I J C T A, 9(11) 2016, pp. 5511-5520

A SYSTEMATIC SURVEY ON SAFETY AND SECURITY ASPECTS OF SAFETY CRITICAL SYSTEM

Raj Kamal Kaur Grewal[*] , and Babita Pandey[**]

Abstract: The migration towards digital control systems makes new safety and security threats that could result in loss of life, damages to property and environment regarded as safety critical system. To address this safety and security issues in the safety critical system, this paper provides the survey on safety and security aspects; similarities and disparities between them and relevant risk assessment techniques. In addition to this, summarize the key challenges (open issues) in safety critical system.

Key Words: Safety critical system, Security, Safety.

1. INTRODUCTION

Traditional control systems were based on mechanical and electromechanical devices. But currently, it has become difficult and expensive to deploy, maintain and operate them according to the functional requirements of industrial needs. To handle this problem, information technologies and communication devices are being incorporated into modern control systems such as [1]: Process control system, Cyber-physical system, Supervisory control and data acquisition systems (SCADA) and Commercial off-the-shelf. These control systems provide new facilities such as [2]: permit us to work quicker, remotely monitor and control the system’s function, provides safety and timely service but in turn, it increases the degree of complexity, makes the system vulnerable for opening the door to external attacks. The failure of such systems can be catastrophic; causing harm to both life and the environment. Now a day’s Safety Critical Systems (SCSs) are widely utilized in many areas such as transportation, aerospace, medical, information system and nuclear industries.

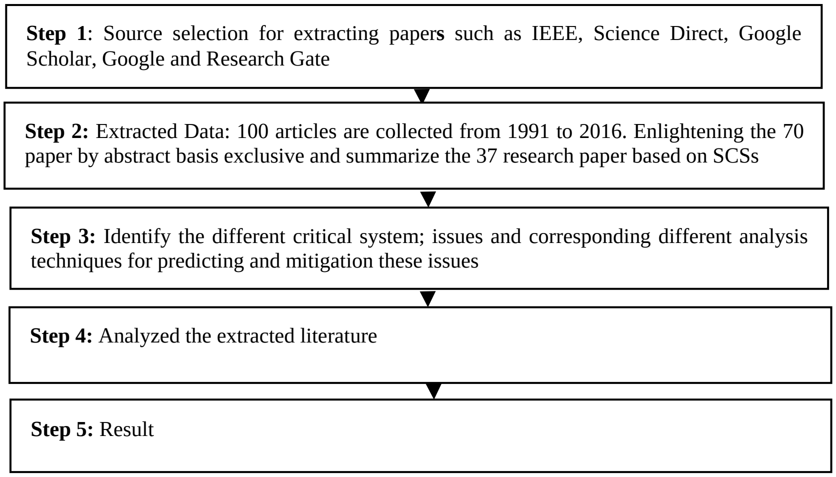
The main intent of this paper is to concentrating on safety and security aspects; similarities/difference between these aspects; several key challenges of SCSs which are identified throughout analysis of existing literature on safety critical systems. In addition to this, summarize methodologies and generic phases to evaluating these (safety and security) issues in SCSs. Figure 1, shows reviewed flow, it was initiated to extract the published paper of SCSs between 1991 to 2016 in International journals, IEEE transaction, Elsevier and Springer using the keywords such as “safety critical system”, “safety”, “security”, “safety and security analysis techniques” and “challenges of safety critical system”. Extract the relevant 37 articles out of 100 articles of SCSs. From this literature review, identified various SCSs such as medical, transportation, power and

[*] School of Computer Application Lovely Professional University Phagwara, Punjab
Email: grewal.rajkamal03@gmail.com

[**] School of Computer Application Lovely Professional University Phagwara Punjab Email: shukla_babita@yahoo.co.in

information systems and their corresponding issues such as safety and security. Further, the extracted literature has analyzed in tabular form and report the result.

This paper is structured as follows. Section 2 defined the different SCSs, Section 3 clarifying the meaning of terms safety and security used in the context of this survey, Section 4, summarize similarities and difference between these aspects. In Section 5, present phases and approaches for assessing of safety, security, and combined safety-security aspects. In Section 6, present result and discussion; section 7 present the challenges of SCSs and concluding remarks is defined in Section 8.



