Cyberphysical Systems

Subjects: Computer Science, Information Systems

Contributor: Sokratis Katsikas, Georgios Kavallieratos

Cyber-physical systems (CPS) merge the physical and cyber world to support critical functions and services. Cyber-security and safety are interdependent in such systems and therefore their study should be performed jointly. Various approaches have been proposed for cyber-security and safety co-engineering. In this entry, the key results of a comprehensive survey of such co-engineering approaches, along with various aspects of the problem that have not been sufficiently addressed in these methods, are presented.

Keywords: Safety ; Cyber-security ; co-engineering ; survey

1. Introduction

Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. They are deployed in various application domains, such as automotive, smart manufacturing, and healthcare. The analysis of cyber-security and safety for such systems is important, and usually complicated due to strong dependencies between the cyber-security and safety domains. Three types of dependencies have been identified and analyzed in [1]; **Conditional dependencies, Reinforcement,** and **Conflict**. Such dependencies are studied and addressed by cyber-security and safety co-engineering approaches in varied degrees of depth and scope. Three different categories of cyber-security and safety co-engineering exist [2]; 1)**Security-informed safety approaches:** Approaches that extend the scope of safety engineering by adapting cyber-security-related techniques. 2) **Safety-informed security approaches:** Approaches that extend the scope of security engineering by adapting safety-related techniques, and 3) **Combined safety and security approaches:** Combined approaches for safety and cyber-security co-engineering.

Cyber-security and safety co-engineering approaches aim to identify, assess, and manage risks related to both security and safety in systems which are influenced by both the cyber and the physical world/environment. Although various surveys of cyber-security and safety co-engineering methodologies exist in the literature, the analysis and comparison of the existing methods vary in both the depth and the scope of the analysis. Piètre-Cambacédès et al. [3] surveyed the differences and similarities between safety and security aspects focusing on their dependencies per application domain. Kriaa et al. [4] conducted a survey of safety and security analysis methods and analyzed methods for industrial control systems. Various safety and security risk assessment methods, categorized according to their application domain, were reviewed by Chockalingam et al. [5]. Abulamddi [6] surveyed existing methods for safety and security requirements engineering in CPSs. A systematic literature review was conducted by Lisova et al. [7] that focused on already developed and evaluated methods. Lyu et al. [8] provided a short survey, in which five integrated safety and security co-engineering methods were analyzed. Finally, Paul and Rioux [2] provided an extended bibliography of research papers on safety and cyber-security co-engineering since the early 90's without, however, analyzing them.

This entry provides a summary of the results of a comprehensive review of sixty-eight co-engineering approaches [10]; it presents the key characteristics of such approaches, and it identifies issues for cyber-security and safety joint analysis that are not sufficiently addressed by the existing co-engineering methods.

Figure 1 provides a comprehensive picture of the current methodologies for cyber-security and safety analysis of CPSs, that forms a taxonomy of such methods. The attributes utilized for the analysis are used in prior surveys or related publications [4][5][7][8][9]. Further, the following characteristics provide additional insight into understanding the operational capacity of each method: Process (the extent to which the method is supported by a systematic and structured process), Scalability, Creativity (the extent to which the method includes mechanisms to stimulate creativity among the stakeholders), Communication (the extent to which the method offers features to facilitate communication between different stakeholders), Conflict resolution (the extent to which the method facilitates the identification and study of potential conflicts between safety and security aspects), Software tool (the extent to which the method is supported by software tools).

2. Methodologies for Cyber-security

Figure 1 also depicts (in parentheses) the number of existing co-engineering methodologies that have the corresponding attribute. Thus, it provides a bird's eye view of the area. By leveraging this information, the weaknesses and strengths of existing approaches can be identified, thus allowing the identification of still open issues in the joint analysis of cyber-security and safety.

