Inadequate risk analysis might jeopardize the functional safety of modern systems[1]

By Kaj Hänninen[2], Hans Hansson[3], Henrik Thane[4] and Mehrdad Saadatmand[5]

Abstract: In the early 90s, researchers began to focus on security as an important property to address in combination with safety. Over the years, researchers have proposed approaches to harmonize activities within the safety and security disciplines. Despite the academic efforts to identify interdependencies and to propose combined approaches for safety and security, there is still a lack of integration between safety and security practices in the industrial context, as they have separate standards and independent processes often addressed and assessed by different organizational teams and authorities. Specifically, security concerns are generally not covered in any detail in safety standards potentially resulting in successfully safety-certified systems that still are open for security threats from e.g., malicious intents from internal and external personnel and hackers that may jeopardize safety. In recent years security has again received an increasing attention of being an important issue also in safety assurance, as the open interconnected nature of emerging systems makes them susceptible to security threats at a much higher degree than existing more confined products.

This article presents initial ideas on how to extend safety work to include aspects of security during the context establishment and initial risk assessment procedures. The ambition of our proposal is to improve safety and increase efficiency and effectiveness of the safety work within the frames of the current safety standards, i.e., raised security awareness in compliance with the current safety standards. We believe that our proposal is useful to raise the security awareness in industrial contexts, although it is not a complete harmonization of safety and security disciplines, as it merely provides applicable guidance to increase security awareness in a safety context.

Introduction

Software intensive safety-critical systems have been around for a few decades now and there are well-established approaches for ensuring their safety, essentially originating from safety practices within the aerospace industries. Safety practices in these and other domains are dictated by safety-standards that prescribe how systems should be developed, verified and maintained to minimize risks of accidents during the lifetime of a product.

[1] This work was performed in the FIA-PiiA project within the Swedish national Vinnova funded strategic innovation programme Process-industrial IT and Automation; www.piia-sip.se
[2] Mälardalen University (kaj.hanninen@mdh.se)
[3] SICS Swedish ICT Västerås and Mälardalen University (hansh@sics.se)
[4] Safety Integrity AB (henrik.thane@safetyintegrity.se)
[5] SICS Swedish ICT Västerås (mehrdad@sics.se)

When developing safety related electronic and programmable control systems, there are a number of sector specific standards that need to be considered, for example:

- ISO13849 and IEC62061 for machines with moving parts (e.g., Industrial robots),
- ISO26262 for Automotive,
- EN50129/EN50128 for Railway, and
- IEC61508 for generic control systems

These standards outline the requirements and recommendations for the safety work in the respective domain. Many of the sector specific standards that have been developed in recent years stem from the IEC61508 standard. In developing a sector specific standard the IEC61508 has been a fundamental source of inspiration for the developers of sector specific standards. Some concepts from the IEC61508 have been adapted as is, whereas other concepts have been reworked to fit the practices in the specific domains.

Safety-related systems connected to the Internet

Traditionally, safety related systems have been closed stand-alone products, but recently they are increasingly interconnected or provided with interfaces to the Internet to allow remote diagnostics or enhanced Infotainment as in the case of modern cars. Allowing external communication is an enabler for many useful and exciting functions and services, but is also potentially dangerous, as it opens up for a whole range of security threats. An example is the remote operation of a Jeep Cherokee[6] via the infotainment interface, allowing remote control of braking and steering. A more classical example is the Stuxnet Worm[7] that specifically targets PLCs, which are used in automation of e.g., machinery on factory assembly lines. Stuxnet is believed to be a jointly built American-Israeli cyber weapon, built to target Iranian centrifuges for separating nuclear material. Further examples include hacked insulin pumps and drug infusion pumps. Hacks of the latter have even prompted warnings from the US FDA[8] resulting in guidance on how to address cyber-security to assure safety of medical devices. There are also examples of hacks causing damage to the environment, including a disgruntled former employee that hacked a water treatment facility in Queensland, Australia, deliberately spilling nearly a million liters of raw sewage into local waterways and parks[9].