Step 1: Source selection for extracting papers such as IEEE, Science Direct, Google Scholar, Google and Research Gate

Step 2: Extracted Data: 100 articles are collected from 1991 to 2016. Enlightening the 70 paper by abstract basis exclusive and summarize the 37 research paper based on SCSs

Step 3: Identify the different critical system; issues and corresponding different analysis techniques for predicting and mitigation these issues

Step 4: Analyzed the extracted literature

Step 5: Result

Figure 1 Systematic review process

2. SAFETY CRITICAL SYSTEM

Before considering the safety and security aspects of systems, there is a need to get aware of critical systems and their facilities. SCSs are extensively used in various domains such as power, medical, transportation and information system.

Power system is a system of electrical components that supply, transfer and uses the electric power. These power control system consequently supply reliable electric power within a predetermined time period to critical devices or apparatus, provide remotely monitoring, collect a larger amount of information, facilitate network management and energy optimization, whose failure would jeopardize the physical condition and individual safety or result in harm to property [1].

C**yber-physical medical device** is wireless sensor system that gathers the diagnostic information, monitor the physical condition and medication administration of patients. The medical device industry is experiencing a fast transformation, embracing the capability of embedded software and system network. The software is a critical part of the medical device, provide high-quality continuous care for patients, remotely monitoring of implanted devices may help to find out malfunctions which direct to longer survival of patients. The failure of medical device’s software contributes to the damage or demise of patients [3].

Transportation control system can be extensively classified as "reactive/responsive systems" which interact with their surroundings through sensors and actuators. This software based system facilitates transportation organizers with simply monitoring, dispatching transportation resources, analyze the accident with the location which is instantly sent to the server so that the nearest hospital could be find and an emergency vehicle is sent to the catastrophe zone. The failures in complex systems result in serious loss of material and human life [4]. The aviation control system is transitioning to use of the global positioning system for route and precision approaches [5].

Information system provides the useful information that can be helpful for decision making. Currently, with the popularization of the computer and Internet technologies, electronic documents have become an essential resource in organizations. The failure of several information systems has become the reason for the loss of monetary and human life [5].

3. SAFETY AND SECURITY TERMINOLOGY

Before dealing with safety and security issues of any SCSs, it is necessary that one should be aware about these terminologies; its similarities and differences.

Safety is freedom from catastrophe or losses. It concerned with preventing accidents by identifying latent weaknesses, initial events, interior risk, and possibly unsafe states and then applying suitable alleviations to decrease the risks to a tolerable level. It is categorized into two classes [6]: primary safety-critical software (refers to the failure of implanted software systems which causes the failure of hardware and directly threaten persons) and secondary safety-critical software (refers to systems whose failure results in hazard in other systems which can cause directly human injury or environmental damage) as shown in Fig. 2. Many researchers have proposed various techniques that used for safety risk analysis in SCSs are: [7, 8, 9, 10, 11, 12, 13, 14, 15].

Security is protection against external attacks and interference. It avoids unauthorized disclosure and alteration data. Many researchers have proposed various techniques that are used for security risk analysis in SCSs such as: [1, 16, 17, 18, 19, 20, 21]. With the increase of incorporate information technologies into manufacturing control systems, such communities have become progressively attentive of the potential dependencies between safety and security aspects and the need to handle both aspects jointly. Studies [22, 23, 24, 25] focuses on both safety-security risk assessment in SCSs.

