Identifying the Cybersecurity Body of Knowledge for a Postgraduate Module in Systems Engineering

Sune Solms, Lynn Futcher

Identifying the Cybersecurity Body of Knowledge for a Postgraduate Module in Systems Engineering

S von Solms[1] [0000-0002-1857-1683] and L Futcher[2][0000-0003-0406-8718]

[1] Department of Electrical Engineering Science,
University of Johannesburg, Johannesburg, South Africa
[2] School of Information and Communication Technology,
Nelson Mandela University, Port Elizabeth, South Africa
svonsolms@uj.ac.za, Lynn.Futcher@mandela.ac.za

Abstract. In the light of Industry 4.0, there exists a drive in engineering to include cybersecurity in the design, development and maintenance of smart cyber-physical systems. The high interconnectivity of these systems make these systems more susceptible to cyberattacks. In South Africa, the engineering education space does not traditionally cater for cybersecurity training in undergraduate or post-graduate studies. The lack of cybersecurity education in engineering and the need for cybersecurity knowledge in the industry highlights a knowledge gap in the field of cybersecurity engineering. This paper describes the process followed to determine the body of knowledge which should be considered for a postgraduate module in cybersecurity in engineering in South Africa. Findings show that topics related to Software Security, Systems Security and Organizational Security are deemed most important for inclusion in the cybersecurity body of knowledge for a postgraduate module in Systems Engineering.

Keywords: Cybersecurity, Curriculum design, Systems Engineering, Education, Postgraduate Education.

1 Introduction

Industry 4.0, referred to as Industrial Internet of Things (IIoT) or the fourth industrial revolution, describes the use of new digitized and connected industrial systems [1]. In the light of these new developments, the systems designed by engineers are fundamentally changing. The interconnected nature of systems developed for Industry 4.0, called Industry 4.0-ready systems, means that cyberattacks can have extensive effects on these engineering systems – more so than in the past. Therefore, engineers designing, developing, managing and operating these systems should treat security as a key concern, incorporating security across the entire lifecycle from the start [2, 3].

The cybersecurity workforce worldwide is one of the fastest growing fields globally, with gaps in the workforce estimated to reach 1.8 million by 2022 [4, 5, 6, 7]. South Africa (SA) is also low in cybersecurity professionals, evident from the number of cybersecurity engineering positions advertised and vacant [8]. Many students graduating

from engineering degrees in SA lack the cybersecurity knowledge and skills needed within their specific engineering industry as they often receive only an overview of cybersecurity [4, 9, 10]. The lack of cybersecurity content in South African engineering education creates a gap in cybersecurity knowledge amongst engineers in industry.

This paper describes the process followed to determine the body of knowledge which can be considered in a postgraduate cybersecurity module for Systems Engineering in SA. The paper is structured as follows: Sections 1 and 2 present the introduction and background to the paper, while Section 3 discusses the research methodology followed. Section 4 highlights the significance to engineering education for the cybersecurity knowledge areas prescribed by the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017). Section 5 presents feedback from engineering professionals relating to body of knowledge, where Section 6 concludes the paper.

2 Curriculum development for the cybersecurity skills gap

Industry and professional institutes are driving strategies to update engineering frameworks to include security. The National Institute of Standards and Technology (NIST) published the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, providing guidance on workforce development, training and education of cybersecurity professionals [11]. The International Council of Systems Engineering (INCOSE) chartered a working group to update formal systems engineering processes to include security "as a fundamental part of system engineering" [12]. Engineering organizations are starting to recognize that security integration in engineering systems cannot only be limited to the IT industry, but that it must be included in software development, risk management, human factors and all other areas within an organization [13, 14]. There exists a high demand in cybersecurity professionals in the engineering space in SA, indicative that little progress has been made in the education space. Throughout academic institutions globally, only a handful of undergraduate and postgraduate degrees in cybersecurity exist. In SA, there are no known comprehensive engineering cybersecurity courses offered by South African universities, based on their undergraduate and postgraduate syllabus descriptions [10]. 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 CSEC2017 guideline provides comprehensive curricular guidance for cybersecurity education efforts. It aims to support the development of future programs and associated educational efforts at the post-secondary level [4]. This framework provides clear guidance which can be utilized in the development of cybersecurity courses in engineering in SA. CSEC2017 states that it should be used in collaboration with competencies defined in the workplace. Therefore, the development of an engineering cybersecurity module requires input from the engineering industry to ensure that the competencies and knowledge included in the module accurately map to the industry needs.

