Scientific Research Publishing

Journal of Computer and Communications, 2017, 5, 94-100
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Survey of Approaches Reconciling between Safety and Security Requirements Engineering for Cyber-Physical Systems

Mohammed F. H. Abulamddi

Department of Software Engineering, University of Palestine, Al-Zahra, Palestine
Email: m.abulamddi@up.edu.ps

How to cite this paper: Abulamddi, M.F.H. (2017) A Survey of Approaches Reconciling between Safety and Security Requirements Engineering for Cyber-Physical Systems. *Journal of Computer and Communications*, **5**, 94-100.
http://dx.doi.org/10.4236/jcc.2017.51008

Received: December 21, 2016
Accepted: January 17, 2017
Published: January 20, 2017

Abstract

The fields of safety and security use different conceptual standards and methods. As a consequence, these two separate but related research areas utilize different approaches. Addressing the integration between safety and security concerns in this context, we would conduct a survey exploring approaches and standards that were created by the scholars to combine safety and security requirement engineering.

Keywords

Standards, Security, Safety, Reconcile, Dependability Requirements

1. Introduction

This paper presents our work-in-progress on approaches (in terms of Standards, Conceptual Framework, Risk-Based Model and Terminology) that were created by the scholars to combine safety and security requirement engineering.

Modern cyber-physical systems are found in important domains such as smart grid, automobiles, medical devices, building automation, avionics, nuclear plants, etc. Hence, they are increasingly prone to security violations. Often such vulnerabilities occur as a result of contradictory requirements between the safety/real-time properties and the security needs of the system. Many safety-critical systems have security issues (e.g. in a railway network management system), so communication between a train coordinator and train drivers must be authorized to ensure safe operation of the railway. Other systems may not have direct safety implications (e.g. an online banking system) but have security aspects with critical consequences.

As described in Axelrod [1], there are major cultural and orientation differenc-

es between software engineers responsible for safety-critical software-intensive systems and those responsible for security-critical systems. This is in large due to the requirement for security-critical systems to protect sensitive information (such as non-public personal information, and health-related data), intellectual property, versus the need to ensure that safety-critical systems (such as avionics software and software running on industrial control systems) do not harm people or the environment because these orientations are so different, and may have little overlap. The threats to these systems, their vulnerabilities and the consequences of breaches, malfunctions and failure are also very different.

The development of cyber-physical systems where safety and security are important aspects follows the same approach for assessing risk involved with the systems. In the safety field, the benefits of a system and its features have to be balanced against the possible accidental harm it might impose, while the security field needs to consider such benefits against possible malicious harm.

To clarify the difference between the meaning of safety and security, we referred to a study done by Cambacédès and Chaudet [2] which clarifies the differentiation of meaning of the two words in industrial and academic sectors. The study is focused on twelve industrial sectors that have created standards for safety and security, which have been linguistically analyzed in relation to safety and security concepts. The study points out the gap and the differences between the ways which each of the industrial sectors follows. For example, chemical industry has different safety and security concepts compared to power grid industry. The study also included the variations of concepts of safety and security as shown in Table 1.

Because we live in the Internet of Things (IoT) era where almost everything is connected to the networks, legacy techniques and standards have become unable to cope with the rapid change in terms of understanding and studying the environment of the Internet and the potential risks and challenges that may arise when current systems that work in isolated environments are connected to the network. This pushed the different industrial organisations to increase the pace at which standards and measures are improved like in the SCADA nuclear industry. For example, new standards were issued at the beginning of 2014 in the

Table 1. Explicit and exclusive definitions of security and safety in the literature [2].

Reference	Safety	Security
Firesmith [3] [4]	"The degree to which accidental harm is prevented, reduced and properly reacted to."	"The degree to which malicious harm is prevented, reduced and properly reacted to."
Line *et al.* [5]	"The inability of the system to affect its environment in an undesirable way."	"The inability of the environment to affect the system in an undesirable way."
Burns *et al.* [6]	"A system is judged to be safety critical in a given context if its failure could be sufficient to cause absolute harm."	"A system is judged to be security critical in a given context if its failure could be sufficient to cause relative harm, but never sufficient to cause absolute harm."

draft document IEC 62645 for security compatible standards after serious potential risks were recognised.

