Towards Educational Guidelines for the Security Systems Engineer

Suné von Solms, Annlizé Marnewick

Towards educational guidelines for the security systems engineer

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

Abstract. Industry 4.0 will impact the systems engineering landscape and cybersecurity in the future. The education needs of system engineers working in these environments will change as the system landscape adapt to the Industry 4.0 changes. This research aims to explore the impact of Industry 4.0 on systems engineering and security requirements which must be catered for in future in this changing Industry 4.0 landscape. Although it is not certain yet how the landscape will change, this research starts to explore what the potential education needs could be for system engineers to understand all future cybersecurity requirements. The results of this research indicate that security requirements engineering will be needed in the first requirements stage of the systems development life cycle. Secondly, a new set of expert engineering skills will be required to identify future threats and vulnerabilities which could impact the system landscape. These results can be used as a guideline to start thinking how system engineers should be educated for the future.

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

1 Introduction

The rise of Industry 4.0, also referred to as the Industrial Internet of Things (IIoT) or the fourth industrial revolution, defines the use of new digitized and connected industrial systems, assumed to yield extensive industry-spanning opportunities [1]. These new systems are expected to be smart cyber-physical systems which communicate and work with other systems and humans in real time [2]. The interconnected nature of Industry 4.0–driven operations and systems means that the impact and effects of cyberattacks on these systems will be more extensive on the engineering systems than before [3].

The fear of industry and academia is that the designers, manufacturers and their supply networks may not be prepared for the risks that these Industry 4.0–driven systems presents. This posts one of the biggest challenges for engineering design and also for engineering education [3, 4]. To address these uncertainties, the engineering space has recently seen a large drive to include extensive cybersecurity processes into systems

engineering process requirements engineering. This is due to the traditional systems engineering processes being inadequate for the development of secure systems, as cybersecurity had less impact on business operations as the environment were isolated versus the new connected environment [5, 6]. In the past, security integration in engineering systems was limited to the IT industry, where security were added after the completed system was developed. However, with the new drive for integration, security must be included in software development, risk management, human factors and all other areas within an organization [7, 8]. The International Council of Systems Engineering (INCOSE) has chartered a working group in 2016 to start the processes required for fostering security within systems engineering, where system security is "accepted and practiced as a fundamental part of system engineering" [5] and where security is incorporated across the entire systems development lifecycle [9, 10].

There exist limited studies in the field of systems engineering that aim to investigate how the cybersecurity knowledge and skills of the systems engineer in the industrial workforce are changing. This research aims to investigate the additional cybersecurity-related activities the systems engineer will be responsible for in order to design Industry 4.0-ready systems. As the range of cybersecurity activities are so wide-ranging throughout the design of engineering systems, this paper will only consider the activities in the Requirements and Conceptualization phase of an engineering project.

2 Overview of the current systems engineering landscape

The increased connectivity of smart systems essential for Industry 4.0 requires the design of smart, autonomous technologies. These connected, smart systems, aiming to fully integrate the digital and physical world, introduce a new set of cyber risks. The interconnected nature of these systems requires organizations to employ professionals with the skills and competencies to design Industry 4.0–ready systems. For cyber risks to be adequately addressed, cybersecurity strategies should be fully integrated into organizational and design strategies from the start [3].

When designing traditional systems, the systems engineer would typically leave the cybersecurity aspects of a system to the security professionals [5]. In many cases the security features of a system were treated as of secondary importance. One of the main work roles of the systems engineer is to derive a complete set of functional requirements (criteria defining specific behavior and functions) and non-functional requirements (criteria indicating the operation and constraints) of the system. Security is generally considered a non-functional requirement and are typically considered less important than functional requirements [5, 6]. It is stated by Dove et al. [5] that "as long as systems engineers do not consider security a functional requirement, it will not be likely to rise to the top of the implementation checklist". To address this issue, INCOSE admits that new approaches to systems engineering will need to be implemented in order to meet the need for secure systems in the era of Industry 4.0 [5].

The National Institute of Standards and Technology (NIST) produced the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework in August 2017 which highlights the need for interdisciplinary nature of cybersecurity work and provides guidance on workforce development, training and education of cybersecurity professionals [11]. This includes information regarding cybersecurity-related activities and tasks of an organization and the relevant work role responsible for each activity or task. It also details the knowledge, abilities and skills required by a professional in order to successfully execute the applicable tasks and activities [6, 11-15]. As the updating of the systems engineering framework by INCOSE to include cybersecurity is still a work in progress, the NICE Cybersecurity Workforce Framework publication is currently used to evaluate the inclusion of cybersecurity considerations in the system development life cycle (SDLC) of systems engineering.