Although there are well-established security engineering lifecycles, it should be clear from the above examples that there is a lack of guidance on how to combine and exchange knowledge and results of the work in the disciplines. Moreover, the distinction between safety and security is not always clear. What is clear however is that security threats must be considered in the safety work, as system safety (beyond any reasonable doubt) cannot be established for modern open interconnected systems unless the safety work is extended

[6] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[7] https://en.wikipedia.org/wiki/Stuxnet
[8] http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm456832.htm
[9] http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

to take aspects of security into account. Nevertheless, current safety standards do generally not prescribe that security threats shall be evaluated in terms of potential hazards, and consequently there are no requirements on mitigations of those threats.

For instance, the railway standards EN50126, EN50128 and EN50129 describe security as an element that can be considered as a component of RAMS (Reliability, Availability, Maintainability, Safety). However, the consideration of security is outside the scope of the standards (with the exception of security in terms of protection against unauthorized access). The road vehicle standard ISO26262 do not mention security at all. The IEC61508 standard recommends that reasonably foreseeable security threats originating from malevolent or unauthorized action should be analyzed. For guidance on vulnerability and risk analysis the standard refers to IEC62443.

The main reason why security is given less attention in the safety standards is the limit of scope that all functional safety standards prescribe. They are essentially restricted to protection against failures and a degree of foreseeable misuse of the systems, not against intentional abuse and misuse.

Safety standards are out of synch with recent developments

Although some safety standards recommend addressing security, it is perfectly possible to get a product approved according to safety standards, while there are still remaining security dependencies that could impact safety and cause an accident. This does not imply that the safety or security works are flawed, contrary it implies that addressing of the interdependencies between them are not regulated or guided enough in normative safety standards. As companies tend to focus on getting an approval by safety-certification authorities, rather than ensuring safety under all conditions including security threats. If this practice is not amended, we are bound to see incidents and accidents in the near future.

In these perspectives the long revision periods of safety standards is a real and serious problem. The committees working on these standards are for each new revision trying to catch up with new developments in the industry in terms of new technologies, increased complexity, new application domains, etc. As such, the standards are often out-of-date, and have usually a 10-year turnaround time between new versions. Thus, the rapid technical development is in itself a threat to safety. Updating and extending the scope of standards is however not a simple task. Considering that it is non-trivial to understand the interdependencies and differences between modern safety critical and security critical systems, regulating processes and providing recommendations for activities and allocation of responsibilities in assuring risk reduction, becomes extremely difficult.

Considering security risks in the safety management process

Our claim is that an extended safety approach, considering relevant aspects of security together with safety, is required to amend the current practice. For the approach to be applicable in industrial contexts, and approvable by

assessment authorities, the extension must be performed in such way that the proposals complies with the normative safety standards. A harmonization of the activities within the practices has been subject for the research community since the early 90s (see e.g., [2]-[61]; [55] presents an extensive survey of approaches combining safety and security). A problem with extensive harmonization approaches is that they may invalidate recommended normative activities, recommendations or practices in the standards. This implies that they need to be adapted by standardization authorities, i.e., they are generally not directly applicable in an industrial context, unless the normative standards are updated to support them. A typical example of this is the efforts in harmonization of risk classification schemes/procedures of different disciplines.

Safety and Security in an industrial Case Study
We have taken initial steps towards development of an extended safety approach in the context of current standards. We considered a wide range of security threats and applied a safety standard (IEC62061 – "Safety of Machinery") and a security standard (ISA/IEC-62443, "Industrial communication networks") on a real industrial case. These standards both have the goal to reduce risk, but have somewhat different approaches to manage risk. We have studied the standards, identified commonalities and differences, and based on the differences we have extended the regular safety risk management process to include security threats.

In the following we outline the basic steps to extend the activities of a risk management process that complies with IEC62061.

- **Extending the System Definition:** The system definition is the foundation on which all succeeding functional safety work is based. It defines the scope and intended functionality of the product, its environment, as well as its interfaces. All risk analysis is based on the system definition. Specifically, the hazards identification process starts from the system definition in identifying all hazards that can lead to accidents, incidents, damage or significant financial losses. It is therefore important that the system definition is complete and correct to facilitate the identification of all potential sources of hazards. With the increasing interconnectivity of modern automation control systems, the functional safety system definition must be extended to cover not only failures from within the product itself, but also intentional misuse and sabotage.