It is essential, when implementing critical safety software, that this software is able to verify whether the system is safe or not and it is usually on a high level of verifiability. This is not an easy process as the software systems could be complicated and therefore it would be difficult to determine whether they are truly safe or not. The goals of such standards can be summarised in the three following points:

"*Development*" is the process of putting the new system through the process of defining potential risks and threats in order to discover them and set out a methodology to avoid them. "*Operational management*" is the process of evaluating risks and threats which have been controlled to reach a higher degree of safety for the system. It also sets out a clear guide that explains every part of the system and how to interact with it, and trains the users on how to use the system. "*Certification*" is the process of proving the claimed system that has been developed is a safety system and to determine the degree of its safety.

Safety-critical and security-critical software systems are dynamic and interactive resulting in having unintentional hazards. The upgrading process is continuous as the main objective of monitoring the residual risk and its compliance to the standards and certificate [1].

In this article, we will conduct a survey according to the standards and approaches that combine safety and security. Combining safety and security models have been under focus from different perspective and areas. Some researchers focused on developing the architectural framework while others focused on narrowing down the gap between the definitions and terminology adaptation in both safety and security or narrowing down techniques and tools used in the system development life cycle.

2. Combining Safety and Security in Terms of Standards and Approach

New standards were created to deal with software-intensive systems: cyber-physical systems and shared-control systems [7] [8] [9]. These modern standards define the nature of maintaining (considering its software systems legacy, and connecting these systems to the network is highly risky because they lose the security engineering resistance), or building these systems from scratch to match the requirements of safety and security engineering. Not only that, new laws such as Cyber-security Act of 2012 appeared [10]. This bill addresses the threats and weaknesses in critical systems that are connected to the network and tries to take over them.

High-Assurance Cyber Military Systems (HACMS) Clean-Slate Approach, was introduced based on the highest quality results for critical systems regarding the safety and security engineering specifications DARPA [11], through the use of a rigid language for mathematical representation or a semi-automated executable code synthesis to get formal functions, which are machine-checkable

proofed leading to having code that meets with functional specification as well as security and safety specifications (Figure 1), where the blue squares represent formal specification, the most important synthesizer component, for a domain-specific is the synthesizer which takes the safety and security policies of an element, a functional specification, a description of the target hardware, resource constraints, and the description of the specific environment for the system to run in.

ISO 14971, standard addresses manufacturing medical devices and developing the software for them [7]. It also aims to integrate the process of risk management and an early stage of design, to produce evidence that their risk assessment process [7] has considered and addressed both intentional risks and unintentional hazards of the medical device with appropriate security controls as part of the device's design. Medical device manufacturers should consider the malicious activity during the early phases of the requirements engineering.

The draft guidance [9] titled "Management of Cyber-Security in Medical and Hospital Network", discusses the security risks against medical devices and imposes procedures to implement safeguards in order to reduce and avoid hazards related to device failure due to a malicious attack.

3. Combining Safety and Security in Terms of Conceptual Framework

A new approach has been found, through research that is currently being used to deal with safety "*Unintentional*" accident and security "*Intentional*" risk in systems that directly interact with the environment, like the new generation of nuclear power plants [12]. This method is called defense in depth (DiD) and used artifact term "Systems Theory" [13]. The systems that use DiD analysis get the results as a preventive plan based on the application of more than one safety layer to face more than one accident. These safety layers are a result of the nature

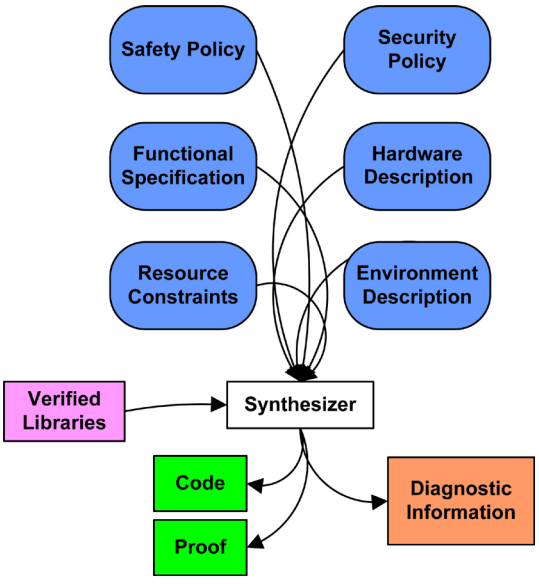

Figure 1. HACMS clean-slate approach, adapted from [11].

