Over 20 years of research into cybersecurity and safety engineering: a short bibliography

S. Paul & L. Rioux
Thales Research and Technology, France

Abstract

This paper provides a bibliography of research papers on safety and cybersecurity co-engineering since the early 90s. It only covers papers that address both safety and security architecting and/or engineering specialties explicitly and simultaneously.

Keywords: safety, cybersecurity, engineering.

1 Introduction

Safety and security are two risk-driven activities that are traditionally tackled separately. Since the 9/11 attacks on the Twin Towers and the discovery of the Stuxnet computer worm in June 2010, it is more and more recognised worldwide that both engineering specialties cannot continue to ignore each other.

It is evident that there are major opportunities to share on onomastics, algorithms, processes, (formal) methods and tools, in particular to reach higher levels of safety and security assurance at contained costs. Much work has already been done. This paper provides a snapshot bibliography in safety and cybersecurity co-engineering, going back to the early 90s, even if the majority of the papers are quite recent.

Safety and security are often considered as sub-factors of dependability (Laprie [1]), however the present state of the art covers dependability engineering publications only if both concerns are mentioned explicitly (Rushby [2]).

Our state of the art is organised as follows. A first group (cf. §2) comprehends the papers that state the issues related to engineering safety and cybersecurity separately, and assert that there is room for improvement, but do not explain how. The second group (cf. §3) comprehends the papers that propose to extend

WIT Transactions on The Built Environment, Vol 151, © 2015 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE150291

the scope of safety engineering by adapting cybersecurity-related techniques. The third group (cf. §4) comprehends the papers that propose to improve cybersecurity engineering by adapting safety-related techniques. With respect to the second and third groups our paper complements the recent state of the art by Pièrre-Cambacedes and Bouissou [3]. The fourth group (cf. §5) of publications advocates clean slate approaches for safety and cybersecurity co-engineering.

2 Houston, we have a problem!

A number of papers explicitly state the issues related to engineering safety without security, or engineering safety and security separately, and assert that there is room for improvement, but they do not explain how, e.g. Pfitzmann [4], Nordland [5], Gerhold [6], Schwarz [7], Wiander [8]. Many of these papers are domain specific, e.g. ICAO [9], Deleuze *et al*. [10], Bloomfield *et al.* [11], Gebauer [12], 79 FR 60574 [13], or Vogt [14].

Beyond just expressing the issues, some papers also provide high-level recommendations on the manner to address them or on the directions to investigate, but they do not run that road themselves, e.g. Daniel [15], Carter [16], Eames and Moffett [17], Smith *et al*. [18], Dewar [19], Saglietti [20] and Goertzel and Feldman [21].

Running a bit against the current, Hansen [22] recalls that even though safe systems were not designed to be secure, they often offer good properties against attacks, with a tendency to fail-safe.

3 Improving safety engineering with security considerations

Safety engineering traditionally excludes malevolent behaviour. This is usually an implicit assumption, but it is (or was) sometimes explicitly stated. Attacks on safety-critical systems have recently changed the game. The safety engineering community is addressing the issue by elaborating new techniques and standards, e.g. S+IEC 61508 [23], to seamlessly cope with cybersecurity threats that can have an impact, direct or indirect, on safety. It is possible to organise these new techniques in two sets.

The first set consists of established safety-related techniques that are enhanced to also cope with some security issues within a safety engineering process, e.g. Winther *et al*. [24], Winther [25], Yang and Yang [26], Cusimano and Byres [27], Schmittner *et al*. [28, 29], Gorbenko *et al*. [30], Babeshko *et al*. [31], Bezzateev *et al*. [32] and Bieber and Brunel [33].

The second set consists of security-related techniques that are adapted to enhance safety engineering, e.g. Johnson [34], Sindre [35], Stålhane and Sindre [36], Raspotnig ansd Opdahl [37] and McGuire [38].

Security specification is sometimes defined as the specification of what the system should not do, i.e. negative properties, e.g. non-interference in multi-level security. But negative properties are not an exclusivity of security. Such security for safety approaches are proposed by Rushby [39] and Simpson *et al*. [40].

If the major part of the paper contributions relates to adaptations, there are also some novel and/or disruptive approaches, e.g. Sommerville [41], Olive *et al*. [42], Knorreck and Apvrille [43], Pedroza *et al*. [44], Apvrille and Roudier [45] and Brunel *et al*. [46, 47].