  In doing this, the traditional reasoning about sources of hazards (failures and foreseeable misuse) must be extended to also include intentional misuse. This implies that the failure model of the environment and interface parts of the system definition will have to be extended with actors and assets being part of, or interfacing, the system. With the complexity and interconnection of entities within modern systems, the establishment of a system definition is however not trivial. To support the definition process, guidance on typical assets and actors that may affect operations are necessary. Within our work,

we identified the following threats and interfaces as important to consider when extending a typical safety system definition (note that the list is not complete in any sense, it is purely for guidance)

- People (internal and external personnel, design authorities, subcontractors, competitors, litigants, press, hackers, criminals, terrorist etc.)
- Nature and accidents (e.g., fires, storms, floods, transportation accidents etc.)
- Interfaces and assets (e.g. fieldbuses and I/O for system functionality, internal product buses and interfaces, sensors, actuators, configuration interfaces, control interfaces, monitoring interfaces and diagnostics interfaces, maintenance interfaces, testing interfaces and upgrading interfaces, infotainment interfaces, external product interfaces (e.g., authentication and authorization interfaces, session management interfaces, USB interfaces etc.), cellular interfaces and additional assets such as., mobile-enabled devices, printers, USB devices, control centers, cloud services, computers, etc.).

The idea with the guidance list is to identify points allowing tampering with wireless and wired communication links, USB ports, user interfaces, etc. and tampering by personnel (both internal and external) during development, testing, maintenance, production, and operation. These assets and actors must all be included as extensions to the traditional system definition and thus the scope and boundary of a traditional system definition will be extended thereafter.

Establishing a system definition has traditionally been the responsibility of the safety organization. It is clear that this work cannot be performed by the safety organization alone. We cannot expect them to have the overall knowledge of everything included in modern interconnected systems. Instead, establishing a system definition should be a joint work that gathers the organizational teams that together can contribute with their knowledge in an effort to establish a complete and correct definition.

- **Extending the Hazards Analysis**: Hazard analysis is the second most important step (after writing the system definition) in the safety management process of developing safe systems. The purpose of the analysis is to identify, quantify, rank, and list hazards that can cause accidents or losses during the lifetime of the product. The hazard analysis can be performed with various techniques, and at different stages of the lifecycle. A preliminary hazard analysis is usually performed in the concept phase before any development has been initiated. The hazard analysis is then refined when more details of the system design emerges, and repeated when performing maintenance. A typical hazard analysis that focuses on safety is guided by experiences from similar projects and different analysis techniques such as fault tree analyses, failure mode and effects analyses, event

tree analyses etc. The security domain has similar guidance from e.g., threat models, attack tree analyses etc. In our extension of the hazard analysis, we include security threats in the safety analysis, where we essentially assume that failures are not only stemming from the system itself but also from people with malicious intent. The extended scope of the system definition allows for previously unforeseen safety hazards, and additional ways in which a system might enter a hazardous state, to be identified. This results in a more security-aware safety management process.

- **Risk Classification and Mitigations:** Each hazard that has been identified during the hazard analysis must be classified in terms of risk[10] according to the schemes proposed in the safety standards. The new security related hazards that have been found using the extend hazard analysis have therefore to be classified according to the same scheme. Note that this does not imply that the risk classification proposed by the security standards should be ignored for security risks. The reason to classify the security related safety risks according to a safety scheme serves two main purposes: 1) to assure compliance with the safety standard being used and 2) to assure that all safety risks have been classified according to the same scheme. Note also that risk classification stemming from any reused sources of already identified hazards may have to be re-assessed[11] since the scope of the system definition has changed. All hazards (new as well as old) must then be mitigated with safety measures that are on par with the risk classification of the hazard in order to be able to claim that the risk is tolerable. The functional safety standards mandate different levels of rigor for the development and maintenance process, including techniques and measures to be applied depending on the identified risk level (SIL, ASIL, PL, etc.). A consequence of our extended analysis is that proper mitigations may not be found in the safety standards, but have to be taken from the security standards. Here it is necessary to translate the rigor required between the different domains and standards.