Due to the limited exposure of systems engineers to cybersecurity, many systems engineers lack the knowledge, abilities and skills required to address potential Industry 4.0-related security issues. This lack in cybersecurity knowledge regarding security risk analysis, as well as the lack in vision to consider systems and their threats/risks in their entirety leads to gaps in the security architecture of systems [6, 16].

3 Methodology

This work analyses the activities in the traditional systems development life cycle (SDLC) as well as the updated secure systems development life cycle (S-SDLC) to determine the additional cybersecurity activities required by the process and where the responsibilities lie. As the range of cybersecurity activities are so wide-ranging, this paper will only consider the activities in the Requirements and Conceptualization phase of an engineering project. The research presented in this paper aims to determine the new activities that a systems engineer will be exposed to when developing systems for the Industry 4.0 environment. This work comments on the potential activities and responsibilities shortfall amongst traditional systems engineers in the era of Industry 4.0. The methodology followed consists of the following steps:

1. To conduct a content analysis on the traditional SDLC processes captured by the ISO/ICE/IEEE 15288:2015 [17] standard to identify the range of security activities included in the SDLC and where the responsibility lies.
2. To conduct a content analysis on the NIST NICE Cybersecurity Workforce Framework [11] to determine the proposed cybersecurity related activities required in the S-SDLC and where the responsibility lies.
3. Comment on the activities, knowledge, abilities and skills differences between the two processes and determine the how the role of the systems engineer in the industrial workforce might change.

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

4 Analysis of security activities in the SDLC

4.1 Responsibilities of the systems engineer in the SDLC

When a new system is developed, a coordination of numerous activities and processes from a collection of professionals are required. The systems engineer's responsibility starts with the need of a new system or problem that must be solved, and ends when the system is operational and used by end-users or customers. The responsibility of the systems engineer would be based on individual experience, systems engineering knowledge and current system complexity. One of the main work roles of the systems engineer is to derive a complete set of functional and non-functional requirements of the system. This requirements engineering process uses the results of risk analysis and threat assessments as goals that must be met by the system to initialize the elicitation activity [15]. This risk analysis and threat assessment is traditionally the responsibility of a systems engineer. In the traditional SDLC, the goal of the risk management processes, according to Parnell et al. [18], is to identify, assess and take action to reduce risks of system technical performance, cost and schedule estimates. However, the analysis and assessment of extreme risks, including cybersecurity, is not traditionally seen as the systems engineer's responsibility but rather an expert risk analyst [19].

Sage and Rouse [19] states the following responsibilities of a systems engineer relating to requirements engineering:

1. Need identification and customer linkage: the need is identified through the matching of the need with the technical feasibility and provide the linkage between the customer's needs and the design of the system.
2. Requirements management: the customer needs is developed as in input to determine the systems and functional requirements.
3. Architecture and systems design: design the system's concept and link the requirements with the configuration.
4. Technical risk and management: perform a technical risk assessment and manage these risks during trade-off analysis.

It can be seen that no direct mention is made of any security related responsibilities. Traditionally, when designing systems, the systems engineer would leave the cybersecurity aspects of a system to the security professionals [5].

4.2 Overview of the SDLC

In industry, systems engineers utilize best practice systems engineering processes and methods to execute the activities during system development. System development progresses through the life cycle stages, and make use of decision gates to determine the way forward [20]. This discovery process is generally structured into stages throughout the system life cycle where it is conceptualize, developed, produced, utilized, supported and retired [18]. Fig. 1 illustrates a generic systems engineering life cycle as described by ISO/IEC/IEEE 15288:2015.

Fig. 1. Generic Systems engineering generic life cycle [16, 18]

The process model followed by a systems team depends on prior experience of the resources and standard approaches used by the organization or problem type to be solved, therefore there does not exist one SDLC for all engineering systems [19]. Comparisons of the available life cycle models used by various organizations or disciplines are available in literature [18, 20]. A typical SDLC used in a commercial systems integrator environment is illustrated in Fig. 2.

