

The most important part is the NIST 800-57, which defines many different cryptographic and security requirements and parameters. Moreover, this standard give also clear overview of the cryptographic algorithm sustainability (life-time) based on the security level strength. These information might be used for security metrics establishment.

III. Metrics for Security and Performance

A. Security Metrics

The IEC 62443 standard introduced in Chapter II deals largely with defining security requirements for assets in the ICS. The security is solved in standard IEC 62443-3-2 by dividing defined assets into security zones, which are defined on the basis of common set factors [35]. For connections between different zones are used conduits which can be represented e.g. VPN connections. For each zone, there are also defined 7 fundamental requirements (FR) in the 62443 standard [26]:

- FR 1 - Identification and authentication control,
- FR 2 - Use control,
- FR 3 - System integrity,
- FR 4 - Data confidentiality,
- FR 5 - Restricted data flow,
- FR 6 - Timely response to events,
- FR 7 - Resource availability.

Each of the FR may take five security levels (SL), that are specifically defined in 62443-3-3 [26]. Below is a list of general definitions for each SL [26]:

- SL 0 - No specific requirements or security protection necessary.
- SL 1 - Protection against casual or coincidental violation.
- SL 2 - Protection against intentional violation using simple means with low resources, generic skills, and low motivation.
- SL 3 - Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills, and moderate motivation.
- SL 4 - Protection against intentional violation using sophisticated means with extended resources, IACS specific skills, and high motivation.

The number of possible variation V of FR (n = 7) and SL (k = 5) is:

$$V_k' = n^k = 5^7 = 78125. \tag{1}$$

The first SL 0 is mostly not used because it does not define any security for the FR. Therefore, we can exclude the SL0 (k = 4) to reduce the number of variation:

$$V_k' = n^k = 4^7 = 16384. \tag{2}$$

These are still too many variants to be used in the real PLC as it would make the trinity balancing very difficult. Based on our best practice, the ideal k would be 3 as it gives possibility to chose general SL and still have space for lower or higher requirements. The k = 3 also corresponds to NIST 800-82 definition of threats and security level, which also defines three levels: (i) Low, (ii) Moderate, and (iii) High [16]. However, the ideal number of variation should be in units and k = 3 leaves 2187 variations. The another possible reduction might be made with selecting specific use-case and its needs, where it would be possible to reduce the final number of variation to

units by excluding also some of the FR. Further, there must be defined appropriate representation for the combination of FR and SL, which might be a security vector [36]:

$$[X_1, X_2, X_3, X_4, X_5, X_6, X_7], \tag{3}$$

where the value of X_i stands for SL1–4 and i represents the FR1–FR7 and the represents values in range of 0–4, which stands for SL0–SL4. However, the security level is very abstract and it would not be possible to include it in the PLC processes such as design, simulations, implementation, testing and others. For the clearer definition, we can use another NIST standard publication the NIST 800-57 [31]. This standard defines five life-time levels for cryptographic algorithms, see Tab. II.

TABLE II. CORRELATION BETWEEN IEC SL AND NIST CRYPTOGRAPHY ALGORITHM LIFETIME.

SL	**Lifetime**	**Sym**	**Asym**	**ECC**	**HASH A**	**HASH B**
0	(Legacy)	80 b	1024 b	160 b	80 b	-
1	2016–2030	112 b	2048 b	224 b	224 b	-
2	> 2030	128 b	3072 b	256 b	256 b	80 b
3	≫ 2030	192 b	7680 b	384 b	384 b	224 b
4	⋙ 2030	256 b	15360 b	512 b	512 b	256 b

Note: Sym...Symmetric Algorithms; Asym...Asymmetric Algorithms; ECC...Elliptic Curves; HASH A...Digital signatures or hash-only applications; HASH B...HMAC, Key Derivation Functions or Random Number Generation.

Based on the Tab II and NIST recommendation NIST 800-57 [31], we can already define clear cryptographic algorithms for different FR as for example displayed in Tab. III for information security.

