Identifying Security Requirements Body of Knowledge for the Security Systems Engineer

Suné Von von Solms, Annlizé Marnewick

Identifying Security Requirements Body of Knowledge for the security systems engineer

Suné von Solms[1] [0000-0002-1857-1683] and Annlizé Marnewick[2] [0000-0002-7458-1296]
[1] Department of Electrical Engineering Science
[2] Postgraduate School of Engineering Management
University of Johannesburg, Johannesburg, South Africa
svonsolms@uj.ac.za

Abstract.
The interconnected nature of Industry 4.0–driven operations and systems is introducing the use of new digitized and connected industrial systems. These new connected environments impact system security, requiring engineers to include elicitation of security requirements as functional requirements. Academia and industry argue that systems engineers are not adequately prepared for the security-related activities required in the specification of secure systems. This paper utilizes a cybersecurity framework to create the body of knowledge related to Security Requirements Engineering for a module in systems engineering. The determined body of knowledge show Risk Management, Laws and Regulations, and Human Factors related to security must be considered in the changing technological landscape. Although not all systems engineers must have expert knowledge in this field, all systems engineers must have fundamental knowledge in security practice and the ability to apply systems thinking.

Keywords: Engineering education, Security, Security requirements engineering, Industry 4.0, Systems engineering.

1 Introduction

In traditional systems design, security considerations of a system were limited to the integration of security added after the completed system was developed [1, 2, 3], treating security features as of secondary importance. The Industrial Internet of Things (IIoT) defines the use of new digitized and highly connected systems [4], which require these systems to be designed, developed and managed by engineers while considering the impact and effects of cyberattacks on these systems throughout the whole system [5]. In reaction to these required changes in design, the systems engineering community identified security roles and responsibilities applicable to the entire systems development life cycle for future connected environments [6], namely the secure systems development life cycle (S-SDLC) [5]. Various sources argue that all engineering disciplines must understand and practice security through all phases of the system lifecycle to meet the project's requirements and manage an acceptable level of risk [8, 9].

In systems engineering, a holistic cybersecurity view is required by Systems Engineers (SEs) to design secure systems as the S-SDLC requires the execution of various specialized security tasks, such as security requirements planning which requires the evaluation of functional systems requirements relating to security and translation into technical solutions [11]. Globally, engineering industries are observing that SEs are not adequately prepared to execute many of these tasks, including the incorporation of system security requirements into the system [11, 12]. Therefore, industries require SEs with holistic cybersecurity knowledge and Security Requirements Engineers (SREs) who can conduct the security requirements process, minimizing the risk during systems development lifecycle [8].

In the South African (SA) engineering space, there exists a high demand in cybersecurity engineering professionals. However, throughout academic institutions in SA there are no known comprehensive cybersecurity engineering courses offered, based on their undergraduate and postgraduate syllabus descriptions [9]. In systems engineering, the lack of cybersecurity content or modules in SA engineering education and the need for cybersecurity professionals point toward a gap in cybersecurity knowledge amongst engineers in industry. The need for such a skill requires the addition of security requirements engineering to the education in systems engineering curricula [13]. The aim of this paper is to design a cybersecurity module for systems engineering students focusing on security requirements engineering.

2 The need for security requirements engineering education

Engineering industries globally are observing that SEs are not adequately prepared to incorporate system security requirements into the system [12], which constitutes the need for an additional SE who possesses the knowledge, skills and competencies related to security requirements [11]. This includes the consideration of security requirements as an integral part of system requirements to reduce systems weakness [8], treating security requirements as functional requirements and not just non-functional requirements or of secondary importance [14, 15]. However, not all system engineers can be trained to become security experts. Therefore, academia should develop security experts as a path in system engineering, including the SRE [16].

In the paper entitled “Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline”, the authors argue that cybersecurity must be integrated into existing academic disciplines, not simply be developed as separate degree programs [13]. As with a module educating SEs to have a holistic view of cybersecurity, a module must exist in which a SE responsible for requirements engineering must be educated on the security factors influencing requirement engineering. To ensure the development of relevant content for such modules, this research investigates internal and external factors of the cybersecurity and systems engineering fields which can influence and impact the content of a cybersecurity curriculum.