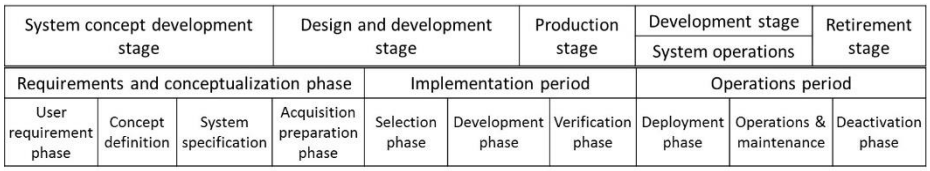

Fig. 2. Typical SDLC for commercial systems integrator environments

During the SDLC stages shown in Fig. 2, the processes prescribed by standards and systems engineering communities are invoked [20]. The processes currently included in the body of knowledge do not directly include a process relating to security. In order to determine where the security-related activities are included in the systems engineering process, a content analysis is performed on the ISO/ICE/IEEE 15288:2015 framework, described in the subsequent section.

4.3 Content analysis of security in Systems Engineering Processes

A content analysis was performed on the ISO/IEC/IEEE 15288 2015 - Systems and software engineering - Systems life cycle processes document. The search term "security" was used in order to determine where security-related actions are included in the SDLC and who the responsible professionals are. Security activities show to impact three processes shown in Table 1.

Table 1. Results of content analysis of ISO/IEC/IEEE 15288 2015.

Search Phrase	Results	Process	Comment on content
security	3	Agreement process	Security is noted as an increasing concern. ISO/IEC 27036 is referred to for guidance how to secure information in supplier relationships.
		Infrastructure management process	ISO/IEC 27036 is referred to for guidance how to secure outsourced infrastructure.
		Project planning process	ISO/ICE 15026 and ISO/IEC 27036 is referred to for guidance related to ISO/IEC 27036 objectives and constraints related to assurance and security

It can be seen from the table that all the references to security in the document are references to other standards documents. It is noted in the ISO/ICE/IEE 15288 standard that "information security for supplier relationships" must be carefully considered [17]. It can be deduced from this analysis that the traditional SDLC does not include dedicated security activities. The systems engineering community acknowledged this lack and has responded with integration of security engineering into the systems engineering processes [14, 22, 23].

5 Analysis of security activities in the S-SDLC

5.1 Overview of the S-SDLC

The systems engineering community is in the process to identify security roles and responsibilities applicable to the entire systems development life cycle for future connected environments [22]. Various researchers have developed S-SDLC suggestions to show how and where security can be included in the S-SDLC. In these suggestions, security is included throughout the systems development life cycle stages. The first step in the proposed S-SDLC is the introduction of a new security requirements engineering process which is a sub process of the traditional requirements engineering activity [15]. The S-SDLC, illustrated in Fig. 3, indicates the updated Requirements and Conceptualization phase to illustrate the addition of the security requirements engineering process.

<table>
<tr><th colspan="4">Requirements and conceptualization phase</th><th colspan="3">Implementation period</th><th colspan="3">Operations period</th></tr>
<tr><td>User requirement phase</td><td>Concept definition</td><td rowspan="3">System specification</td><td rowspan="3">Acquisition preparation phase</td><td rowspan="3">Selection phase</td><td rowspan="3">Development phase</td><td rowspan="3">Verification phase</td><td rowspan="3">Deployment phase</td><td rowspan="3">Operations & maintenance</td><td rowspan="3">Deactivation phase</td></tr>
<tr><td>Risk Analysis</td><td>Risk assessment</td></tr>
<tr><td colspan="2">Security requirements engineering</td></tr>
</table>

Fig. 3. S-SDLC indicating the addition of risk analysis and assessment relating to security requirements engineering

This security requirements engineering process's purpose is to elicit the security requirements the system should cater for in order to reduce risk [24]. The new security requirements engineering process is depended on a security risk analysis and assessment activity to derive a complete set of requirements [6, 15].

The goal of the security risk analysis is to identify potential sources of threats or vulnerabilities the new system could have. The risks identified must then be assessed to determine the potential impact on the organizations operations, assets, individuals and other implications [25]. The result of the risk assessment is then used as an input to the security requirements engineering process. The results are analyzed to identify suitable security requirements that can mitigate the potential threats and vulnerabilities within the organization's risk management strategy [15].