TABLE III. EXAMPLES OF SUITABLE ALGORITHMS FOR GENERAL INFORMATION SECURITY IN DEFINED SL AND FR.

FR / SL	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	SHA-1	PW_{80}	CRC32C	2TDEA	any	>s	1N
1	SHA_{224}	PW_{112}	MD5	3TDEA	periodic	<s	2N
2	SHA_{256}	PW_{128}	SHA-1	AES_{128}	periodic	<ms	3N
3	SHA_{384}	PW_{192}	SHA_{224}	AES_{192}	real-time	<us	3N5
4	SHA_{512}	PW_{256}	SHA_{256}	AES_{256}	advanced	<ns	4N

Note: FR1...Identification and authentication control (Authentication); FR2...Use control (Authorization, where PW_i stands password with i bit-length); FR3...System integrity (Integrity); FR4...Data confidentiality (Confidentiality); FR5...Restricted data flow (data flow monitoring any, static, dynamic, real-time or advanced), FR6...Timely response to events (Reactibility in time units), FR7...Resource Availability (Availability, where N stands for the nines principle, i.e. 3N5 means availability of 99.95%).

These are examples of defined metrics (SL) for selected use-case (general information security) with clear security requirements and recommendations for defined FR. Based on (3) the final vector (randomly selected) might look as follows:

$$[0, 1, 3, 3, 2, 4, 5], \tag{4}$$

which means system with these final security parameters: no identification or authentication methods (FR1), simple 80 b password (FR2), SHA-1 algorithm used for integrity (FR3), AES-128 used for data confidentiality, no monitoring for data flow (FR5), fast reactibility in seconds (FR6), and 99.99% availability (FR7).

B. Performance Metrics

There are over hundreds of performance metrics, which are influencing the PLC and might be impacted by the security solutions such as effectiveness, efficiency, cost, cycle time, productivity, waste reduction, regulatory compliance, and many others. However, the international organization MESA identified 28 most important metrics divided to [39]:

- Improving Customer Experience and Responsiveness, which contains: On-Time Delivery to Commit, Manufacturing Cycle Time and Time to Make Changeovers.
- Improving Quality, which contains: Yield, Customer Rejects/Return Material Authorizations/Returns, and Supplier's Quality Incoming.
- Improving Efficiency, which contains: Throughput, Capacity Utilization, Overall Equipment Effectiveness, and Schedule/Production Attainment.
- Reducing Inventory, which contains: Work in Process Inventory/Turns.
- Ensuring Compliance, which contains: Reportable health and safety incidents, Reportable environmental incidents, and number of non-compliance events per year.
- Reducing Maintenance, which contains: Percentage planned vs. emergency maintenance work orders and downtime in proportion to operating time.
- Increasing Flexibility and Innovation, which contains: rate of new product introduction and engineering change order cycle time.
- Reducing costs and Increasing profitability, which contains: total manufacturing cost per unit excluding materials, manufacturing cost as a percentage of revenue, net operating profit, productivity in revenue per employee, average unit contribution margin, return on assets/return on net assets, energy cost per unit, cash-to-cash cycle time, EBITDA (Earnings Before Interest, Taxes, Depreciation, and Amortization), customer fill rate/on-time delivery/perfect order percentage.

Some of the metrics are subjective and qualitative, which will always depend on the PLC manager (the company) or the end-user (the customer). However, the provided metrics has also several quantitative parameters, which could be measured and brought into the context of security, i.e., each information system has physical resource, which impacts it's final efficiency (performance), such as memory (B), energy power (Ah), processor performance (cycles), data usage (B), and others. If we bring these into the context of selected use-case, we are able to investigate also the relation between security and performance. The main attribute for the metrics should be portability that the results might be transparent and used also in different applications or cases.

The performance itself is requirement and attribute of the system. Moreover, it is always necessary to define the border value for the performance regardless the metric. The minimum performance level must be always respected.