Beyond the aforementioned focused techniques, there are various initiatives of the safety community which address the issue in a more comprehensive manner, in particular with respect to standards, e.g. SEISES [48], Bieber *et al*. [49], Paulitsch *et al*. [50], MODSafe [51], Bock *et al*. [52] and Goertzel *et al*. [53]. We can distinguish two categories of initiatives. The first category defines new approaches that include security aspects whist maintaining compliance to existing standards. The second category defines new standards, or new versions of standards, that natively include security aspects.

Initiatives of the first category usually consist in analysing the gaps and overlaps between two (or more) existing standards in order to identify additional activities that need to be performed with respect to one standard used as baseline, in order to achieve dual compliance, e.g., Corneillie *et al*. [54], Alves-Foss *et al*. [55], Taylor *et al*. [56, 57], Novak *et al*. [58], Ridgway [59], Derock *et al*. [60], Blanquart *et al*. [61] and Czerny [62].

Initiatives of the second category are essentially domain-specific, e.g. ED-202 [63], ED-202A [64] as discussed in Casals *et al*. [65], Rowe [66], Joyce and Fabre [67], and EN 20159 [68], or S+IEC 61508 [23] as discussed in McGuire [38] and Schoitsch [69].

4 Improving security engineering with safety techniques

Safety engineering is recognised as a more mature engineering speciality than security engineering. Thus, multiple authors propose to adapt safety engineering techniques to the security domain. Most approaches are technical, but there are a few exceptions, e.g. Brostoff and Sasse [70], Fruth and Nett [71] and Gutgarts and Temin [72].

Papers describing focused technical approaches include Lynch [73], Foster [74], Lano *et al*. [75], Srivatanakul *et al*. [76], Daruwala *et al*. [77], Helmer *et al*. [78], Brooke and Paige [79], Murdoch *et al*. [80], Nicol *et al*. [81] and Rushdi and Ba-Rukab [82, 83].

Beyond specific techniques, some papers have a more comprehensive approach by adapting the overall good practices and lessons learnt of safety engineering to security engineering, e.g. Axelrod [84] and Young and Leveson [85].

5 Towards safety and security co-engineering

Amongst the first communities to address the relations between safety and security was the formal methods community, with the challenge of formalising the concepts, the mechanisms employed to safeguard them, and their interplay, e.g. Rushby [2, 39], Burns *et al*. [86], Stavridou and Dutertre [87], Ramirez *et al*. [88]. This community is still very active, e.g. Boettcher *et al*. [89], EURO-MILS

[90], Müller *et al*. [91], Tverdyshev [92], Fisher [93] and Tiwari *et al*. [94] in the scope of DARPA I2O HACMS [95] and Delange [96]. A comprehensive review of Formal Methods for Safe and Secure Computers Systems is given by Garavel and Graf [97].

Some studies are less formal, but have the similar goals of better understanding the relations between safety and security, e.g. Piètre-Cambacédès and Chaudet [98], and establishing a common information model for safety and security, e.g. Avizienis *et al*. [99], Jonsson [100], Jonsson and Olovsson [101], Stoneburner [102], Firesmith [103, 104], Mattila [105], Burns *et al*. [86] and Piètre-Cambacédès and Chaudet [98]. A compromise between formal and non-formal approaches is proposed by Chapon and Piètre-Cambacédès [106] and Sadvandi *et al*. [107].

Unifying focused engineering techniques used in safety and security is often recommended, e.g. by Lano *et al*. [75], Fovino *et al.* [108], Förster *et al.* [109], Steiner and Liggesmeyer [110], Piètre-Cambacédès and Bouissou [111] and Reichenbach *et al.* [112]. Except for Raspotnig and Opdahl [113], few papers however propose a framework to justify why specific attention is given this or that technique.

Even if a unification or harmonisation of the safety and security engineering approaches is commonly proposed, disruptive focused techniques are also proposed, e.g. Sallhammar *et al.* [114], Aven [115], Kornecki *et al.* [116] and Vouk [117].

Beyond the aforementioned focused techniques, there are various proposals for an overall unification, e.g. the MAFTIA project [118], Hessami [119], SafSec [120], Jackson and Dobbing [121], Ibrahim *et al.* [122], Firesmith [103], Raspotnig and Opdahl [37], Raspotnig *et al*. [123], and Raspotnig [124], Katta *et al*. [125], Pedroza *et al*. [44], Sadvandi *et al*. [107], Aoyama and Koike [126], Axelrod [127–129], Schoitsch [130], Line *et al*. [131], Aven [132, 133], Förster *et al*. [109], Aoyama *et al*. [126], Banerjee *et al*. [134] and the SeSaMo project [135] as discussed in Mazzini *et al*. [136] and Favaro and Stroud [137].