3 Methodology

The aim of this paper is to identify the knowledge areas to be included in a module to provide engineers with cybersecurity knowledge relevant to the industry. To ensure that the knowledge gained by engineering students are deemed relevant in the engineering industry, input from engineering professionals is required. The methodology followed in this study for the identification of cybersecurity content for engineers is shown in the four steps below. The 32-item checklist of the consolidated criteria for reporting qualitative studies (COREQ) was used as a guideline to ensure complete and transparent reporting, comprehensiveness and credibility of this research [15].

1. To investigate the qualification standard and educational requirements for postgraduate studies set out by the Department of Higher Education (DHET) in SA.
2. To determine the broad structure for module development set out in the CSEC2017 guidelines.
3. To investigate the CSEC2017 cybersecurity knowledge areas and how the content relates to the engineering profession, viewed through the disciplinary lens.
4. To construct a module outline, based on the CSEC2017 cybersecurity knowledge areas, relevant to a cybersecurity module in engineering.

Following the process set out in the COREQ criteria, steps 1 and 2 listed above was conducted to clarify the theoretical framework underpinning this study. This framework, discussed in Section 4, organizes the 8 knowledge areas in the CSEC2017 into a structured format to be used as a guideline in the elite interviews (step 3) [15, 16]. Elite interviews were selected as it advances the research process by gathering rich detail about key professional's thoughts and attitudes toward the research topic [17, 18, 19]. In-depth and semi-structured elite interviews were conducted to explore the experiences of participants in the engineering industry and academia and how it relates to the CSEC2017 framework [19, 20]. The design of the elite interviews as well as the analysis and findings are discussed in Section 5. Step 4, discussed in Section 5, follows a general inductive approach to summarize the data collected from the interviews; to determine the links between the research objectives and the findings; and finally to construct a module outline deduced from the collected data (20].

4 Towards determining the structure/context for a cybersecurity engineering module

4.1 Overview of South African postgraduate engineering degrees

The Bachelor of Engineering (B.Eng) degrees in SA are structured to provide a coherent core in mathematics, natural sciences and engineering fundamentals for a solid platform for further studies [21]. The Higher Education Qualifications Sub-Framework (HEQSF) states that a B.Eng degree must provide graduates with a well-rounded, broad

education to prepare them for ”professional training, post-graduate studies or professional practice in a wide range of careers” [22]. The B.Eng program is structured so that engineers will be able to further deepen their knowledge on a specific, sub-discipline, or specialist topic as the need arises. As the B.Eng degree is structured toward a more general engineering knowledge base, the creation of degrees or modules dedicated to cybersecurity should be developed at the postgraduate level.

HEQSF stipulates two variants of a Master’s degree: a research Master’s degree by dissertation, or a Master’s degree by coursework and mini-dissertation. A research Master’s degree requires a student to complete a single advanced research project in a specialized field of study. A coursework Master’s degree requires students to complete a coursework programme to provide a broad exposure to a field. Generally, engineering professionals from industry are more inclined to pursue a coursework Master’s as it provides a broad understanding of the field of study. The University of Johannesburg (UJ) in SA is in the process of finalizing a coursework Master’s degree in Systems Engineering with the aim to provide engineering professionals specialized systems engineering knowledge. As there exists a drive from industry to include security into the development of new engineering systems in general, the inclusion of a cybersecurity module for the Systems Engineering coursework Master’s qualification is motivated.

4.2 Cybersecurity curricular guidelines

CSEC2017 indicates that cybersecurity programs require curricular content which includes the theoretical and conceptual knowledge essential to understanding the discipline. It states that the content which must be included in any cybersecurity program must have a balance of “breadth and depth, along with an alignment to workforce needs”. The CSEC2017 model divides the cybersecurity content into 8 knowledge areas along with 6 cross cutting concepts. These knowledge areas and concepts must be viewed through a disciplinary lens which represents the underlying discipline which will form the foundation of the cybersecurity module, in this case, engineering [4].