IV. Relation between Security and Performance

The data-set was obtained from open-data benchmark, which offers results from many different experimental measurements on the Skylake Core-i5 CPU test platform with 2.7 GHz frequency [40]. The Fig. 2 provides relation between security and performance for FR1 with linear dependency.

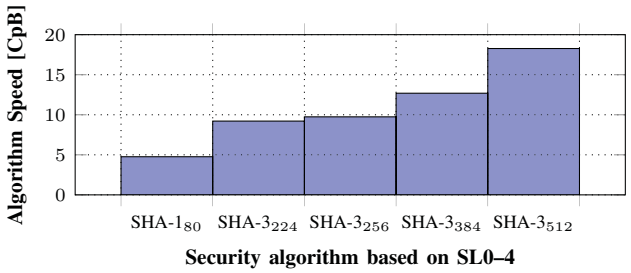

Fig. 2. The relation between SL and selected performance metric for FR1.

The FR2 would have minimum impact on the system performance as it is just simple password with fixed length for authorization. Further, the relation for FR3 is displayed on Fig. 3 with also linear dependency.

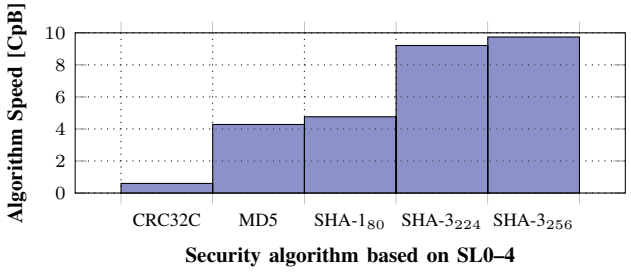

Fig. 3. The relation between SL and selected performance metric for FR3.

The relation for FR4 is displayed on Fig. 4. The anomaly for SL0 and SL1 is caused by old DES algorithm (TDEA), which is not optimized for modern systems and compared with much more modern cryptographic algorithm AES-128 is much slower as showed in the graph. The dependency is linear if we exclude the algorithms for SL0 and SL1.

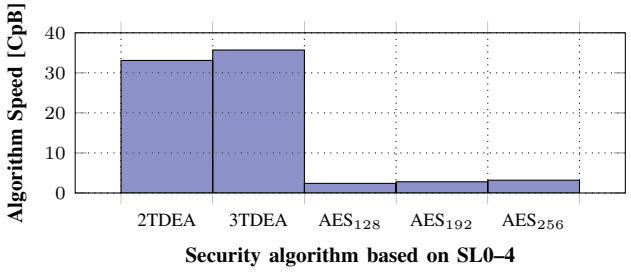

Fig. 4. The relation between SL and selected performance metric for FR4.

The relation between security and performance for FR5 is minimal if we consider the passive monitoring same as for FR6. Moreover, the FR7 is defining the reliability (availability) of the system, which should have positive effect on the performance and then the negative effect is also not considered.

V. Conclusion and Future Work

Safety, security, and performance are a key factor for operation technologies. In most of the published standards, performance is often neglected. Based on this, we focus on security standard IEC 62443, where security is divided into categories that can be used to obtain the security vector. Moreover, we consider also the correlated standard NIST 800-82, which provides a clear definition of security requirements through the other linked standards such as NIST 800-57.

Further, we bring clear methodology for defining the security level and security metrics. We brought them into the context of performance. Moreover, we provide examples of the relation between security and performance. These synergies are supported with real experimental measurements to highlight the dependency of the performance on selected security algorithm (level).

Our research and the idea of the paper is coming from the research conducted in research project Aggregated Quality Assurance for Systems (AQUAS H2020-EU.2.1.1.7 ID: 737475), which is focused among the others on investigating the trinity relation between security, safety, and performance. This paper is an early-stage research and provides the first-phase results for relation between two selected parameters. However, the future work should focus on the three-dimensional relation of all three parameters. To create clear overview of dependency for these parameters, see Fig. 5.