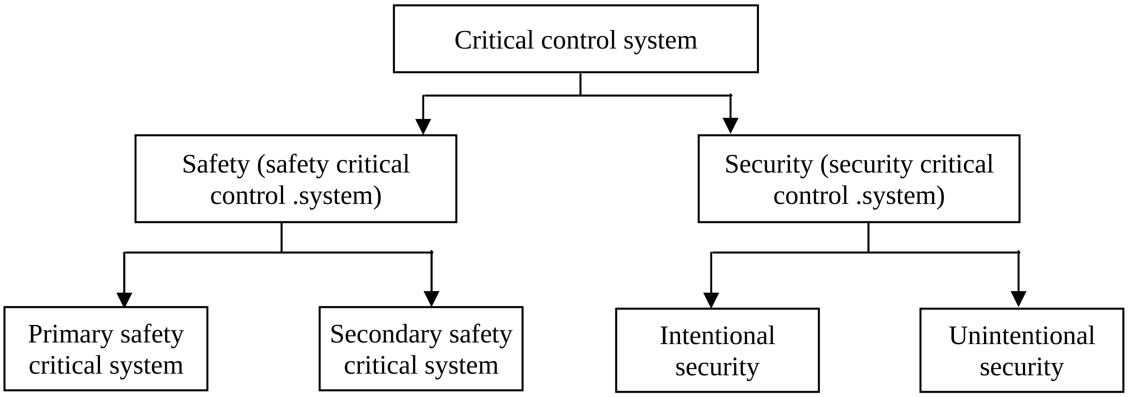

Critical control system
Safety (safety critical control .system)
Security (security critical control .system)
Primary safety critical system
Secondary safety critical system
Intentional security
Unintentional security

Figure 2 Critical control system with safety and security aspects

4. SIMILARITIES AND DIFFERENCE BETWEEN SAFETY AND SECURITY ASPECTS

Safety and security, although different, but share some similarities. According to [26], both aspects are considered as non-functional requirements, the main aim is to protect. In [27] defined that both safety and security deals with risks include protective measures, and generate requirements. Therefore, these commonalities indicate that some of the techniques which are suitable for one domain could also be relevant to the other. For instance, tools/techniques that assess the hazards in safety-related systems, i.e, HAZOPS and FMECA, have been utilized to analyze security aspect

[1]. In [28] demonstrates some commonalities between safety and security as security could improve from fault tolerant and hazard investigation methods that utilized by safety engineers. In turns, safety might be better by the use of fault preventative methods that is utilized by the security field. Although safety and security share several similarities, but there are some dissimilarities between these two aspects. Safety is protecting the environment from the system and security is protecting the system from the environment. In other words, they are entirely separate concern defined in [26] with an example, the system may be safe but not secure such as a medical information system allow a doctor to directly get the patient records without using a secret key. On the other hand, a secure system may not be safe, for instance: if it takes a longer time to enter a secret key then the patient may die before they can get their records. [1] depict the major dissimilarity between safety and security is the source of risk: safety consider hazards, (how the system may damage the surrounding because of system failure or some mixture of accidental situation), on the other hand, security considers threats and takes into account on how potential attacks may effect on the system's property and its function due to vulnerability. [1, 29, 30] demonstrate the dissimilarities in the nature of consequences of safety and security. The risk of safety could have a probable impact on the system surroundings whereas security is related to risks on the outcomes of the system itself as depicted in Fig.3. [31] define that safety is protection against random occurrences (i,e undesirable incidents) and security is protection against intended occurrence (i.e, wanted incidents). In [1] describes the difference between assessments security threats and safety hazards. In the case of security, the source of threats to be evaluated are usually not well known by predictor and cover a very extensive range of probable scenario. In the case of safety, the characteristic of hazards are more feasible and a number of conditions to be taken into account may also be condensed to a set that is constrained.

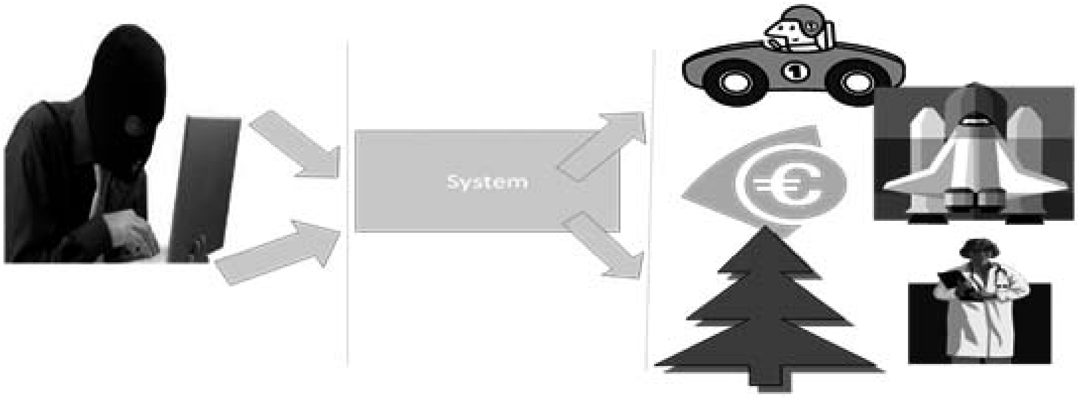


Figure 3 Security vs safety

5. PROCESS OF SECURITY AND SAFETY ASSESSMENT:

There are several safety and security risk analysis methodologies that can be used but they all incorporate the following phases [27] as shown in Fig 4a and 4b. The detail summary of different critical systems, issues and assessment techniques are shown in Table1.