- **Assessing Risk Mitigations:** It is advisable that the safety management process distinguish between hazards discovered from a pure safety perspective, hazards discovered from a security perspective that have safety impact, and hazards discovered from an extended safety perspective that includes security threats. The main reason why the origins of the hazards should be categorized is the fact that this allows risk reduction measures to be more appropriately designed. Where the origins of the hazards are purely safety related (e.g., due to failures, foreseeable misuse etc.) the risk reduction

[10] For example, IEC 62061 mandates a classification procedure that considers the consequence of each hazard, the severity (S) of each hazard, the anticipated rate (F) of occurrence, the anticipated occurrence probability (P) of each hazard and measures for hazard avoidance (A)

[11] This implies that reusing experiences and sources such as preliminary hazard lists from previous projects have to be subject to reassessment and re-classification even if the context and functionality remains the same as for previous analyses

measures, techniques and recommendations in safety standards may be followed. For the other cases the risk reduction process needs to consider if the risk can be reduced according to a safety standard or according to a security standard, or with a combination of both safety and security standards. Note however that in order to be able to certify the product, the development and maintenance process steps required in the safety standard must be followed in all cases when implementing mitigations even if the mitigation comes from a security standard.

Reference system – Case study

To validate our proposed approach we have studied a system for material transportation in a mining environment provided by the PiiA-WROOM [12] project. The system is currently under development and will comprise a set of vehicles that cooperate to transport material in an underground mine. A novel characteristic of the system is that some vehicles can be manually or remotely driven during operation. When remotely driven, an operator in a control room above ground controls the vehicle via wired and wireless networks. An advantage is that when there are still hazardous dust and gases remaining after blasting in the mine, the vehicles can be operated remotely from above ground and begin transporting material before it is safe for humans to be present in the mine. These types of systems, with remote controlled or partially autonomous vehicles, are believed to become a common setup in mines.

We studied the system setup and performed a preliminary hazard analysis according to the IEC62061 safety standard. Typically, these types of systems are analyzed and certified in a modular way, meaning that each vehicle or piece of equipment is analyzed for risks, developed and certified in isolation without considering security threats. To test our method we extended the system definition and performed an extended hazard analysis including security threats from intentional and accidental misuse of the system. We managed, quite easily, to identify new unforeseen safety hazards, and additional ways in which a system might enter a hazardous state. These hazards and the events leading to them would not have been found with a traditional safety approach, i.e., these hazards were not found when using the original scope of the IEC62061 system definition and hazards analysis, since the root causes were not considered to be failures.

The exercise clearly shows that interconnected systems, in this case a system-of-systems, lead to additional hazards when security is considered. The risk classification was done according to the IEC62061 and the security related hazards were also given SIL (safety integrity level) classifications. This allowed us to prioritize the risks and to propose suitable mitigations. Mitigation and countermeasures were chosen from the safety and security domains.

Using this new approach, which in essence is harmonized with IEC62061, allows us to develop, and according to IEC62016, certify a complex interconnected system-of-systems subject to security threats.

[12] http://www.projdb.processitinnovations.se/Aktivitet.aspx?id=219

Conclusion/ Summary

We have investigated existing functional safety standards and identified critical shortcomings when they are applied to networked systems: they do not consider security threats that may lead to accidents. Likewise, security standards do not cover safety aspects to the same rigor as the safety standards.

To remedy this, we propose an approach that considers security threats in the safety work process. The approach can be seen as an initial step towards an integrated approach for safety and security, something that will be needed for keeping risks of accidents and incidents in future networked cooperating products at acceptable levels.

We applied our approach to the IEC62061 functional safety standard in a case study that clearly shows that we systematically can identify additional hazards stemming from security threats that would not have been identified using a traditional safety approach. Since the hazard analysis process is harmonized with the IEC62061 standard we believe that it is now possible to develop and certify complex interconnected system-of-systems according to IEC62016, taking security threats into account. Our approach is general and can be applied also to other standards.