3 Methodology

A preliminary investigation into a basic body of knowledge of a SE cybersecurity module was presented in [10] which provided a baseline for this research. This paper builds on the work done in [10] where a broader spectrum literature was considered to inform a module in SE. The framework described by Knapp et al (2017) was developed to ensure that cybersecurity certifications remain relevant in industry, by identifying factors which professional bodies recognize as important to a relevant certification. These relevant factors are then used to inform a current curriculum to remain relevant to industry requirements.

This framework was adapted to analyze professional certifications to help shape a new cybersecurity module related to SE. The module was validated against the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) guidelines. The adapted framework followed is illustrated in Figure 1 below.

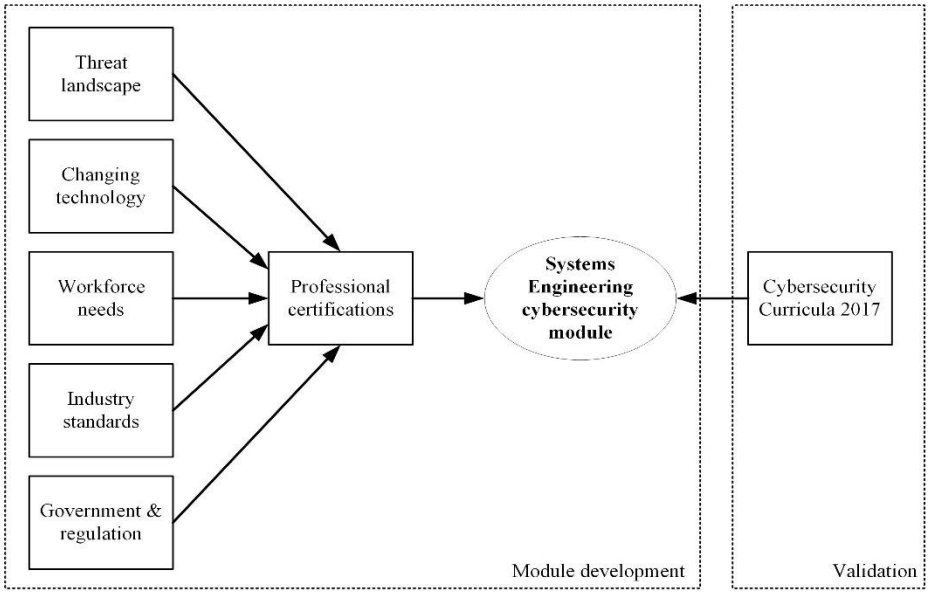

Fig. 1. Methodology for module development [17]

1. Step 1: Review the key input factors that certifying bodies consider relevant, including threat landscape, technology changes, industry standards, workforce needs, and government and regulation as per the framework in [17]. From this review, relevant cybersecurity knowledge and skills are determined.
2. Step 2: Development of a draft SE cybersecurity module from the data collected in Step 1.
3. Step 3: Validate the developed SE cybersecurity module against the CSEC2017 guidelines.

The results of the various steps are discussed in the subsequent sections.

4 Review of Input Factors

To analyze the significant factors that professional certifying bodies consider most important relating to cybersecurity in systems requirement engineering, literature was reviewed to determine specific skills, knowledge and activities relating to security in requirements engineering. The five input factors, shown in Fig. 1, is considered. This is not an exhaustive list and other factors can be considered but is considered comprehensive to provide relevant information for module development [17].

4.1 Threat landscape

The changing technological landscape constantly gives rise to new threats and risks, like protection of information and information systems and communications and network security [20]. As cybersecurity threats are constantly evolving, it is essential to consider literature discussing any new threats relating to engineering systems and how they should be managed. Traditionally, security requirements were considered as non-functional requirements [11, 14, 15]. Other instances include where security requirements are developed independently from the rest of the requirements engineering activity and hence not integrated into the requirements engineering activities [11]. Generally, this leads to serious design challenges and wide-ranging security vulnerabilities. New requirements must be considered by SEs as part of each system to create innovative solutions to address the new risks. Researchers argue that many security problems can be eliminated through the integration of security with requirements engineering [5, 7, 19]. By conducting security requirements in the early stages of the development process with the system requirements specifications, security threats can be avoided very early in the systems development process as security is adequately planned, acquired, built in, and deployed as an integral part of the system [5, 7, 19].