Safety analysis

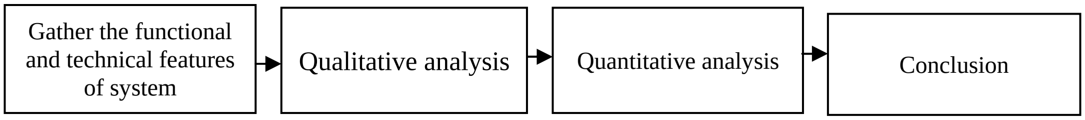


Figure 4(a) Phases of safety [27] [[analysis

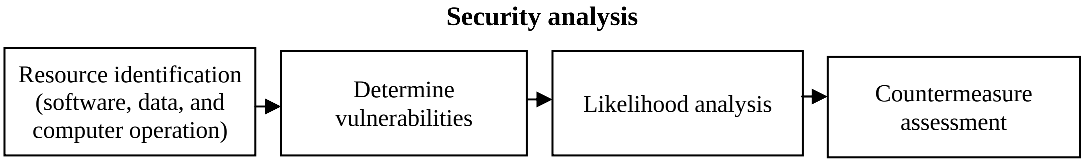

Security analysis
Resource identification (software, data, and computer operation)
Determine vulnerabilities
Likelihood analysis
Countermeasure assessment

Figure 4 (b) Phases of security []analysis

Table 1
Detail summary of SCSs, issues and assessment techniques

Author, Year	*Safety critical systems* (Case study is used for evaluating proposed approach)	*Issues*	*Assessment Techniques/methodology*
Singh and Rajput (2016)	Nuclear power plant (Shutdown system 2(SDS2))	Identify and addressing the safety issue of SDS2	Petri Net (PN)
Subramanian and Zalewski (2013)	Cyber-physical system (Oil - pipeline control system)	Evaluate the safety - security cyber-physical system	Non-functional requirement approach
Bompard et al. (2009)	Smart grid	Cyber security assessment for smart grid	Novel mathematical framework based on game theory
Kornecki et al. (2013)	Aviation system	Analyzed the requirement of safety-security issues and mitigate them in critical system	Fault tree analysis
Schmittner (2014)	Distributed industry measurement critical system	Analyzed combined safety-security aspects of complex mission critical system	Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) approach
Roth and Liggesmeyer (2013)	Tire pressure monitoring system	Modeling and categorized safety - security issues of the cyber-physical system	State/event fault tree
Kharchenko et al. (2015)	Field-programmable gate array based instrumentation and control system	Analyzed and assured security issues of instrumentation and control system	Used gap analysis, intrusion modes and effects criticality analysis technique
Park et al.,(2007)	Functional block module of nuclear digital	Evaluate the safety of the functional block module of the nuclear digital protection system	Software Hazard and Operability Analysis (HAZOP) and software fault tree analysis(SFTA)
Yoo and Cha (2012)	Nuclear power reactor protection system software in Korea	Verification of safety of reactor protection system	Software fault tree
Garrett and Apostolakis (2002)	Space based reactor control system	Automatically analyzed or validating the safety(hazards analysis i.e, unknown failure analysis)digital instrumentation requirement of software control system	Dynamic flow graph methodology
Shimeall and Gill(1991)	Military flight control system	Analyze the software safety of digital control system	Integrated fault tree analysis and timed Petri net
Goddard (1993)	Hughes aircraft	Evaluate the safety of embedded real time control system	Failure mode and effect analysis (FMEA)