References

[1] A. Burns, J. McDermid, J. Dobson, *On the Meaning of Safety and Security*, Oxford Journals Science & Mathematics Computer Journal, Volume 35, Issue 1, 1991

[2] D. Brewer, *Applying Security Techniques to Achieving Safety*, Directions in Safety-Critical Systems, 1993

[3] V. Stavridou, B. Dutertre, *From security to safety and back*. Proceedings of the computer security, dependability and assurance: from needs to solutions, 1998

[4] A. Simpson, J. Woodcock, J Davies, *Safety through security*, Proceedings of the 9th international workshop on software specification and design, Washington DC, USA, 1998

[5] D. P. Eames, J. Moffett, *The integration of safety and security requirements*, Proceedings of the 18th international conference on Computer Safety, Reliability and Security (SAFECOMP), Toulouse, France, Sept, 1999

[6] R. Winther, O-A. Johnsen, B. Gran, *Security Assessments of Safety Critical Systems Using HAZOPs*, Proceedings of the 20th international conference on Computer Safety, Reliability and Security (SAFECOMP), Budapest, Hungary, Sept, 2001

[7] J. Smith, S. Russell, M. Looi, *Security as a Safety Issue in Rail Communications*, Proceedings of the 8th Australian workshop on Safety critical systems and software, SCS, 2003

[8] T. Srivatanakul, J. A. Clark, F Polack, *Effective Security Requirements Analysis: HAZOP and Use Cases*, Information Security Volume 3225 of the series Lecture Notes in Computer Science, 2004

[9] S. Lautieri, D. Cooper, D. Jackson, *Safsec: commonalities between safety and security assurance*, Proceedings of the 13th Safety Critical Systems Symposium, Southampton, UK, 2005

[10] S. Zafar, RG. Dromey, *Integrating safety and security requirements into design of an embedded system*, Proceedings of 12th Asia-Pacific software engineering conference, APSEC, Taipei, Taiwai, 2005

[11] G. Stoneburner, *Toward a unified security-safety model*, Computer, Vol.39, 2006

[12] T. Aven, *A unified framework for risk and vulnerability analysis covering both safety and security*, Reliability Engineering & System Safety, Volume 92, Issue 6, 2007

[13] TJ. Cockram, SR. Lautieri, *Combining security and safety principles in practice*, Proceedings of the 2nd international conference on institution of engineering and technology system safety, London, UK, 2007

[14] T. Novak, A. Treytl, P. Palensky, *Common approach to functional safety and system security in building automation and control systems*. Proceedings of the 12th conference on emerging technologies and factory automation (ETFA), Patras, Greece, September, 2007

[15] T. Novak, A. Treytl, A. Gerstinger, *Embedded security in safety critical automation systems*, Proceedings of the 26th international system safety conference (ISSC 2008), Vancouver, Canada, 2008

[16] Novak T, Treytl A. Functional safety and system security in automation systems–a life cycle model. In: Proceedings of the IEEE international conference on emerging technologies and factory automation, ETFA; 2008.

[17] B. Hunter, *Integrating Safety and Security Into the System Lifecycle*, Improving Systems and Software Engineering Conference (ISSEC), Canberra, Australia, August, 2009

[18] I. Nai Fovino, M. Masera, A. De Cian, *Integrating cyber attacks within fault trees*, Journal of Reliability Engineering and System Safety, Volume 94, Issue 9, 2009

[19] M. Sun, S. Mohan, L. Sha, C. Gunter, *Addressing safety and security contradictions in cyber-physical systems*, Proceedings of the 1st workshop on future directions in cyber-physical systems security (CPSSW09), Newark, NJ, USA, 2009

[20] T. Novak, A. Gerstinger, *Safety- and Security-Critical Services in Building Automation and Control Systems*, Transactions on Industrial Electronics, Volume: 57, Issue 11, 2010

[21] A.J. Kornecki, J. Zalewski, *Safety and security in industrial control*, Proceedings of the 6th Annual Workshop on Cyber Security and Information Intelligence Research, CSIIRW, Oak Ridge, USA, 2010

[22] A. Derock, *Convergence of the latest standards addressing safety and security for information technology*, On-line proceedings of embedded real time software and systems (ERTS2), Toulouse, France, 2010