It is difficult to assess which unified approach will emerge as we believe that the ultimate approach to co-engineering has not yet been found, cf. Kriaa *et al*. [138].

Unification initiatives can also be found in standards, e.g. ISO 31000 [139], IEC 31010 [140], ISO/IEC 15026-2 [141] OMG SACM [142]. In domains in which compliance to standards is of utmost importance, generic co-engineering approaches and technical solutions as presented above are rarely helpful, especially when one starts searching for the devil in the details, cf. Åkerberg [143] and Braband [144, 145].

Of course, when both safety and security concerns are addressed for a giving system, striking the proper balance between these two, sometimes contradictory, sets of requirements may be a challenge. Proposals are given by Nielson and Nielson [146] and Labreuche and Lehuédé [147], and further ones should be published in the scope of the MERgE project [148].

6 Future work

The ITEA2 MERgE project was launched at the end of 2012 to address the industrial challenges of efficiently and economically handling multi-concerns, with a particular focus on the co-engineering of the safety and security specialities. The research work presented here represents a snapshot of this collaborative work. A more comprehensive review of the safety and cybersecurity engineering state of the art will be provided soon in Paul *et al*. [149].

Acknowledgements

The research leading to these results has received funding from the European Union ITEA 2 Programme (Call 6) under grant no. 11011 (MERgE). The authors wish to acknowledge F. Vallée and A. Faucogney (ALL4TEC), T. Wiander (STUK) and J. Brunel (ONERA).

References

[1] J.-C. Laprie, Dependability: Basic Concepts and Terminology, vol. 5, Vienna: Springer, 1992, pp. 3–245.
[2] J. Rushby, "Critical properties: survey and taxonomy," Menlo Park, 1994.
[3] L. Piètre-Cambacedes and M. Bouissou, "Cross-fertilizations between safety and security engineering," *Reliability Engineering & System Safety,* vol. 110, pp. 110–126, 2013.
[4] A. Pfitzmann, "Why Safety and Security Should and Will Merge, Volume," in *Computer Safety, Reliability, and Security, Lecture Notes in Computer Science*, vol. 3219, 2004, pp. 1–2.
[5] O. Nordland, "Some Security Aspects in Safety-Related Systems," in *The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop*, 2008.
[6] L. Gerhold, "The Future of Research on Safety and Security in Germany – Results from an Explorative Delphi Study," in *Security in Futures – Security in Change, Proceedings of the Conference "Security in Futures – Security in Change", 3–4 June 2010, Turku, Finland*, B. Auffermann and J. Kaskinen, Eds., 2011.
[7] R. Schwarz, "My thoughts on safety and security metrics," in *1st IESE Workshop on Safety and Security*, Kaiserslautern, 2014.
[8] T. Wiander, "Positive and Negative Findings of the ISO/IEC 17799 Framework," in *Proceedings of the 18th Australasian Conference on Information Systems (ACIS)*, Toowoomba, 2007.
[9] ICAO, "Study on the Safety and Security Aspects of Economic Liberalization," International Civil Aviation Organization, 2005.
[10] G. Deleuze, E. Chatelet, P. Laclemence, J. Piwowar and B. Affeltranger, "Are safety and security in industrial systems antagonistic or