Knowledge areas. The 8 knowledge areas stipulated in the CSEC2017 include: Data, Software, Component, Connection, System, Human, Organizational and Societal Security. Each area contains a range of knowledge units and related topics. Apart from the 8 knowledge units and related topics included in a knowledge area, each knowledge area contains a number of essential topics which should be included in every cybersecurity program. These topics capture the skills and knowledge that all students introduced to cybersecurity should acquire, regardless of discipline or program focus and is CSEC2017 states that essential topics should be included early in cybersecurity programs and reinforced throughout. As the envisaged postgraduate cybersecurity module aims to introduce engineers to the concepts of cybersecurity, these essentials must be covered in the module. These topics are provided in Table 1.

Table 1. Overview of essential topics included in each Knowledge Area

Knowledge Area	Essentials
Data Security	Basic cryptography concepts; Digital forensics; End-to-end secure communications; Data integrity & Authentication; Information storage security.
Software Security	Fundamental design; Security requirements & role in design; Implementation issues; Static & dynamic testing; Configuring & Patching; Ethics.
Component Security	Vulnerabilities of system components; Component lifecycle; Secure component design principles; Supply chain management security; Security testing; Reverse engineering.
Connection Security	Systems, architecture, models, & standards; Physical component interfaces; Software component interfaces; Connection attacks; Transmission attacks.
System Security	Holistic approach; Security policy; Authentication & Access control; Monitoring; Recovery and Testing; Documentation.
Human Security	Identity management; Social engineering; Awareness & Understanding; Social behavioral privacy and security; Personal data privacy and security.
Organizational Security	Risk management; Governance & Policy; Laws, ethics & compliance; Strategy & planning.
Societal Security	Cybercrime and Cyber law; Cyber ethics; Cyber policy; Privacy.

Cross cutting concepts. CSEC2017 indicates that the knowledge areas are not mutually exclusive. There exist cross cutting concepts which provide students with an understanding of how the various knowledge areas relate to each other and reinforces the security mindset which they should possess. The 6 cross cutting concepts are: Confidentiality, Integrity, Availability, Risk, Adversarial Thinking and Systems Thinking. These concepts must be included throughout the envisaged engineering module.

Disciplinary lens. CSEC2017 states that a cybersecurity program must be created through the view of a specific disciplinary lens, representing the computing discipline relevant to the field of study. The planned module is for engineering professionals from the broad engineering discipline aiming to gain a Master's degree in Systems Engineering. Although the field of systems engineering cannot directly be associated with a computing discipline, the majority of systems developed today are highly-connected cyber-physical systems. Therefore, the disciplinary lens would be systems engineering.

5 Cybersecurity knowledge through the engineering lens

To determine the cybersecurity body of knowledge through the systems engineering lens, the CSEC knowledge units were presented to engineering professionals. Four in-depth and semi-structured elite interviews were scheduled, two with engineering professionals in academia (referred to as Academic 1 and Academic 2 in Tables 2 to 9) and two with engineering professionals in industry (referred to as Industry 1 and Industry 2 in Tables 2 to 9). All four participants are professionally registered engineers with ECSA, selected based on their knowledge of and experience in systems engineering.

The participants were provided with information regarding the researchers and their affiliations, the nature of the research, how long the interview will take, how the data will be used and where the results will be anonymously disseminated [23]. A detailed table of all knowledge units in the 8 knowledge areas, summarized in Table 1, were constructed to use as a guideline for the elite interviews. Each participant were asked open-ended questions, followed-up by closed-ended questions, where the combination of open- and closed-ended questions enabled the participants provide their views in their own words, but also provided the structured data required to populate Tables 2 to 9 [23]. The participants were guided through the table and prompted to comment on the relevance of each knowledge unit to systems engineering as well as the depth of which they felt it should be included in the module. The results of these discussions are captured in Tables 2 to 9 below where the feedback is coded as follows:

- Essential (E): Included in depth in the module. All essential topics were automatically marked "E" for essential.
- Overview (O): Included to provide a high level knowledge on the topic.
- Too Technical (TT): Not included due to the high technical nature of the topic.
- Additional Content (AC): Relevant and nice to have as additional content.
- Not Relevant (NR): Topic not directly relevant to systems engineering as task might sit with another professional.