5.2 Responsibilities of the systems engineer

The literature states that the security requirements engineering process will in future potentially be integrated with the requirements activity as the systems engineer is generally the person with the holistic view of the system. This will require the systems engineer to develop the knowledge, competencies and skills in order to do complete security requirements.

The risk assessment and threat analysis activities, required as an input to the new security requirements engineering process, are additional activities not previously included within the system engineering responsibility. Traditionally, the risk analysis performed by the systems engineer did not include activities relating to security and only considered technical risk assessment, as discussed in Section 4.1. For the system engineer to perform the new security risk analysis and threat assessment, he/she will require new knowledge, competencies and skills.

If the systems engineer is not the professional who will take responsibility for these tasks, these tasks must become the responsibility of another cybersecurity professional. In order to determine the responsible professional(s) for these security-related activities, a content analysis was performed on the NIST NICE Cybersecurity Workforce Framework [10], described in the subsequent section.

5.3 Content analysis of security in S-SDLC

The NIST NICE Cybersecurity Workforce Framework describes an organization's cybersecurity needs by defining *Specialty Areas*, *Work Roles* and *Tasks*. Each specialty area represents an area of concentrated work, where each work role indicates the responsible person, and each task an activity. A range of steps were followed to determine who would be the professionals responsible for security-related risk assessment and requirement tasks according to the NIST NICE Cybersecurity Workforce Framework.

Step One. Who is responsible for the security requirements engineering tasks of the NIST cybersecurity framework? A content analysis was done of the phrase "security requirements" within the NICE Framework. The results relating to work roles are shown in Table 2 below.

Table 2. Results of content analysis on "security requirements" in NICE Cybersecurity Workforce Framework.

Search Phrase	# results	Work Role	Work Role Description
security requirements	1	Security Architect	Protects the organization's mission and that the business processes are adequately addressed in all aspects of enterprise architecture.

Only one work role included the phrase “security requirements”. Per definition, the Security Architect is not a work role which is included in the SDLC requirements and conceptualization phase. As a specific work role is not allocated for security requirements relating to the systems engineering and the SDLC, a second content analysis was done of the phrase “functional requirements” within the NICE Framework. The results are shown in Table 3 below.

Table 3. Results of content analysis on “functional requirements” in NICE Cybersecurity Workforce Framework.

Search Phrase	# results	Work Role	Work Role Description
functional requirements	1	Systems Requirements Planner	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

The framework only has one work role, namely Systems Requirements Planner, allocated to the tasks relating to functional requirements. As security requirements not listed as a separate function for the Systems Requirements Planner, it can be assumed that security requirements engineering activity remains the responsibility of the Systems Requirements Planner, which per definition relates to the systems engineer. Input to guide the security requirements engineering activity is the risk identification and assessment of all potential threats and vulnerabilities.

Step Two. Who is responsible for the risk analysis and threat assessment tasks of the NIST cybersecurity framework?

Content analysis was performed to identify who is responsible for risk analysis and threat assessment of the NIST cybersecurity framework. A search was done on the phrases “risk assessment”, “assessment”, “threat” and “vulnerabilities” within the NICE Framework. The results relating to work roles in the SDLC are shown in Table 4 below. From this result of this analysis, it can be seen that the work roles assigned for risk assessment includes the Security Control Assessor and Vulnerability Assessment Analyst. The Research and Development Specialist and the Exploitation Analyst are assigned to assess threats.

These roles are not roles traditionally defined in systems engineering processes, which would indicate that these are new roles required for the Industry 4.0 environment. Therefore, the S-SDLC will require a new type of engineer functioning as a Vulnerability Assessment Analyst and Exploitation Analyst who must perform the risk assessments and threat analysis activities. In the current environment a systems engineer developing the solution will not be able to take on these activities in addition to his/her existing work.

Table 4. Results of content analysis on "risk assessment", "assessment", "threat" and "vulnerabilities" in NICE Cybersecurity Workforce Framework.

Search Phrase	Results	Work Role	Work Role Description
risk assessment	0	-	-
assessment	2	Risk Management - Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls.
		Vulnerability Assessment and Management - Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
threat or vulnerabilities	3	Vulnerability Assessment Analyst	Duplication – see above
		Technology R&D (TRD) - Research and Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
		Exploitation Analyst	Analyzes collected information to identify vulnerabilities and potential for exploitation.