[23] H. Li, Y. Wang, J. Han, C. Luo, *The merging trend of software security and safety*, International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), Xi'an, China, 2011
[24] C. Raspotnig, P. Karpati, V. Katta, *Enterprise, A Combined Process for Elicitation and Analysis of Safety and Security Requirements*, Business-Process and Information Systems Modeling Volume 113 of the series Lecture Notes in Business Information Processing, 2012
[25] S. Sadvandi, N. Chapon, L. Pièrre-Cambacédès, *Safety and Security Interdependencies in Complex Systems and SoS: Challenges and Perspectives*, Proceedings of the 2nd International Conference on Complex Systems Design & Management, 2011
[26] C.W Johnson, *CyberSafety: On the Interactions between Cyber Security and the Software Engineering of Safety-Critical Systems*, Proceedings of the 20th Safety-Critical Systems Symposium, Bristol, UK, February, 2012
[27] P. Bieber, J-P. Onera, A. Blanquart, G. Descargues, M. Thales, S. Dulucq, *Security and safety assurance for aerospace Embedded Systems*, Proceedings of the 6th international conference on embedded real time software and systems (ERTS2), Toulouse, France; 2012
[28] S.O. Johnsen, *Resilience at interfaces: Improvement of safety and security in distributed control systems by web of influence*, Information Management and Computer Security, Volume 20, Issue 2, 2012
[29] F. Reichenbach, J. Endresen, MMR. Chowdhury, J. Rossebo, *A pragmatic approach on combined safety and security risk analysis*. Proceedings of the 23rd international symposium on software reliability engineering workshops (ISSREW), Dallas, USA, 2012.
[30] R. Bloomfield, K. Netkachova, R. Stroud, *Security-informed safety: if it's not secure, it's not safe*. Software Engineering for Resilient Systems, Volume 8166 of the series Lecture Notes in Computer Science, 2013
[31] L. Pietre-Cambacedes, M. Bouissou, *Cross-fertilization between safety and security engineering*, Reliability Engineering & System Safety, Volume 110, February, 2013
[32] S. Bezzateev, N. Voloshina, P. Sankin, *Joint Safety and Security Analysis for Complex Systems*, Proceedings of the 13th conference of FRUCT association, Petrozavodsk, Russia, April, 2013
[33] C. Raspotniga, A. Opdahla, *Comparing risk identification techniques for safety and security requirements*, Journal of Systems and Software Volume 86, Issue 4, 2013
[34] C. Raspotnig, V. Katta, P. Karpati, A.L. Opdahl, *Enhancing CHASSIS: A Method for Combining Safety and Security*, Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES), Regensburg, Germany, Sept. 2013,
[35] N. Silva, R. Lopes, *Practical Experiences with real-world systems: Security in the World of Reliable and Safe Systems*, Proceedings of the 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Budapest, Hungary, June, 2013
[36] N. Subramanian, J. Zalewski, *Assessment of safety and security of system architectures for cyberphysical systems*, Proceedings of the 7th international systems conference (SysCon), Orlando, USA, 2013
[37] M. Steiner, P. Liggesmeyer, *Combination of safety and security analysis- finding security problems that threaten the safety of a system*, Proceedings of the DECS workshop at the 32nd international conference on computer safety, reliability and security (Safecomp), Toulouse, France, 2013
[38] AJ. Kornecki, N. Subramanian, J. Zalewski, *Studying interrelationships of safety and security for software assurance in cyber-physical systems: approach based on Bayesian belief networks*, Proceedings of the federated conference on computer science and information systems (FedCSIS), Krakow, Poland, September, 2013
[39] W. Young, NG. Leveson, *Systems thinking for safety and security*, Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC), New York, NY, USA, 2013
[40] N. Nostro, A. Bondavalli, N. Silva, *Adding Security Concerns to Safety Critical Certification*, International Symposium on Software Reliability Engineering Workshops (ISSREW), Naples, Italy, November, 2014
[41] V. Kharchenko, O. Illiashenko, A. Kovalenko, V. Sklyar, A. Boyarchuk, *Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique*, Proceedings of the 22nd International Conference on Nuclear Engineering, Prague, Czech Republic, 2014
[42] B. Malinowsky, H-P. Schwefel, O. Jung, *Quantitative safety and security analysis from a*