complementary issues?," in *17th European safety and reliability conference (ESREL)*, Valencia, CRC Press, 2009, pp. 3093–3100.
[11] R. Bloomfield, R. Bloomfield, I. Gashi and R. Stroud, "How secure is ERTMS?," in *Workshop on Dependable and Secure Computing for Large-scale Complex Critical Infrastructures (DESEC4LCCI)*, Herrenkrug, 2012.
[12] C. Gebauer, "Safety & security as drivers for future system development," in *1st Workshop on Safety & Security*, Kaiserslautern, 2014.
[13] 79 FR 60574, "Request for Comment on Automotive Request for Comment on Automotive Security," in *Federal Register Volume 79, Issue 194 (October 7, 2014)*, 194 ed., vol. 79, Office of the Federal Register, National Archives and Records Administration, 2014, pp. 60574–60583.
[14] R. Vogt, "Safety/security conflicts in large system architectures," in *1st Workshop on Safety and Security*, Kaiserslautern, 2014.
[15] H. Daniel, "Security in Safety Systems: the Need to Step beyond Traditional Engineering," in *The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop*, 2008.
[16] A.-L. Carter, "Safety-Critical versus Security-Critical Software," in *5th IET International Conference on System Safety*, Manchester, 2010.
[17] D. P. Eames and J. Moffett, "The Integration of Safety and Security Requirements," in *SAFECOMP '99 Proceedings of the 18th International Conference on Computer Computer Safety, Reliability and Security*, London, Springer-Verlag, 1999, pp. 468–480.
[18] J. Smith, S. Russell and M. Looi, "Security as a Safety Issue in Rail Communications," in *Proceedings of SCS'03, 8th Australian Workshop on Safety Critical Systems and Software, Canberra, October 9–10, 2003*, vol. 33, I. Australian Computer Society, Ed., ACM, 2003, pp. 79– 88.
[19] R. B. K. Dewar, "Safety and security: two sides of the same coin?," in *The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop*, 2008.
[20] F. Saglietti, "Common Analysis and Verification Techniques for Safety- and Security- Critical Software Systems," in *The Relationship between Safety & Security in Software-Based Systems, SafeComp Workshop*, 2008.
[21] M. K. Goertzel and L. Feldman, "Software Survivability: Where Safety and Security Converge," in *Proceedings of the AIAA Infotech@Aerospace Conference*, Seattle, 2009.
[22] K. Hansen, "Security attack analysis of safety systems," in *Proceedings of IEEE Conference on Emerging Technologies & Factory Automation (ETFA)*, Mallorca, 2009, pp. 1–4.
[23] S+IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission, 2010.
[24] R. Winther, O.-A. Johnsen and B. A. Gran, "Security assessments of safety critical systems using HAZOPs," in *SafeComp'01 Proceedings of the 20th International Conference on Computer Safety, Reliability and Security*, Springer-Verlag, Ed., London, 2001, pp. 14–24.

[25] R. Winther, "Qualitative and Quantitative Analysis of Security in Safety and Reliability Critical Systems," in *Probabilistic Safety Assessment and Management*, vol. 6, C. S. .. U. Schmocker and V. N. Dang, Eds., London, Springer, 2004, pp. 2345–2351.
[26] L. Yang and S. H. Yang, "A Framework of Security and Safety Checking for Internet-Based Control Systems," *Int. J. Information and Computer Security,* vol. 1, no. 1/2, pp. 185–200, 2007.
[27] J. Cusimano and E. Byres, "Safety and Security: Two Sides of the Same Coin," April 2010. [Online]. Available: http://www.controlglobal.com/articles/2010/safetysecurity1004.
[28] C. Schmittner, T. Gruber, P. Puschner and E. Schoitsch, "Security Application of Failure Mode and Effect Analysis (FMEA)," in *33rd International Conference on Computer Safety, Reliability and Security (SafeComp)*, Florence, 2014b.
[29] C. Schmittner, Z. Ma and P. Smith, "FMVEA for Safety and Security Analysis," in *1st International Workshop on the Integration of Safety and Security Engineering (ISSE), 33rd International Conference on Computer Safety, Reliability and Security (SafeComp)*, Florence, 2014a.
[30] A. Gorbenko, V. Kharchenko, O. Tarasyuk and A. Furmanov, "F(I)MEA-technique of Web Services Analysis and Dependability Ensuring," in *Rigorous Development of Complex Fault-Tolerant Systems, Lecture Notes in Computer Science*, vol. 4157, M. Butler, C. B. Jones, A. Romanovsky and E. Troubitsyna, Eds., Berlin Heidelberg, Springer, 2006, pp. 153–167.
[31] E. Babeshko, V. Kharchenko and A. Gorbenko, "Applying F(I)MEA-technique for SCADA-Based Industrial Control Systems Dependability Assessment and Ensuring," in *Third International Conference on Dependability of Computer Systems*, Szklarska Poreba, 2008.
[32] S. Bezzateev, N. Voloshina and P. Sankin, "Joint Safety and Security Analysis for Complex Systems," in *13th Conference of Open Innovations Association FRUCT*, Petrozavodsk, Russia, 2013.
[33] P. Bieber and J. Brunel, "From Safety Models to Security Models: Preliminary Lessons Learnt," in *1st International Workshop on the Integration of Safety and Security Engineering (ISSE)*, Florence, 2014.
[34] R. G. Johnson, "Adversarial safety analysis: borrowing the methods of security vulnerability assessments," *Journal of Safety Research,* vol. 35, no. 3, pp. 245–248, 2004.
[35] G. Sindre, "A look at misuse cases for safety concerns," in *Situational Method Engineering: Fundamentals and Experiences*, vol. 244, S. Boston, Ed., IFIP, 2007, pp. 252–266.
[36] T. Stålhane and G. Sindre, "Safety Hazard Identification by Misuse Cases: Experimental Comparison of Text and Diagrams," in *Model Driven Engineering Languages and Systems, Lecture Notes in Computer Science*, vol. 5301, Springer Berlin Heidelberg, 2008, pp. 721–735.
[37] C. Raspotnig and A. L. Opdahl, "Improving security and safety modelling with failure sequence diagrams," in *International Journal of Secure Software Engineering (IJSSE)*, 2012a, pp. 20–36.