In addition to documenting the relevance of each knowledge unit, the researcher made notes detailing contextual details and quotes for data analysis and interpretation.

Data Security. This knowledge area includes topics related to the protection of data at rest, during processing, and in transit. A systems engineer should have a good understanding of the system as a whole, not necessarily details relating to technical aspects. A good overview is required to understand where and how this fits into the system.

Table 2. Data Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
Cryptography	TT	TT	O	O
Digital Forensics	O	O	O	O
Data Integrity and Authentication	E	E	E	O
Access Control	O	E	E	O
Secure Communication Protocols	TT	TT	E	O
Cryptanalysis	TT	O	E	O
Data Privacy	O	O	E	O
Information Storage Security	TT	TT	E	O

Software Security. This knowledge area covers the development and use of software to preserve the security properties of the information and systems it protects. This knowledge area is relevant to engineers developing Industry 4.0-ready systems as all these systems contain software to a certain extent.

Table 3. Software Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
Fundamental Principles	O	O	E	O
Design	E	E	E	E
Implementation	TT	O	NR	O
Analysis and Testing	O	O	NR	E
Deployment and Maintenance	O	O	NR	O
Documentation	AC	O	NR	O
Ethics	E	E	E	O

Component Security. This knowledge area covers topics relating to the design, procurement, testing, analysis and maintenance of components to be integrated into larger systems. A systems engineer should have a good understanding of the system as a whole, not necessarily the technical details relating to the components aspects.

Table 4. Component Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
Component Design	O	TT	NR	O
Component Fabrication	TT	TT	NR	TT
Component Procurement	TT	TT	NR	TT
Component Testing	TT	TT	NR	O
Component Reverse Engineering	TT	TT	NR	TT

Connection Security. This knowledge areas covers the aspects relating to securing the connections between components, including physical and logical connections.

Table 5. Connection Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
Physical Media	TT	TT	TT	O
Physical Interfaces and Connectors	TT	TT	TT	O
Hardware Architecture	O	TT	TT	O
Distributed Systems Architecture	E	TT	TT	O
Network Architecture	O	TT	TT	O
Network Implementations	TT	TT	TT	O
Network Services	TT	TT	TT	O
Network Defense	TT	TT	TT	O

A systems engineer does not necessarily have to have all the technical knowledge relating to connections, but rather a holistic view of the system.

Systems Security. This knowledge area contains topics relating to the security aspects of systems that are composed of components and connections, and use software. This knowledge area covers security from a system view, which is typically where the systems engineer operates from.

Table 6. Systems Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
System Thinking	E	E	E	E
System Management	E	E	E	E
System Access	O	O	E	O
System Control	O	O	E	O
System Retirement	E	O	O	O
System Testing	E	E	O	E
Example System Architectures	TT	O	NR	O

Human Security. This knowledge area covers the protection of individuals' data and privacy in the context of organizations and personal life. As individuals will be responsible for the operation and use of the designed system, the human aspects cannot be ignored by a systems engineer.

Table 7. Human Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
Identity Management	O	O	E	O
Social Engineering	AC	O	NR	O
Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	AC	O	NR	O
Awareness and Understanding	AC	NR	E	O
Social and Behavioral Privacy	NR	NR	NR	O
Personal Data Privacy and Security	NR	NR	E	O
Usable Security and Privacy	NR	NR	E	O

Organizational Security. This knowledge area relates to the protection of organizations from cybersecurity threats and managing risk. As any systems engineer operates within an organization or develops systems to be used in an organization, aspects of the organizational security cannot be ignored.

Table 8. Organizational Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
Risk Management	E	E	E	E
Security Governance & Policy	E	E	E	O
Analytical Tools	O	TT	E	O
Systems Administration	NR	NR	E	O
Cybersecurity Planning	O	O	E	O
Business Continuity, Disaster Recovery, and Incident Management	O	NR	O	O
Security Program Management	E	O	O	O
Personnel Security	AC	O	E	O
Security Operations	AC	O	E	O

Societal Security. This knowledge area covers topics that has a broad impact on society as a whole. Any engineer must always be aware of the impact and ethics surrounding the developed systems.