NIST Special Publication 800-64 - Security Considerations in the System Development Life Cycle [7] comments on the enforcement of security requirements throughout the phases of the life cycle. Nejib and Beyer (2016) comment on the importance of systems engineers towards contributing to secure systems [8]. They considered current and evolving policies, guidance, and standards (ISO 15288:2015) regarding security activities in the S-SDLC and provide a framework which identifies the security-related activities applicable to systems engineers. The 5 SE processes related to requirements engineering was identified as important processes which an SRE should implement.

The identified 5 processes will be used as inputs to the cybersecurity module. The output of this investigation yielded the following [8]:

- Elicit Stakeholder Requirements
- Define Stakeholder Security Requirements
- Analyse and Maintain Stakeholder Security Requirements
- Define Systems Security Requirements
- Analyse and Maintain Systems Security Requirements

4.2 Workforce needs

Von Solms and Marnewick (2018) identified that within the S-SDLC, specialized security-related requirement actions relevant to the 5 processes identified in Section 4.1 requires the skills of a System Requirements Planner – a position generally filled by a SE [11]. To identify the tasks, skills, knowledge and abilities required by the SE to perform these tasks, the 81 tasks, skills, knowledge and abilities documented in NIST 800-181 relating to this position were investigated. The factors relevant to the requirements engineering process (5 processes identified in section 4.1) were determined.

The output of the analysis is shown in Table 1 below where the NIST code in provided with a shortened description. These 22 identified factors will be used as inputs to the cybersecurity module.

Table 1. Tasks, skills, knowledge and abilities requirements from NIST 800-181 [22]

Code	Table 2 reference code	Code	Table 2 reference code
T0033	Risk assessment & feasibility study	K0012	Requirements analysis
T0039	Functional requirements evaluation	K0038	Data risk management
T0052	Scope definition	K0044	Cybersecurity and privacy
T0062	Requirements development	K0045	Security systems engineering principles
T0127	Integration of security policy & regulation	K0067	SDLC process
T0174	Needs analysis	K0102	SDLC process
T0235	Requirements modelling	K0164	Functionality, quality, and security requirements integration
T0300	User interface requirements		
T0454	Baseline requirements	S0008	System analysis
K0002	Risk management	S0010	Requirements analysis
K0003	Cybersecurity regulation & laws	S0050	Requirements modelling
K0004	Cybersecurity and privacy	S0134	Review and validation
K0005	Cyber threats and vulnerabilities	S0367	Cybersecurity privacy principles application
K0006	Impact analysis	A0064	Translate requirements operational impact
K0008	Operational business domain knowledge	A0123	Cybersecurity privacy principles application

4.3 Changing technology

Changing technological landscapes, including Industry 4.0 requirements, bring changes to the cybersecurity landscape. The security areas will differ for each new system, so the SRE must be able to elicit the security requirements upfront, impacting the system in development. Salini et al [19] states that every SRE must have the knowledge related to various types of security requirements and factors which influence requirements. Elicitation of requirements includes considering various non-technical aspects, which includes standards and best practices [11], laws and regulations, as well as knowledge relating to human factors, which can be considered expert knowledge to be used as input to security requirements engineering and threat analysis.

The Cyber Security Body of Knowledge (CyBOK) is one framework developed to provide guidance on the foundational and generally recognized knowledge on cybersecurity [23]. To identify the cybersecurity body of knowledge which applies to the SRE, the 19 top-level knowledge areas (KAs) documented in the CyBOK were evaluated. The category “Human, Organizational, and Regulatory Aspects” were considered relevant to the SRE as humans, organizations and regulations must be considered when

requirements are defined. The output of the analysis is shown in Table 2 below where a unique code in provided with a shortened description. These 3 identified factors will be used as inputs to the cybersecurity module.