communication perspective, Proceedings of the 8th International Conference on Performance Evaluation Methodologies and Tools, Bratislava, Slovakia, 2014
[43] M. Ito, *Finding Threats with Hazards in the Concept Phase of Product Development*, Systems, Software and Services Process Improvement, Volume 425 of the series Communications in Computer and Information Science, 2014
[44] J. Fruth, E. Nett, *Uniform Approach of Risk Communication in Distributed IT Environments Combining Safety and Security Aspects*, Integration of safety and security engineering workshop (ISSE), Florence, Italy, September, 2014
[45] G. Sabaliauskaite, A. Mathur, *Aligning Cyber-Physical System Safety and Security*, Proceedings of the 1st Asia - Pacific Conference on Complex Systems Design & Management, CSD&M Asia, Singapore, 2014
[46] C. Woskowski, *A Pragmatic Approach towards Safe and Secure Medical Device Integration*, Computer Safety, Reliability, and Security, Volume 8666 of the series Lecture Notes in Computer Science, 2014
[47] W. Young, NG. Leveson, *An integrated approach to safety and security based on systems theory*. Communications of the ACM, Volume 57, Issue 2, 2014
[48] K. Netkachova, K. Müller, M. Paulitsch, R. Bloomfield, *Investigation into a layered approach to architecting security informed safety*, Proceedings of the 34th Digital Avionics Systems Conference (DASC), Prague, Czech Republic, September, 2015
[49] G. Macher, A. Holler, H. Sporer, E. Armengaud, C. Kreiner, *A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems*, Computer Safety, Reliability, and Security, Volume 9338 of the series Lecture Notes in Computer Science, 2015
[50] J. Draeger, *Roadmap to a Unified Treatmap of Safety and Security*, Proceedings of the 10th IET System Safety and Cyber-Security Conference, Bristol, UK, 2015
[51] K. Netkachova, K. Müller, M. Paulitsch, R. Bloomfield, *Security Informed Safety Case Approach to Analysing MILS Systems*, The International Workshop on MILS: Architecture and Assurance for Secure Systems, Amsterdam, The Netherlands, January, 2015
[52] D. Iacono, F. Brancati, F. Rossi, A. Bondavalli, *Thinking outside the vehicle: the impact of connected vehicles on safety and security*, Proceedings of the 45th International Conference on Dependable Systems and Networks (DSN), Rio de Janeiro, Brazil, 2015
[53] T. Gu, M. Lu, L. Li, *Extracting interdependent requirements and resolving conflicted requirements of safety and security for industrial control systems*, 1st International Conference on Reliability Systems Engineering (ICRSE), Beijing, China, 2015
[54] S. Paul, *On the Meaning of Security for Safety (S4S)*, The 6th International Conference on Safety and Security Engineering (SAFE), Opatija, Croatia, 2015
[55] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, Y. Halgand, *A survey of approaches combining safety and security for industrial control systems*, Reliability Engineering and System Safety, Volume 139, 2015
[56] C. Schmittner, Z. Ma, *Towards a Framework for Alignment Between Automotive Safety and Security Standards*, Computer Safety, Reliability, and Security Volume 9338 of the series Lecture Notes in Computer Science, 2015
[57] A. Kornecki, J. Zalewski, *Aviation Software: Safety and Security*, Wiley Encyclopedia of Electrical and Electronics Engineering, Published Online: 16 March 2015
[58] N. Kuntze, C. Rudolph, *Security vs. Safety: Why do people die despite good safety?,* Integrated Communication, Navigation, and Surveillance Conference (ICNS), Herdon, USA, April, 2015
[59] G. Macher, A. Holler, H. Sporer, E. Armengaud, C. Kreiner, *A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems*, Integration of safety and security engineering workshop (ISSE), Delft, The Netherlands, September, 2015
[60] B. Chen, C. Schmittner, Z. Ma, W. Temple, X. Dong, D. Jones, W. Sanders, *Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective*, Integration of safety and security engineering workshop (ISSE), Delft, The Netherlands, September, 2015
[61] M. St John-Green, R. Piggin, J.A. McDermid, R. Oates, *Combined security and safety risk assessment: What needs to be done for ICS and the IoT*. In Proceedings of the IET System Safety and Cyber Security Conference, Bristol, 2015