6 Discussion & Recommendations

System engineers cater for both physical and information security as part of the design [17], with the principle that the design of the system must prevent intentional introduction of faults with consequences of various impacts [26]. From this it is acknowledged that security is traditionally only considered and designed for the environment the system will operate in. As future environments will be much more connected, it has been highlighted that cybersecurity should be considered during the entire systems development lifecycle and not just bottom up during design and validation [27]. The analysis performed in Section 4 shows that there exist a clear need for the inclusion of cybersecurity-related activities in the SDLC. Cybersecurity skills related to security risk analysis, threat assessment and security requirements engineering, must be included in the systems engineering process.

Form the analysis done in Section 5, it can be seen that the cybersecurity-related activities added to the S-SLDC does not clearly indicate who the responsible person will be in a systems engineering context. It can then be argued that the additional cybersecurity-related activities may befall the systems engineer by default if no cybersecurity specialist is assigned to the process. The security risk analysis requires a holistic technical view, but also needs security risk scenario analysis and threat analysis skills, which most systems engineers do not currently possess.

The results of this study can pose the case for a new type of engineer to become an expert in the function of security risk analysis and threat assessment. The reason for this is that an engineer typically has a sound systems thinking ability to understand the holistic environment in order to identify all influences on the environment. An engineer capable of sound systems thinking skills as well as cybersecurity-related knowledge, skills and competencies relating to cybersecurity would form an important part of a systems engineering process in the future of Industry 4.0-ready systems. The requirement for this new type of systems engineer calls for the development of engineering education to include cybersecurity-related knowledge, skills and competencies into systems engineering curricula. Systems engineers need to be educated in the fields of security risk analysis and threat assessment, as well as security requirements engineering.

Currently, there only exist a hand full of known postgraduate cybersecurity engineering degrees worldwide, with even less of these focusing on cybersecurity within systems engineering. Two known Master's degrees include the Master of Science in Systems Engineering at Johns Hopkins Whiting School of Engineering [28] and the MS in Systems Engineering with Certificate in Cybersecurity University of Maryland, Baltimore County [29]. Currently no known postgraduate cybersecurity engineering degrees are offered by South African institutions [30]. The inclusion of cybersecurity in dedicated systems engineering modules and courses are even scarcer, leading to the existence of a mismatch between cybersecurity education in systems engineering and cybersecurity requirements from industry. Therefore, inclusion of cybersecurity in currently systems engineering courses or the creation of a cybersecurity systems engineering degree or postgraduate module is recommended.

7 Conclusion

This paper argues that in the light of Industry 4.0, there exist a need for the creation of systems with a greater level of connectivity, where cyberattacks on these systems may be more extensive than before [3]. It is therefore required by designers, manufacturers and supply networks to be prepared for the risks that these new Industry 4.0–driven systems presents.

This paper shows through content analyses that the current systems engineering processes do not consider all security activities needed in the light of the fourth industrial

revolution. This paper also shows that when considering the new cybersecurity activities proposed to be included in the Requirements and Conceptualization phase of an engineering project, new cybersecurity-related knowledge and skills will be required. It is argued that these activities will require the addition of a systems engineer who possesses the knowledge, skills and competencies related to security risk analysis and threat assessment. As these knowledge and skills are not currently taught to systems engineers, it is argued that there exist a need in engineering education for the creation of such course or modules.

Future research would include an investigation on the identified cybersecurity-related activities and determine the relevant knowledge areas, abilities and skills required to successfully implement these activities. Future work must also consider other phases in the SDLC and determine the cybersecurity-related activities and where the responsibility lies. This work serves as a driver towards the creation of cybersecurity-related content into engineering education.

References

1. Kiel, A.: What do we know about "Industry 4.0" so far? Proceedings of the International As-sociation for Management of Technology (IAMOT 2017) (2017).
2. Hermann, M., Pentek, T. and Otto, B.: Design Principles for Industrie 4.0 Scenarios, in 49th Hawaii International Conference on System Sciences (HICSS), pp. 3928-3937 (2016).
3. Waslo, R., Lewis, T., Hajj, R. and Carton, R.: Industry 4.0 and cybersecurity Managing risk in an age of connected production, Deloitte University Press2017, https://www2.deloitte.com/insights/us/en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html, last accessed 2018/04/18.
4. Motyl, B., Baronio, G., Uberti, S., Speranza, D. and Filippi, S.: How will Change the Future Engineers' Skills in the Industry 4.0 Framework? A Questionnaire Survey, Procedia Manufacturing, vol. 11, pp. 1501-1509 (2017).
5. 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 (2016) last accessed 2018/04/21.
6. Kim, Y.: Activities of Security Engineering in System Development Life Cycle: Security Engineer's View, presented at the 14th International Conference on Applications of Computer Engineering (ACE '15), Seoul, South Korea, September 5-7 (2015).
7. 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).
8. Haridas, N. Software Engineering – Security as a Process in the SDLC. SANS Institute InfoSec Reading Room (2007).
9. 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 (2015) last accessed 2018/05/21.
10. 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 (2016) last accessed 2018/05/21.