Table 1 Contd…

Lee and LU (2012)	Airlock system of a Canada deuterium uranium (CANDU) reactor of nuclear power plant	Assessment the safety (reliability and failure) of airlock system	Fault tree (FT) and PN (Mapping of FT into PN)
Jiaxi et al. (2006)	Cyber security vulnerability in SCADA systems, power management systems and management information systems of the power system	Cyber security vulnerability assessment of the power system	Formulas of probabilistic assessment and integrated risk assessment
Henry (2009)	Case study : non-automated hazardous liquid loading process	Evaluating the risk of cyber security (attack: attack space and breadth and depth of attack) on computer network operations on SCADA system	Used Petri nets
Kriaa et al. (2012)	Business corporate network and SCADA	Demonstrate security (modeled the Stuxnet attack) attack	Logic Driven Markov Processes (BDMP) modelling approach (mixture of FT with Markov processes) to model the stuxnet attack using KB3 tool.
Hewett et al., 2014	Sensor network of the smart grid SCADA systems	Analyze security (attacker i.e., Sybil attack, Node Compromise, Eavesdropping and Data Injection) of SCADA system	Game model
Zhang et al., (2010)	Mart information system	Assessment of security risk of software safety critical system	Used the combination of attack tree model and Bayesian network
Leveson and stolzy (1987)	Safety critical real time system	Analyze safety, recoverability and fault tolerance	Petri net for analyzing safety critical real time system
Duran et. al (2013)	Autonomous ground vehicle optical systems	Safety assessment	Bayesian belief network

6. RESULT AND DISCUSSION

This section demonstrate the result, which has been computed through analysing existing SCSs; their safety and security issues; corresponding assessment techniques. The Fig 5, demonstrate the statistics for the safety and security issues validated by studies. The 40% studies focuses on safety and security analysis of SCSs and small faction of the studies (20%) have been done for integrated safety-security issues assessment. The reason behind least studies in the interdependencies between safety and security domains is due to its diversity of interaction safety-security, its sectorial specificities, interdisciplinary and for its business insinuation [1].

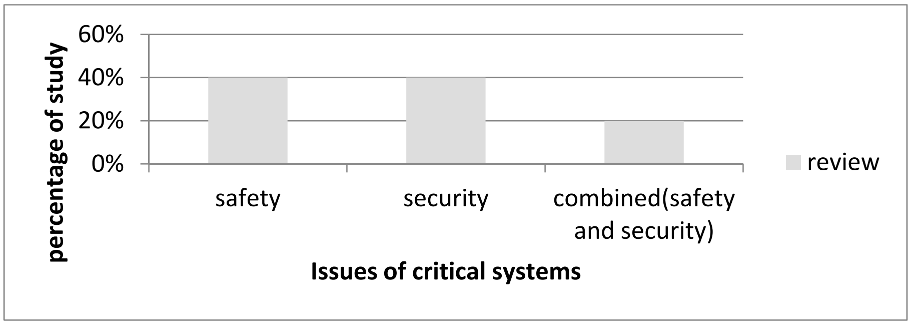


Figure 5 Percentage of studies for each evidence abstraction

7. CHALLENGES OF SAFETY CRITICAL SYSTEM

This section present challenges of SCSs which need to be resolved for assurance of safe and secure system.

Different studies delineated the issues for SCSs such as safety [32], software vulnerabilities, security, software error, unsuited patching and recurrent update for control system [5]; inaccurate specification of quality (reliability, performance and usability) requirement [35], interoperation among heterogeneous applications [33] and interdependencies between safety and security domains[1]. Still these issues are not completely resolved due to the reason: a) the techniques for ensuring the complex safety-security concerns have been slow in development. b) The increased demand of societies and industry has made system more complex c)Absence of modular analysis for certification d) Certification cost is higher d) Deficiency of openness to improvement and new approach e) Lack of techniques for specifying quality(reliability, performance and usability) requirement of software. f) Lack of techniques that provide a high level of assurance of non-interference between SCSs. g) An interruption in the interaction between system engineering and software engineering h) Security in SCSs; and interdependencies between safety and security domains is still challenging task due to its diversity.

Various incidents have occurred due to the reason of these issues such as a) Between 1985 and 1987, six accidents concerned massive overdoses by the Therac-25, it become cause of deaths and serious injuries (reason was safety issue) [36], b) SQL injection vulnerabilities in the Comersus shopping cart 5.09 system in 2005 (caused by security vulnerabilities) [5], c) U.S electric suffered by the cyber attack in 2009 (reason was security issue)[34], d) Saxony-Anhalt train accident , in Germany , 2011 (software problem)[5], e) Emergency-Shutdown of the Hatch Nuclear Power Plant, 2008 and **i**ncorrectly installed engine software caused A400M Crash, 2015 (Reason was Patching and frequent update is not well suited for control system)[5], f) Collision of two trains: Local train and Indore-Gwalior Intercity Express in India, 2010 (safety (collision)) [5] Attackers expose a CarShark software tool, which could kill a car engine remotely, 2010 (the reason is interoperation among heterogeneous applications) [33] and need to specify the quality attributes such as reliability, availability, performance and usability of software control system (Eleven software companies still face this challenges)[35]. For that reasons, there is deliberately need to handle these open issues for reducing the number of accident and to project a system with high security.