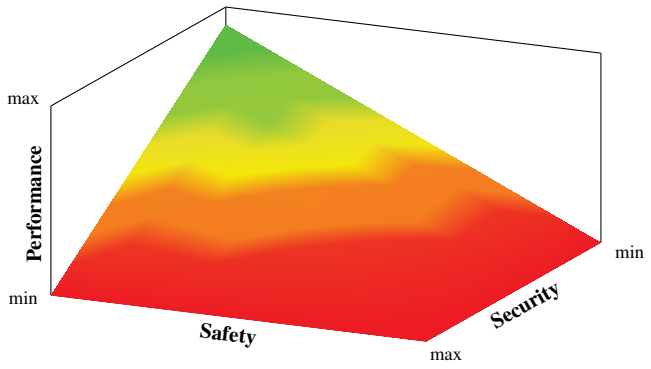

Fig. 5. Example of trinity relation between security, safety and performance.

In the real-case, there is expected that the dependency of all three parameters will not be linear or simply exponential, but much more complex. There will be necessary to investigate the possibilities to combine quantitative and qualitative metrics and inter-connections between all three parameters. However, the results should bring clear overview for OT and PLC. This should help to reduce the product expenses and provide basics for higher PLC automation.

REFERENCES

[1] M. Panda, "Performance analysis of encryption algorithms for security", in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, 2016, pp. 278-284. doi: 10.1109/SCOPES.2016.7955835, [Online].

[2] M. Orgon and I. Bestak, "Performance measurement of encryption algorithms used in PLC devices", in *International Journal of Research and Reviews in Computer Science (IJRRCS)*, 2011, Vol. 2, Iss. 5, pp. 1218-1221. doi: 10.1109/TSP.2012.6256273 , [Online].

[3] A. Ramesh and A. Suruliandi, "Performance analysis of encryption algorithms for Information Security", in *2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, 2013, pp. 840-844. doi: 10.1109/ICCPCT.2013.6528957, [Online].

[4] M. L. Winterrose, K. M. Carter, N. Wagner, and W. W. Streilein, "Balancing Security and Performance for Agility in Dynamic Threat Environments", in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2016, pp. 607-617. doi: 10.1109/DSN.2016.61, [Online].

[5] S. Casciati, Z. C. Chen, L. Faravelli, and M. Vece, "Synergy of monitoring and security", *Smart Structures and Systems*, vol. 17, no. 5, pp. 743-751, May 2016. doi: 10.12989/sss.2016.17.5.743, [Online].

[6] International Labour Office (ILO), "Occupational health and safety: synergies between security and productivity", *International Labour Office*, Geneva committee on Employment and Social Policy: GB295-ESP-3-2006-01-0211-1-En.doc/v2, 2006.

[7] Paul et al. *ITEA2 Project #11011 Recommendations for Security and Safety Co-engineering*. Eindhoven: ITEA2, NL, 2016.

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

[9] A. Gabriel, J. Shi, and C. Ozansoy, "A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method", *IEEE Access*, vol. 5, pp. 12103-12113, 2017. doi: 10.1109/ACCESS.2017.2718568, [Online].

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

[11] M. L. Winterrose, K. M. Carter, N. Wagner, and W. W. Streilein, - Balancing Security and Performance for Agility in Dynamic Threat Environments-, in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2016, pp. 607-617. doi: 10.1109/DSN.2016.61, [online].

[12] V. Liu, A. D. Tesfamicael, W. Caelli, and T. Sahama, "Network security metrics and performance for healthcare systems management", 2015, pp. 189-194.

[13] P. E. Black, K. Scarfone, and M. Souppaya, "Cyber Security Metrics and Measures", *Wiley Handbook of Science and Technology for Homeland Security*, Dec. 2008. doi: 10.1002/9780470087923.hhs440, [Online].

[14] C. Raspotnig, "Requirements for safe and secure information systems", Dissertation for the degree of Philosophiae Doctor, University of Bergen, Department of Information Science and Media Studies, Bergen, 2014.