Table 9. Societal Security knowledge units' relevance to systems engineering discipline

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	*E*	*E*	*E*	*E*
Cybercrime	O	O	O	O
Cyber Law	O	O	E	O
Cyber Ethics	E	E	O	O
Cyber Policy	AC	NR	E	O
Privacy	AC	NR	E	O

The first engineering professional from Industry (Industry 1), stated that one of the most important aspects of cybersecurity in systems engineering lies in the securing of data. Data includes personal data and information related to the working environment. Therefore, knowledge units in the Data Security, Systems Security and Organizational Security knowledge areas were marked as Essential. The second professional from Industry (Industry 2) stated that the System Thinking and Systems Requirements (within the Systems Security knowledge area) are essential for a systems engineer to know. The professional emphasized that a systems engineer should have a fair overview of all the cybersecurity knowledge areas in order to ask the correct questions, although the technical details are not required. A holistic view is more important than the technical detail. The first engineering professional from academia (Academic 1) stated that a holistic view is essential and underlined Systems Security and Organizational Security as the most important for inclusion in depth in the module. The professional agreed that, in order to obtain a solid holistic view of security, the essential topics for each knowledge

area must be included. The second academic (Academic 2) underlined the importance of the Systems Engineering, especially System Thinking. The academic also stated that the highly technical knowledge units are not required.

6 Basic outline of cybersecurity knowledge areas for postgraduate engineering studies

From the discussion in Section 5, a systems engineer needs to maintain a holistic view of the system. The technical details of data, component and communication security are not required in depth, but only a sufficient overview knowledge to understand the role each of these aspects play in the system. It can be argued that the systems engineer should be able to gain only an overview on Data Security, Component Security and Connection Security through the inclusion of only the essential topics. All interviewed professionals stated that a good overview of Human Security, Organizational Security and Societal Security are required in the module. Therefore, these three knowledge areas can be included in the module as overview knowledge units. The only exception is the knowledge unit of Cyber Ethics (within Societal Security), which all professionals feel must be covered in detail in the module as well as Risk Management and Security Governance & Policy (within Organizational Security).

In general, the knowledge areas of Software Security, Systems Security and Organizational Security were deemed the most important for in depth inclusion in the module. The majority of Industry 4.0-ready systems contain some form of software which the systems engineer must understand. System security was underlined as important in most interviews, except for the knowledge unit of Example System Architectures. The inclusion and exclusion of knowledge units are summarized in Table 10 below.

Table 10. Summary of knowledge units included and excluded in body of knowledge

Knowledge Area	Knowledge units included	
	In depth	Overview
Data Security	Essential topics only	-
Software Security	Essentials; Fundamental Principles; Design; Ethics	Implementation; Analysis & Testing; Deployment & Maintenance; Documentation;
Component Security	Essential topics only	-
Connection Security	Essential topics only	-
System Security	System Thinking; System Management; System Testing	System Access; System Control; System Retirement
Human Security	Essential topics	All knowledge units
Organizational Security	Essentials; Risk Management; Security Governance & Policy	Remaining knowledge units
Societal Security	Essentials; Cyber Ethics	Remaining knowledge units

Table 10 provides the body of knowledge for a postgraduate cybersecurity module in Systems Engineering. The module includes the essential topics as prescribed in CSEC2017 as well as topics described by engineering professionals as essential.

7 Conclusion

The creation of systems to comply with Industry 4.0 environments requires highly connected systems which must be able to withstand various types of cyberattacks. There is a drive from the engineering industry to include cybersecurity into the engineering of systems to improve its inherent security. However, many systems engineers are not educated in the field of cybersecurity. Engineering students may receive a high level overview of cybersecurity concepts in some engineering modules, but courses seldom include specialization cybersecurity topics. This lack of cybersecurity content in SA engineering education creates a gap in cybersecurity knowledge amongst engineers.