Table 2. Cybersecurity knowledge requirements from CyBOK [23]

Code	Table 2 reference code
CyBOK1	Risk Management and Governance: Security management systems and organizational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
CyBOK2	Laws and Regulation: International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
CyBOK3	Human Factors: Usable security, social and behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours.

4.4 Industry standards

Industry standard and best practices are considered an important input toward curriculum relevance. Various industry standards and guidelines relating to cybersecurity, including ISO and NIST security frameworks, provides authoritative guidelines, frameworks and procedures to be adopted by industry [17, 24].

Upon the investigation of the eCompetence framework, it was seen that security aspects are only defined in the "Build" function much later in the S-SDLC. This implies that security forms part of the design, but no more detail is provided. Considering security requirements in the eCompetence framework, it was only included in the "Run" phase of the SDLC, implying that security only forms part of the reaction and maintenance processes of a system and not the requirements [25]. A second investigation into the NIST 800-160 [26] framework as well as the INCOSE Systems Engineering Handbook [27] was conducted. These frameworks describe the use of the technical Systems Engineering and Software processes set out in ISO/IEC/IEEE 15288:2015. Nejib et al (2016) mapped the Security Systems Engineering processes described in the NIST 800-160 framework technical processes of ISO/IEC/IEEE 15288:2015, resulting in 27 Security Systems Engineering processes [8]. From these processes, five were related to the Security Requirements phase of the S-SDLC. These five processes were identified in Section 4.1, which already formed part of the input factors to the curriculum.

4.5 Government and Regulation

Following the evaluation done on the key input factor of Changing Technology, is was determined that law and regulations must be viewed as stakeholders in the requirements process. When a system is designed, the requirements of these laws and regulation must be integrated into the requirements of the system itself. Kotonya and Sommerville (1998) commented on the inputs and outputs of the requirements engineering process and stated that two inputs include Organizational Standards and Regulations [25]. In the same manner, all regulations and standards related to cybersecurity must be included in the Security Requirement Specification process. As stated in Section 4.3,

knowledge relating to cybersecurity laws and regulations can be considered specialized knowledge and must be considered as an input factor the curriculum design.

5 Module Development

The input factors identified in Section 4 is now utilized to design a cybersecurity module for systems engineering students focusing on security requirements engineering. The cybersecurity knowledge, tools and skills identified in Section 4 require various levels of understanding by the SRE, ranging from a holistic view regarding systems security to specialized knowledge relating cybersecurity laws and regulations to elicit relevant requirements.

Kossiakoff et al. (2011) derived a range of educational components relating to systems engineering development, based on quality work experience and professional certifications [29]. These components include three overhead components, namely engineering process training, systems thinking activities and systems engineering work experience, each consisting of three sub-activities each. Adapting the generalized activities presented in [29] to the field of requirements engineering, the following development activities were identified to use as a guideline in the development of a module for SREs:

- Engineering process training: which include Process Knowledge, Tools and techniques and Skills
- Systems thinking activities which include Security discipline expertise, Problem solving and Holistic view

The evaluation of the threat landscape in Section 4.1 identified five engineering processes relating to requirements engineering in the S-SDLC. These processes are viewed in relation to the six engineering development activities listed above to generate a Body of Knowledge (BoK) table, namely the rows and columns of the table, respectively. This BoK table is populated by mapping all the knowledge, skills, abilities and tasks identified in the other sections of Section 4 to the six engineering processes and developmental activities. The BoK table is shown in Table 3 below.

This populated table provides an overview on the cybersecurity module for SE students. The columns of the BOK table are the five processes related to the Security Requirements phase of the S-SDLC identified in Sections 4.1 and 4.4. The table is populated with the knowledge, skills, abilities, tasks and requirements identified in Sections 4.2, 4.3 and 4.5. This table can provide guidance to determine the content of a Security Requirements Engineering module in systems engineering as the codes in the table indicate the topics of interest for each Security Requirements process in the S-SDLC.