8. CONCLUSION

The subject of software control system’s safety and security has profound technical, professional, students and personal aspect for the individual; who are involved in research, development, selling and are relayed upon computer controlled system. The complexity of the critical system is rising as more and more functionality is provided by software solutions. The intention of this study is to define the very important aspect of SCSs such as safety and security, its similarities and difference; different formal modeling techniques to resolve these issues and phases which followed by assessment techniques for evaluating them. In addition to this, this work present the challenges for the safety critical system. It is concluded from the review that still there is a need to consider some metrics such as safety, security, quality assurance, device interdependency for complete system certification due to the increasing in size and functionality of software control system.

References

[1] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, “A survey of approaches combining safety and security for industrial control systems”, Reliability Engineering and System Safety, 139, pp. 156-178, 2015.

[2] B. Littlewood, L. Bainbridge, and R.E Bloomfield, “The use of computers in safety-critical applications”, London, UK: Health and Safety Commission, pp.1-98, 1998.

[3] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, “Security challenges for medical devices”, Communications of the ACM, 58(4), pp. 74-82, 2015.

[4] M. Abinaya, and R.U. Devi, “Intelligent vehicle control using wireless embedded system in transportation system based on GSM and GPS technology”, International Journal of Computer Science and Mobile Computing, Vol. 3, Issue.9, pp.244-258, 2014.

[5] J.C. Knight, “Safety critical systems: challenges and directions”, Proceedings of the 24rd International Conference on Software Engineering, IEEE, pp. 547-550, 2002.

[6] I. Sommerville, Software Engineering. 9th edition, PEARSON, 2011.

[7] D.R. Duran, E. Robinson, A.J. Kornecki and J. Zalewski, “Safety analysis of autonomous ground vehicle optical systems: Bayesian belief networks approach”, Proceedings of the Federated Conference on Computer Science and Information Systems IEEE, pp.1419–1425, 2013.

[8] C.J. Garrett, and G.E. Apostolakis, “Automated hazard analysis of digital control systems”, Reliability Engineering and System Safety, 77(1), pp. 1-17, 2002.

[9] P.L. Goddard, “Validating the safety of embedded real-time control systems using FMEA”, Proceedings in Reliability and Maintainability Symposium, IEEE pp. 227-230, 1993.

[10] A. Lee, and L. Lu , “Petri net modeling for probabilistic safety assessment and its application in the air lock system of a CANDU nuclear power plant”, Procedia Engineering, Elsevier, 45, pp. 11-20, 2012.

[11] N.G. Leveson, and J. L, Stolzy, “Safety analysis using Petri nets”, IEEE Transactions on Software Engineering, 13(3), pp. 386-397, 1987.

[12] G.Y. Park, J.S. Lee, S.W. Cheon, K.C. Kwon, E. Jee, and K. Y. Koh, “Safety analysis of safety-critical software for nuclear digital protection system”, Computer Safety, Reliability, and Security, Springer Berlin Heidelberg, pp. 148-161, 2007.

[13] L.K. Singh, and H. Rajput, “Ensuring safety in design of safety critical computer based systems”, Annals of Nuclear Energy, 92, pp. 289-294, 2016.

[14] T.J. Shimeall, R.J. McGraw Jr, and J.A. Gill, “Software safety analysis in heterogeneous multiprocessor control systems”, Proceedings in Reliability and Maintainability Symposium, IEEE pp. 290-294, 1991.

[15] J. Yoo, E. Jee, and S. Cha, "Formal modeling and verification of safety-critical software” Software, IEEE 26(3), pp.42-49, 2009.

[16] Bompard, E, Gao, C, R. Napoli, A. Russo, M. Masera, and A. Stefanini, “Risk assessment of malicious attacks against power systems,” IEEE Transactions on System, Man, and Cybernetics, vol. 39, no. 5, pp. 1074-1084, 2009.