of the system itself. DiD method can be summarized in four essential phases: *Prevention*, *Control*, *Protection*, and *Mitigation* respectively. It is important to mention that this analysis will be performed in compatibility with the comprehensive overview specified in safety and security goals which affect the safety policy that prioritises the requirements in case of a conflict as in safety requirement the term "*Constraints*" is used. It describes limitations on how the goals can be achieved. But requirement refers to the behavior required to satisfy the system's goals [13].

Cambacédès and Chaudet focused on building SEMA referential framework [2]. The motivation behind this was to reveal the ambiguity of safety and security terms as researches focused on revising and analysing technical reports published by official bodies from several industries from safety and security perspective as well as academic researches. The second reason is that there are industries that overlap with each other and therefore it was important to reveal the ambiguity in each and every industry. Furthermore, to better reveal the ambiguity, definitions and terminologies were addressed separately and reflected upon SEMA Framework resulting in the ability of narrowing between the different industries from safety and security perspectives.

In 2007, Novak *et al.* proposed a complete life-cycle model [14]. And demonstrated the life-cycle model of safety and security to serve in building automation and control systems (BACS) by using guidelines for network hazards and threats linking the reflections on both safety and security requirements.

4. Combining Safety and Security in Terms of Risk-Based Model

Mayer *et al.* [15] propose security requirements engineering process that consists of the following four steps: context analysis and asset identification, security goal determination, refinement of these goals to security requirements, and countermeasures selection. Both of the latter two steps are based on a risk analysis approach named model-based information system security risk management (ISSRM). Thereby, Mayer *et al.* propose to make use of Yu's i* [16] [17] requirements engineering techniques, which can also be used to deal with security requirements [18]. The proposed method by Mayer *et al.* comprises security requirements elicitation driven by a risk analysis method. It also supports analyzing security requirements through context and asset analysis.

Eames and Moffett presented an integrated process to take the potential conflicts or synergies between safety and security requirements into account. In 2005, the SafSec methodology was used as a unified risk assessment framework aiming at reducing the effort, cost and timescales associated with certification of modular systems [19].

5. Combining Safety and Security in Terms of Terminology

Avizienis *et al.* [20] addressed taxonomy of dependable and security by defining dependability from the security perspective and explained the means that could

help achieve dependability in security. Furthermore, the researchers focused on taxonomy of threats, taxonomy of faults, and pathology of failure in the sense of explaining the terminologies but did not reflect them on a model.

Firesmith [3] [4] [21] addressed the terminology of the taxonomy of safety and security as addressed by other researchers but what makes his researches different is that he focused on narrowing down the gap between safety engineering and security engineering through the implementation of information model that relies on integrating and linking safety and security while maintaining survivability and established underlying foundational concepts between them and safety concepts and relations using UML. Furthermore, in his latest work [4] he redefined safety engineering and security engineering from his definitions so, the size of the comparison is clearly shown in the definitions he proposed and has also worked on enhancing it in tutorials [4].

6. Summary and Further Work

The meaning of the terms—security and safety varies considerably from one context to another, leading to potential ambiguities. These ambiguities are very problematic in the critical infrastructure of the protection domain, which involves multiple actors and engineering disciplines. Avoiding misunderstandings caused by the ambiguities during the early stages of system design and risk assessment can be benefited. It also helps to ensure a more consistent and complete risk coverage. The researchers have explored integration between safety and security through using different structured approaches, so they can thereby act as an interface for active interactions in risk and hazard management in terms of universal coverage, finding solutions for differences and contradictions which can be overcome by integrating the safety and security domains and using a unified system analysis approach that will result in analysis centrality.

In the future work, we would conduct a survey exploring technical languages that were created by the scholars to combine safety and security requirement engineering and accident analysis technique languages.

References

[1] Axelrod, C.W. (2012) Engineering Safe and Secure Software Systems. Artech House, Norwood.