This paper included an investigation to determine the body of knowledge for the creation of a postgraduate cybersecurity module in systems engineers. The CSEC2017 framework were utilized as a baseline for the module outline, and presented to engineering professionals to determine relevant body of knowledge for systems engineering. The knowledge areas were discussed with engineering professionals from academia and industry through interviews to determine which areas are considered essential for inclusion in the module. The basic body of knowledge for a postgraduate cybersecurity module is presented, which states that the knowledge areas of Software Security, Systems Security and Organizational Security were deemed the most important for in depth inclusion in the module along with the essential topics stipulated in the CSEC2017 document. The main limitation of this work is that this basic body of knowledge was guided by the input from only four professional participants, two from academia and two from industry. However, this is deemed sufficient for a preliminary investigation providing a baseline from which to work. Future work will include the collection of input from a broader spectrum of top-level professionals to inform the new postgraduate module in Systems Engineering.

References

1. Kiel, A.: What do we know about "Industry 4.0" so far? Proceedings of the International Association for Management of Technology (IAMOT 2017) (2017).
2. Morgan, S.: IBM's CEO On Hackers: "Cyber Crime Is The Greatest Threat To Every Company In The World", https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#1baf053373f0, last accessed 2017/01/09 (2005).
3. Tamura, E.: Hewlett Packard Enterprise Leads Transformation of Cyber Defense with "Build it In" and "Stop it Now", http://www8.hp.com/us/en/hp-news/press-release.html?id=2184147#.WtlU5S6uyUl, last accessed 2017/01/09 (2006).
4. 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).

5. Morgan, S.: Cybersecurity job market to suffer severe workforce shortage. CSO, https://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html, last accessed 2018/04/30 (2005).
6. Suby, M. and Dickson, F.: The 2015 $(ISC)^2$ Global Information Security Workforce Study. Frost and Sullivan White Paper (2015).
7. Cisco Advisory Services. Mitigating the cybersecurity skills shortage (2015).
8. Fripp, C.: South Africa simply doesn't have enough cybersecurity experts. https://www.htxt.co.za/2016/08/19/south-africa-simply-doesnt-have-enough-cybersecurity-experts/ last accessed 2018/03/09 (2017).
9. McGettrick, A.: Toward curricular guidelines for cybersecurity, Report of a Workshop on Cybersecurity Education and Training. doi:10.1145/2538862.2538990 (2013).
10. Von Solms, S. and Futcher, L.: Towards the Design of a Cybersecurity Module for Post-graduate Engineering Studies. In: Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017), Adelaide, Australia (2017).
11. Newhouse, W., Keith, S., Scribner, B. and Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Special Publication 800-181, NIST2017 (2017).
12. Dove, R., Bayuk, J., Wilson, B. and Kepchar, K.: INCOSE System Security Engineering Working Group Charter, https://www.incose.org/docs/default-source/wgcharters/systems-security-engineering.pdf?sfvrsn=cc0eb2c6_8, last accessed 2018/03/09 (2016).
13. 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).
14. Haridas, N. Software Engineering – Security as a Process in the SDLC. SANS Institute InfoSec Reading Room (2007).
15. Tong, A., Sainsbury, P. and Craig, J.: Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. International Journal for Quality in Health Care, Volume 19, Issue 6, pp 349–357. (2007)
16. Liamputtong. P. and Ezzy, D.: Qualitative Research Methods, 2nd edn. Melbourne, Victoria Oxford University Press (2005).
17. Davies, P. H. J.: Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services. Politics, Volume 21, Issue 1, pp 73-80 (2001).
18. Aberbach, J. D. and Rockman, B. A.: In the Web of Politics: Three Decades of the U.S. Federal Executive. Washington, D.C.: The Brookings Press (2000).
19. Tansey, O.: Process Tracing and Elite Interviewing: A Case for Non-Probability Sampling, PS: Political Science and Politics, Volume 40, No. 4, pp. 765-772 (2007).
20. Thomas, D.R.: A general inductive approach for analyzing qualitative evaluation data. American journal of evaluation Volueme 27, Issue 2, pp 237-246 (2006).
21. ECSA, Qualification Standard for Bachelor of Science in Engineering (BSc (Eng))/ Bachelors of Engineering (BEng): NQF Level 8 4, 1–10 (2014).
22. The Higher Education Qualifications Sub-Framework. Government Gazette No. 36003 of 14 December 2012. (2013)
23. Harvey, W. S.: Strategies for conducting elite interviews, Qualitative Research, Volume 11, Issue 4, pp 431–441 (2011).