Table 3: Body of Knowledge for Security Requirements Engineering module

		Stakeholder Needs and Requirements Definition Process			**System requirements definition process**	
		Elicit stakeholder requirements	**Define stakeholder security requirements**	**Analyse and maintain stakeholder security requirements**	**Define system security requirements**	**Analyse and maintain system security requirements**
Engineering process training	Process knowledge	Needs analysis (T0174) Law and Regulation (CyBOK2)	Functional requirements evaluation (T0039) Scope definition (T0052)		Risk assessment & feasibility study (T0033) Requirements development (T0062)	Integration of security policy & regulation (T0127)
	Tools and techniques			Baseline requirements (T0454)		Requirements modelling (S0050) (T0235)
	Skills			Requirements analysis (K0012 & S0010)		User interface requirements (T0300) System analysis (S0008)
Systems thinking activities	Security discipline expertise	Risk Management (K0002) Cybersecurity regulation & laws (K0003) Cybersecurity and privacy (K0004) Cyber threats and vulnerabilities (K0005) Impact analysis (K0006) Security systems engineering principles (K0045) Local and industry regulation	Security systems engineering principles (K0045)	Security systems engineering principles (K0045) Human Factors (CyBOK3)	Data risk management (K0038) Security systems engineering principles (K0045) Risk Management and Governance (CyBOK1)	Security systems engineering principles (K0045)
	Problem solving	Operational business domain knowledge (K0008) Cybersecurity privacy principles application (A0123 & S0367) Cybersecurity & privacy (K0044)	Cybersecurity privacy principles application (A0123 & S0367)	Translate requirements operational impact (A0064)	Cybersecurity privacy principles application (A0123 & S0367)	Translate requirements operational impact (A0064)
	Holistic view	SDLC process (K0067 & K0102)	SDLC process (K0067 & K0102)	Review and validation (S0134)	Functionality, quality, and security requirements integration (K0164)	Review and validation (S0134)

Table 3 presents the content for the cybersecurity module for security requirements within a SE curriculum. From the table mapping the systems thinking ability is very important for the future and a lot of focus should be in this area to help teach future students to think in this manner.

6 Module validation

The CSEC2017 framework provides guidance for education efforts in cybersecurity [18] which offers a sound guideline for the validation of the developed module. The CSEC framework divides the cybersecurity content into 8 KAs and states that the content must be aligned to workforce needs by viewing the work through a disciplinary lens. In the development of a cybersecurity module for SEs, von Solms and Futcher (2018) identified systems engineering as the disciplinary lens and determined that 3 of the 8 knowledge areas can be considered too technical for the systems engineering domain [10]. Building on this research, the 5 KAs considered in the validation of this developed module are Software, System, Human, Organizational and Societal security.

The five processes which formed the headings of Table 3 columns were used as the divisions for five module units of work. Using the key words of the various knowledge, skills, abilities and tasks included as entries in the Table 3, the CSEC2017 document was investigated and corresponding KAs and knowledge units (KUs) were identified and indicated in Table 4. When a corresponding CSEC2017 KU could not be found, an addition entry was added to Table 4, named "Systems Engineering Specialized".

Table 4. Security Requirements Engineering Module outline

		Stakeholder Needs & Requirements Definition Process			**System requirements definition process**	
		Elicit stakeholder requirements	Define stakeholder security requirements	Analyse & maintain stakeholder security requirements	Define system security requirements	Analyse and maintain system security requirements
Software Security	Essentials	X	X		X	
	Design	X	X		X	
	Analysis and Testing		X		X	
	Ethics	X				
System Security	Essentials					X
	System Thinking	X	X	X	X	X
	System Management	X				X
	System Control		X			
	System Testing		X		X	
Human Security	Essentials	X		X		
	Social Engineering	X		X		
	Awareness and Understanding	X		X		
	Social & Behavioral Privacy	X		X		
	Personal Privacy & Security	X		X		
	Usable Security and Privacy	X		X		
Organizational Security	Essentials	X				
	Risk Management	X			X	
	Security Governance & Policy	X	X		X	
	Cybersecurity Planning	X				
	Security Program Management	X	X			
	Personnel Security	X				
	Security Operations	X				