[17] M.H. Henry, R.M. Layer, K.Z. Snow and D. R. Zaret, “Evaluating the risk of cyber attacks on SCADA systems via Petri net analysis with application to hazardous liquid loading operations” , IEEE conference on technologies for homeland security, pp. 607–614, 2009.

[18] R. Hewett, S. Rudrapattana and P. Kijsanayothin, “Cyber-security analysis of smart grid SCADA systems with game models” In: Proceedings of the 9th annual cyber and information security research conference. ACM, pp. 109–112, 2014.

[19] Y. Jiaxi, M. Anjia, and G. Zhizhong, “Vulnerability assessment of cyber security in power industry”, 2006 IEEE PES Power Systems Conference and Exposition, pp. 2200-2205, 2006.

[20] V. Kharchenko, A. Kovalenko, O. Siora, and V. Sklyar, “Security assessment of FPGA-based safety-critical systems: US NRC requirements context”, International Conference on Information and Digital Technologies (IDT), IEEE, pp. 132-138, 2015.

[21] Y.K. Zhang, S.Y, Jiang, Y.A. Cui, B.W. Zhang, and H. Xia, “A qualitative and quantitative risk assessment method in software security”, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE),IEEE, Vol. 1, pp. 534-539, 2010.

[22] A. J. Kornecki, and M. Liu, “Fault tree analysis for safety/security verification in aviation software”, Electronics, 2(1), pp. 41-56, 2013.

[23] M. Roth and P. Liggesmeyer , “ Modeling and analysis of safety-critical cyber physical systems using state/event fault trees” , In SAFECOMP 2013-Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, pp. NA, 2013.

[24] N. Subramanian, and J. Zalewski, “Assessment of safety and security of system architectures for cyberphysical systems”, IEEE International Systems Conference (SysCon), pp. 634-641, 2013.

[25] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch , “Security application of failure mode and effect analysis (FMEA)” , In Computer Safety, Reliability, and Security, Springer International Publishing, pp. 310-325, 2014.

[26] C. Johnson, "Topic Description: Security of Safety-Critical Systems", Trends in Information Security, University of Glasgow, pp. 1-2.

[27] D.P. Eames, J. Moffett, “The integration of safety and security requirements”, Proceedings of the 18th international conference on computer safety, reliability and security, Springer Berlin Heidelberg London, UK; pp.468–480, 1999.

[28] D.F. Brewer, "Applying security techniques to achieving safety", RedmillF, Anderson T,editors. Directions in safety–critical systems. London: Springer, pp.246–56, 1993.

[29] B. Hunter, "Integrating safety and security into the system lifecycle", in: Improving systems and software engineering conference (ISSEC), Canberra, Australia, pp.147-158, 2009.

[30] L. Piètre-Cambacédès, and M. Bouissou, "Cross-fertilization between safety and security engineering", Reliability Engineering and System Safety, pp.110–126, 2013.

[31] E. Albrechtsen, “A generic comparison of industrial safety and information security”, Term paper in the PhD course "Risk and Vulnerability", NTNU. December 2002. Available at www.iot.ntnu.no/~albrecht

[32] H. Espinoza, A. Ruiz, M. Sabetzadeh, and P. Panaroni, “Challenges for an open and evolutionary approach to safety assurance and certification of safety-critical systems”, First International Workshop on Software Certification (WoSoCER), IEEE, pp. 1-6, 2011.

[33] E. K. Wang, Y. Ye, X. Xu, S.M. Yiu, L.C.K. Hui, and K.P. Chow, “Security issues and challenges for cyber physical system”, IEEE/ACM International Conference on Green Computing and Communications and International Conference on Cyber, Physical and Social Computing, pp. 733-738, 2010. IEEE Computer Society.

[34] Egozcue, E, Rodriguez, DH, Ortis,JA, Villar, VF and Tarrafeta, L , “Smart Grid Security”, Annex II. Security aspects of smart grid, European Network and Information Security Agency (report), pp.1-63, 2012.

[35] A. Shahrokni and R. Feldt, “Industrial Challenges with Quality Requirements in Safety Critical Software Systems,” 39th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA), IEEE, pp.78-81, 2013

[36] B. S. M. P. S. Ramaiah and A. A. Gokhale, “FMEA and fault tree based software safety analysis of a railroad crossing critical system”, Global Journal of Computer Science and Technology, 11(8), pp.1-5, 2011.