11. Newhouse, W., Keith, S., Scribner, B. and Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, in Special Publication 800-181, NIST2017 (2017).
12. Kissel, R. L., Stine, K. M., Scholl, M. A., Rossman, H., Fahlsing, J. and Gulick, J.: Security Considerations in the System Development Life Cycle, in NIST Special Publication 800-64, NIST2008 (2018)
13. Dawson, M., Burrell, D., Rahim, E. and Brewster, S.: Integrating Software Assurance into the Software Development Life Cycle (SDLC), Journal of Information Systems Technology & Planning, vol. 3, no. 6, pp. 49-53 (2010).
14. Mailloux, L. O., Garrison, C., Dove, R. and Biondo, R. C.: Guidance for Working Group Maintenance of the Systems Engineering Body of Knowledge (SEBoK) with Systems Security Engineering Example, INCOSE International Symposium, vol. 25, no. 1, pp. 1004-1019 (2015).
15. Salini P. and Kanmani, S.: Survey and analysis on Security Requirements Engineering, Computers & Electrical Engineering, vol. 38, no. 6, pp. 1785-1797 (2012).
16. Evans, S., Heinbuch, D, Kyle, E., Piorkowski, J. and Wallner, J.: Risk-based systems security engineering: stopping attacks with intention, IEEE Security & Privacy, vol. 2, no. 6, pp. 59-62 (2004).
17. ISO, ISO/IEC/IEEE International Standard - Systems and software engineering -- System life cycle processes, ISO/IEC/IEEE 15288 First edition 2015-05-15, pp. 1-118 (2015).
18. Parnell, G. S., Driscoll, P. J. and Henderson, D.: Decision Making in Systems Engineering and Management (Systems Engineering and Management). New Jersey: Wiley, pp. 497 (2011).
19. Sage, A. P. and Rouse, W.: Handbook of systems engineering and management (Wiley series in Systems Engineering and Management). Wiley (2009).
20. Walden, D. D., Roedler, G. J., Forsberg, K. J., Hamelin, R. D. and Shortell, T. M.: INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Wiley (2015).
21. Sommerville, I.: Software Engineering, Six Edition ed. Harlow: Addison-Wesley (2001).
22. Nejib, P., Beyer, D. and Yakabovicz, E.: Systems Security Engineering: What Every System Engineer Needs to Know, INCOSE International Symposium, vol. 27, no. 1, pp. 434-445 (2017).
23. Zemrowski, K. M.: NIST Bases Flagship Security Engineering Publication on ISO/IEC/IEEE 15288:2015, Computer, vol. 49, no. 12, pp. 86-88 (2016).
24. Türpe, S.: The Trouble with Security Requirements, in IEEE 25th International Requirements Engineering Conference (RE), 2017, pp. 122-133 (2017).
25. National Institute of Standards and Technology (NIST), Guide for Conducting Risk Assessments, NIST 800-30 (2012).
26. Blanchard B. S. and Blyler, J. E.: System Engineering Management. Wiley (2016).
27. Bayuk J. L. and Horowitz, B. M.: An architectural systems engineering methodology for addressing cyber security, Systems Engineering, vol. 14, no. 3, pp. 294-304 (2011).
28. Johns Hopkins Whiting School of Engineering, Systems Engineering, https://ep.jhu.edu/programs-and-courses/programs/systems-engineering, last accessed 2018/17/26.
29. University of Maryland, Baltimore County, Systems Engineering, http://se.umbc.edu/mssecyber.php, last accessed 2018/17/26.
30. von Solms, S and Futcher, L.: Towards the Design of a Cybersecurity Module for Postgraduate Engineering Studies, in Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017) Adelaide, Australia (2017).