Societal Security	Essentials	X				
	Cybercrime		X			
	Cyber Law	X				
	Cyber Ethics	X				
	Cyber Policy	X				
	Privacy	X	X		X	
Systems Engineering Specialized	Needs analysis	X				
	Requirements tools & modelling					X
	System analysis					X
	Impact analysis	X				
	Security SE principles	X	X	X	X	X
	SSDLC process	X				
	Functionality, quality, and security requirements integration				X	

7 Discussion & Recommendations

From the validation process shown in Table 4, emphasis is placed on five main KAs:

- Systems Thinking: As a SE, the professional must have skill of systems thinking and be able to view a system holistically.
- Risk Management and Governance: The SE must be able to implement and understand risk management of systems and organizational security controls, which requires knowledge of applicable standards, best practices, and approaches. In addition, the new threats that the connected systems introduce must be analysed and risk estimations must be done during requirements phase.
- Security systems engineering principles: The SE responsible for the security requirements engineering needs to have expert knowledge in the security discipline.
- Law and Regulation related to Cybersecurity: All local and international statutory and regulatory requirements, compliance obligations, and security ethics, must be known to elicit security requirements.
- Human Factors: Knowledge relating to human factors and user behaviours and how it impacts security, security culture and awareness must be known by SREs.

These observations support the findings in Table 3 where it was shown that systems thinking skills must be considered in the changing technological landscape. However, the SE must have fundamental expert knowledge in security practice and the ability to apply systems thinking. Security threats will change, and the SE must be able to consider all possible scenarios when specifying requirements. Due to technological changes in systems, this module needs to be developed and used in the training of specialized SEs to prepare them for the changes brought forth by changing technological landscapes.

8 Conclusion

The creation of systems to comply with Industry 4.0 environments and cyberattacks requires the elicitation of security requirements from various sources, including regulations, client needs and human behavioral factors. The elicitation of these security requirements requires a SE who are specialize in the field of security requirements engineering and had specialized knowledge relating to various security aspects which may influence the security requirements of the system.

Engineering education is SA does not include comprehensive cybersecurity modules in systems engineering and does not provide specialized education in the field of security requirements engineering. This paper includes an investigation to determine the BoK for the creation of a module which specializes in security requirements engineering. Input factors from industry were considered to determine the knowledge, skills, abilities and tasks required for security requirements elicitation. The CSEC2017 framework were utilized to validate the educational content to be included in the module. The basic BoK for a security requirement engineering module is presented, which shows that the KAs of Systems Thinking, Risk Management and Governance, Security systems engineering principles, Law and Regulation related to Cybersecurity and Human Factors are the most important for inclusion in the module.

This work will contribute to cybersecurity curriculum design in systems engineering and other specialized systems engineering fields, such as security requirements engineering. This work can also be used as a roadmap for the development of SE modules outside of SA, as it is based on international standards and best practices. However, the laws and regulations relevant to the specific country must be considered.

References

1. Dove, R., Bayuk, J., Wilson, B., Kepchar, K. INCOSE System Security Engineering Working Group Charter (2016). https://www.incose.org/docs/default-source/wgcharters/systems-security-engineering.pdf?sfvrsn=cc0eb2c6_8
2. Shreyas, D. Software Engineering for Security: Towards Architecting Secure Software, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.4064&rep=rep1&type=pdf , last accessed 2018/05/05 (2001).
3. Haridas, N. Software Engineering – Security as a Process in the SDLC. SANS Institute InfoSec Reading Room (2007).
4. Kiel, D. What do we know about "Industry 4.0" so far? . In: Proceedings of the International Association for Management of Technology (IAMOT) (2017)
5. Waslo, R., Lewis, T., Hajj, R., Carton, R.: Industry 4.0 and cybersecurity Managing risk in an age of connected production. Deloitte University Press (2017). https://www2.deloitte.com/insights/us/en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html.
6. Nejib, P., Beyer, D., Yakabovicz, E.: Systems Security Engineering: What Every System Engineer Needs to Know. INCOSE Intnl. Symp. vol. 27, no. 1, pp. 434-445, (2017).
7. Kissel, R. L., Stine, K. M., Scholl, M. A., Rossman, H., Fahlsing, J., Gulick, J.: Security Considerations in the System Development Life Cycle. NIST (2008).
8. Nejib, P., Beyer, D.: Systems Security Engineering Whose Job Is It Anyway. INSIGHT. vol. 19, no. 2, pp. 47-53, (2016).