[15] E. Schoitsch, C. Schmittner, Z. Ma, and T. Gruber, "The Need for Safety and Cyber-Security Co-engineering and Standardization for Highly Automated Automotive Vehicles", in *Advanced Microsystems for Automotive Applications 2015*, 2016, pp. 251-261. doi: 10.1007/978-3-319-20855-8_20, [Online].

[16] *NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security*, Revision 2. Gaithersburg: National Institute of Standards and Technology, 2015.

[17] E. Cosman, *The 62443 Series of Standards: Industrial Automation and Control Systems Security*. Durham: ISA99 Committee, 2018.

[18] *NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers*. Gaithersburg: National Institute of Standards and Technology, 2006.

[19] *NIST Special Publication 800-55 Revision 1: Performance Measurement Guide for Information Security*. Gaithersburg: National Institute of Standards and Technology, 2008.

[20] A. Kiyuna and L. Conyers, *CYBERWARFARE SOURCEBOOK*, 1st ed. Morrisville: Lulu Press, 2015.

[21] J. Lam, "IIET: Cyber security in modern power systems - Protecting large and complex networks", in *IET Cyber Security in Modern Power Systems*, 2016, pp. 1-12. doi: 10.1049/ic.2016.0044, [Online].

[22] E. C. Cosman and J. D. Gilsinn, *NIST Cybersecurity Framework ISA99 Response to Preliminary Version*. Research Triangle Park, NC: International Society of Automation (ISA)/The Automation Federation, 2013.

[23] *Welcome to IEC: Intenational Electrotechnical Commission*. Geneva, Switzerland, 2014.

[24] INCIBE, "EC 62443: Evolution of the ISA 99", *Certsi*, 2015. [Online]. Available: https://www.certsi.es/en/blog/iec62443-evolution-of-isa99. [Accessed: 27-Feb.-2018].

[25] R. S. H. Piggin, "Development of industrial cyber security standards: IEC 62443 for scada and industrial control system security", in *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*, 2013, pp. 11-11. doi: 10.1049/cp.2013.0001, [Online].

[26] *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*. United States of America: ISA, 2013.

[27] *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*, Revision 5. Gaithersburg: National Institute of Standards and Technology, 2017.

[28] *NIST Special Publication 800-28 Version 2: Guidelines on Active Content and Mobile Code*, Version 2. Gaithersburg: National Institute of Standards and Technology, 2008.

[29] *NIST Special Publication 800-52 Revision 1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. Gaithersburg: National Institute of Standards and Technology, 2013.

[30] *NIST Special Publication 800-56A Revision 3: Recommendation for Pair-Wise July Key Establishment Schemes Using Discrete Logarithm Cryptography*, Revision 3. Gaithersburg: National Institute of Standards and Technology, 2017.

[31] *NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General*, Revision 4. Gaithersburg: National Institute of Standards and Technology, 2016.

[32] *NIST Special Publication 800-58: Security Considerations for Voice Over IP Systems*. Gaithersburg: National Institute of Standards and Technology, 2005.

[33] *NIST Special Publication 800-63-3: Digital Identity Guidelines*. Gaithersburg: National Institute of Standards and Technology, 2017.

[34] *NIST Special Publication 800-77: Guide to IPsec VPNs*. Gaithersburg: Information Technology Laboratory, 2005.

[35] *ISA-62443-3-2 Security for industrial automation and control systems: Security risk assessment and system design*, Draft 6, Edit 2. United States of America: ISA, 2015.

[36] Jens Braband. "Whats 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. Proceedings of the 8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)

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

[38] *NIST Special Publication 800-38: Recommendation for Block Cipher Modes of Operation*. Gaithersburg: National Institute of Standards and Technology.

[39] J. Fraser, Industry Direction, and MESA, *Metrics that Matter: Uncovering KPIs that Justify Operational Improvements*. MESA International and Industry Dirtection Inc., 2006.

[40] J. Walton, "Crypto++ 6.0.0 Benchmarks", *Crypto++ Library 6.1*, 2018. [Online]. Available: https://www.cryptopp.com/benchmarks.html. [Accessed: 27-Feb.-2018].