[2] Ludovic, P.-C. and Chaudet, C. (2010) The SEMA Referential Framework: Avoiding Ambiguities in the Terms "Security" and "Safety". *International Journal of Critical Infrastructure Protection*, **3**, 55-66. https://doi.org/10.1016/j.ijcip.2010.06.003

[3] Firesmith, D.G. (2003) Common Concepts Underlying Safety Security and Survivability Engineering. No. CMU/SEI-2003-TN-033. Carnegie-Mellon UNIV Pittsburgh Pa Software Engineering Inst.

[4] Firesmith, D.G. (2010) Engineering Safety and Security-Related Requirements for Software-Intensive Systems: Tutorial Summary. *Proceedings of the* 32*nd ACM/IEEE International Conference on Software Engineering*, **2**, 1-44.

[5] Line, M.B., Nordland, O., Røstad, L. and Tøndel, I.A. (2006) Safety vs. Security? *Proceedings of the* 8*th International Conference on Probabilistic Safety Assessment*

& Management (*PSAM*), ASME Press, New Orleans.

[6] Burns, A., McDermid, J. and Dobson, J. (1992) On the Meaning of Safety and Security. *The Computer Journal*, **35**, 3-15. https://doi.org/10.1093/comjnl/35.1.3

[7] (2012) ISO, BSEN. 14971: 2012, Medical Devices. Application of Risk Management to Medical Devices.

[8] Bouard, J.-P. (2011) IEC 62645 Ed. 1: Nuclear Power Plants-Instrumentation and Control Systems-Requirements for Security Programmes for Computer-Based Systems.

[9] US Food and Drug Administration. FDA Safety Communication: Cyber Security for Medical Devices and Hospital Networks. Retrieved May 1 (2013): 2014.

[10] CSA2012, Last Accessed on 10 April 2016. www.hsgac.senate.gov

[11] Launchbury, J. (2015) High-Assurance Cyber Military Systems (HACMS). DARPA Program Information.

[12] Wallace, E.G., Fleming, K.N. and Burns, E.M. (2009) Next Generation Nuclear Plant Defense-in-Depth Approach. No. INL/EXT-09-17139, Idaho National Laboratory.

[13] Leveson, N. (2011) Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, Cambridge.

[14] Novak, T., Treytl, A. and Palensky, P. (2007) Common Approach to Functional Safety and System Security in Building Automation and Control Systems. *IEEE Conference on Emerging Technologies and Factory Automation*, Patras, 25-28 September 2007, 1141-1148.

[15] Mayer, N., Rifaut, A. and Dubois, E. (2005) Towards a Risk-Based Security Requirements Engineering Framework. Workshop on Requirements Engineering for Software Quality. *Proceeding of Requirements Engineering for Software Quality*, **5**, 89-104.

[16] Yu, E.S.K. (1997) Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering. *Proceedings of the* 3*rd IEEE International Symposium on Requirements Engineering*, Annapolis, 6-10 January 1997, 266-235. https://doi.org/10.1109/ISRE.1997.566873

[17] Yu, E. and Liu, L. (2001) Modelling Trust For System Design Using the I* Strategic Actors Framework. In: Falcone, R., Singh, M. and Tan, Y., Eds., *Trust in Cyber-Societies*. Springer, Berlin, 175-194. https://doi.org/10.1007/3-540-45547-7_11

[18] Liu, L., Yu, E. and Mylopoulos, J. (2003) Security and Privacy Requirements Analysis within a Social Setting. *IEEE International Requirements Engineering Conference*, Monterey Bay, 12 September 2003, 151-161. https://doi.org/10.1109/icre.2003.1232746

[19] Eames, D. and Moffett, J. (1999) The Integration of Safety and Security Requirements. *International Conference on Computer Safety*, *Reliability*, *and Security*, Toulouse, 27-29 September 1999, 468-480. https://doi.org/10.1007/3-540-48249-0_40

[20] Avizienis, A., Laprie, J.C., Randell, B. and Landwehr, C. (2004) Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, **1**, 11-33. https://doi.org/10.1109/TDSC.2004.2

[21] Firesmith, D.G. (2005) A Taxonomy of Safety-Related Requirements.