Figure 1: Attributes: Results

Such issues that have been under-researched have been identified and are listed below:

- *Conflict resolution between cyber-security and safety results*: Goal-oriented integrated co-engineering approaches could lead to less conflicting results. Further, the joint cyber-security and safety analysis should be performed at the early stages (requirements engineering phase) to resolve potential conflicts easier towards the development of safe-and-secure CPSs by design.
- *Standard methodology*: A lack of application-domain-independent methodology has been noticed.
- *Validation*: More research is needed to evaluate the correctness, completeness, effectiveness, efficiency, scalability of existing methods, in a manner that will facilitate comparative assessments.
- *Safety and Cyber-security standards:* Some standards addressing safety and security for industrial control systems exist. Examples of such standards are ISA99/IEC 6443, IEC 62645, IEC TR63609, ISO26262 to name a few; cross-references with other standards (e.g., IEC 61508) also exist. However, the applicability of such standards to effectively address both safety and security, particularly in an industry 4.0 context, is still to be firmly established. The adoption of standards specific for industry sectors, along the lines of the practice followed in the nuclear plant domain will guide the development of safe-and-secure-by-design industrial control systems.
- *Application domains*: The transportation domain prevails among application domains addressed by the existing methods. As several emerging application domains are both safety-and-security-critical (e.g., autonomous vessels, drones), the development of methods addressing specifically systems in such domains remains an issue.
- *Dynamic character of CPS:* The dynamic nature of CPSs is an important issue that needs to be addressed during cyber-security and safety analysis.
- *Model Type*: An approach able to handle the complexity of CPS by leveraging both graphical models and systematic perspectives would allow the consolidation of advantages of both worlds.
- *Holistic approach*: Future methods should enjoy attributes such as scalability, communication, and model type, in order to facilitate the analysis of CPSs when both technical and human aspects are considered.

This entry provided the key findings of our work in [10]. Having revisited the existing surveys for cyber-security and safety co-engineering approaches, the methodologies that have not been reviewed before have been identified. Further, a multi-attribute taxonomy was proposed towards a comprehensive analysis of the existing approaches and the identification of the open issues in the joint analysis of cyber-security and safety in CPSs. Thus, a comprehensive discussion on the recent advances in cybersecurity and safety co-engineering was provided. Building upon the results of this survey, an integrated goal-based approach for joint safety and cyber-security requirements elicitation that enjoys several of the desirable characteristics and attributes of such a method is proposed in [11].

References

1. Pièrre-Cambacédès, L.; Bouissou, M. Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). In Proceedings of the 2010 IEEE International Conference on Systems, Man and Cybernetics, Istanbul, Turkey, 10–13 October 2010; pp. 2852–2861.
2. S. Paul; L. Rioux; Over 20 years of research into cybersecurity and safety engineering: a short bibliography. *SAFE 2015* **2015**, *151*, 335-349, 10.2495/safe150291.
3. L. Pièrre-Cambacédès; M. Bouissou; Cross-fertilization between safety and security engineering. *Reliability Engineering & System Safety* **2013**, *110*, 110-126, 10.1016/j.ress.2012.09.011.
4. Siwar Kriaa; Ludovic Pietre-Cambacedes; Marc Bouissou; Yoran Halgand; A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety* **2015**, *139*, 156-178, 10.1016/j.ress.2015.02.008.
5. Sabarathinam Chockalingam; Dina Hadžiosmanović; Wolter Pieters; André Teixeira; Pieter Van Gelder; Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. *Computer Vision* **2017**, *10242*, 50-62, 10.1007/978-3-319-71368-7_5.
6. Mohammed F. H Abulamddi; A Survey on Techniques Requirements for Integrateing Safety and Security Engineering for Cyber-Physical Systems. *International Journal of Computer Science & Engineering Survey* **2016**, *7*, 1-15, 10.5121/ijcses.2016.7601.
7. Elena Lisova; Irfan Sljivo; Aida Causevic; Safety and Security Co-Analyses: A Systematic Literature Review. *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* **2019**, *1*, 833-833, 10.1109/compsac.2019.00122.
8. Xiaorong Lyu; Yulong Ding; Shuang-Hua Yang; Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications* **2019**, *4*, 221-232, 10.1049/iet-cps.2018.5068.
9. Christian Raspotnig; Andreas L Opdahl; Comparing risk identification techniques for safety and security requirements. *Journal of Systems and Software* **2013**, *86*, 1124-1151, 10.1016/j.jss.2012.12.002.
10. Georgios Kavallieratos; Sokratis Katsikas; Vasileios Gkioulos; Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. *Future Internet* **2020**, *12*, 65, 10.3390/fi12040065.
11. Kavallieratos Georgios; Katsikas Sokratis; Gkioulos Vasileios; SafeSec Tropos: Joint security and safety requirements elicitation. *Computer Standards & Interfaces* **2020**, *70*, 103429, https://doi.org/10.1016/j.csi.2020.103429.