9. Tamura, E. Hewlett Packard Enterprise Leads Transformation of Cyber Defense with "Build it In" and "Stop it Now" (2016). http://www8.hp.com/us/en/hp-news/press-release.html?id=2184147#.WtlU5S6uyUl. Accessed 20 April, 2018.
10. von Solms, S., Futcher, L.: Identifying the Cybersecurity Body of Knowledge for a Postgraduate Module in Systems Engineering. Information Security Education – Towards a Cybersecure Society, pp. 121-132, Cham: Springer International Publishing (2018).
11. von Solms, S., Marnewick, A.: Towards Educational Guidelines for the Security Systems Engineer. Information Security Education – Towards a Cybersecure Society, pp. 57-68, Cham: Springer International Publishing (2018).
12. Bayuk, J.: Systems security engineering: A research roadmap. Systems Engineering Research center (2010). https://www.fbiic.gov/public/2010/sep/SERC-2010-TR-005-Security.pdf. Accessed 7 March 2019.
13. Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Josang, A., Pereira, T., Stavrou, E. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In: Proceedings of the Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (2018)
14. Bayuk, J. L.: Systems Security Engineering. IEEE Security & Privacy. vol. 9, no. 2, pp. 72-74, (2011).
15. Batcheller, A., Fowler, S. C., Cunningham, R., Doyle, D., Jaeger, T., Lindqvist, U.: Building on the Success of Building Security In. IEEE Security & Privacy. vol. 15, no. 4, pp. 85-87, (2017).
16. Oren, J. C.: What Does a Systems Security Engineer Do and Why Do Systems Engineers Care? INSIGHT. vol. 16, no. 2, pp. 16-18, (2013).
17. Knapp, K. J., Maurer, C., Plachkinova, M.: Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. Journal of Information Systems Education. vol. 28, no. 2, pp. 101-113, (2017).
18. Burley, D.L., Bishop, M., Buck, S., Futcher, L., Gibson, C.D., Hawthorne, E., Kaza, S., Levy, Y., Mattord, H., Parrish, A. Cybersecurity Curricula 2017, (2017).
19. Salini, P., Kanmani, S.: Survey and analysis on Security Requirements Engineering. Computers & Electrical Engineering. vol. 38, no. 6, pp. 1785-1797, (2012).
20. Squires, A., Wade, J., Dominick, P., Gelosh, D.: Building a competency taxonomy to guide experience acceleration of lead program systems engineers. Stevens Institute of Technology HoBoKen NJ School of Systems and Enterprises (2011). Accessed 30 January 2019
21. Bayuk, J. L.: Systems-of-Systems Issues in Security Engineering. INSIGHT. vol. 14, no. 2, pp. 22-25, (2011).
22. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST (2017). Accessed
23. Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., Peersman, C.: Scoping the Cyber Security Body of Knowledge. IEEE Security & Privacy. vol. 16, no. 3, pp. 96-102, (2018).
24. Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of Power in Creating de jure Standards: Shaping an International Information Systems Security Standard. MIS Quarterly, 30(Special Issue), 413-438.
25. European committe for standardization, "European e-Competence framework 3.0," 2016.
26. Ross, R., McEvilley, M., Oren, J. C.: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. vol. 800-160, National Institute of Standards and Technology (2016). Accessed 28 January 2019
27. Walden, D. D., Roedler, G. J., Forsberg, K. J., Hamelin, R. D., Shortell, T. M.: INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Wiley (2015).
28. Kotonya, G., Sommerville, I.: Requirements Engineering Processes and Techniques. Chichester: John Wiley & Sons (1998).

29. Kossiakoff, A., Sweet, W. N., Seymour, S. J., Biemer, S. M.: Systems Engineering Principles and Practice: Second Edition. New York: Wiley (2011).