[38] N. McGuire, "Utilizing security methods of FLOSS GPOS for safety," in *Embedded World Exhibition & Conference*, Nürnberg, 2011.
[39] J. Rushby, "Kernels for Safety?," in *Safe and Secure Computing Systems*, Blackwell Scientific Publications, 1989, pp. 210–220.
[40] A. Simpson, J. Woodcock and J. Davies, "Safety through Security," in *IWSSD'98 Proceedings of the 9th international workshop on Software specification and design*, I. C. Society, Ed., Washington, 1998, pp. 18–24.
[41] I. Sommerville, "An Integrated Approach to Dependability Requirements Engineering," in *Current Issues in Safety-Critical Systems*, Springer, Ed., London, 2003, pp. 3–15.
[42] M. L. Olive, R. T. Oishi and S. Arentz, "Commercial Aircraft Information Security — An Overview of ARINC Report 811," in *25th Digital Avionics Systems Conference (DASC)*, Portland, 2006.
[43] D. Knorreck and L. Apvrille, "TEPE: A SysML Language for Time-Constrained Property Modeling and Formal Verification," in *Third IEEE International workshop UML and Formal Methods (UML&FM)*, Shanghai, 2010.
[44] G. Pedroza, L. Apvrille and D. Knorreck, "AVATAR: A SysML environment for the formal verification of safety and security properties," in *11th International Conference on New Technologies of Distributed Systems (NOTERE)*, Paris, 2011.
[45] L. Apvrille and Y. Roudier, "Towards the Model-Driven Engineering of Secure yet Safe Embedded Systems," in *Proceedings of 1st International Workshop on Graphical Models for Security (GraMSec)*, Grenoble, 2014.
[46] J. Brunel, L. Rioux, S. Paul, A. Faucogney and F. Vallée, "Formal Safety and Security Assessment of an Avionic Architecture with Alloy," in *3rd International Workshop on Engineering Safety and Security Systems (ESSS)*, vol. 150, Singapore, EPTCS, 2014a, pp. 8–19.
[47] J. Brunel, D. Chemouil, L. Rioux, M. Bakkali and F. Vallée, "A Viewpoint-Based Approach for Formal Safety & Security Assessment of System Architectures," in *11th Workshop on Model Driven Engineering, Verification and Validation (MoDeVVa)*, Valencia, 2014b.
[48] SEISES, "Cooperative Projects," FUI, 2008. [Online]. Available: http://www.aerospace-valley.com/les-projets?keywords=seises.
[49] P. Bieber, J.-P. Blanquart, G. Descargues, M. Dulucq, Y. Fourastier, E. Hazane, M. Julien, L. Léonardon and G. Sarouille, "Security and Safety Assurance for Aerospace Embedded Systems," in *Embedded Real-Time Software and Systems (ERTS)*, Toulouse, 2012.
[50] M. Paulitsch, R. Reiger, L. Strigini et R. E. Bloomfield, "Evidence-Based Security in Aerospace: From Safety to Security and Back Again", chez *IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 2012.
[51] MODSafe, "Modular Urban Transport Safety and Security Analysis," EU FP7, 01 09 2008. [Online]. Available: http://www.modsafe.eu/.
[52] H.-H. Bock, J. Braband, B. Milius and H. Schäbe, "Towards an IT Security Protection Profile for Safety-Related Communication in Railway

Automation," in *31st International Conference on Computer Safety, Reliability and Security (SafeComp)*, Magdeburg, 2012.

[53] K. M. Goertzel, T. Winograd and B. A. Hamilton, "Safety and Security Considerations for Component-Based Engineering of Software-Intensive Systems," Navy Software Process Improvement Initiative (SPII) and Department of Homeland Security, 2011.

[54] P. Corneillie, S. Moreau, C. Valentin, J. Goodson, A. Hawes, T. Manning, H. Kurth, G. Liebisch, A. Steinacker, Y. Deswarte, M. Kaaniche and P. Benoit, "SQUALE Dependability Assessment Criteria," LAAS-CNRS, 1999.

[55] J. Alves-Foss, B. Rinker and C. Taylor, "Towards Common Criteria Certification for DO-178B Compliant Airborne Software Systems, Comparing Evaluation Assurance Level 5 (EAL5) to DO178," Center for Secure and Dependable Systems, 01 2002. [Online]. Available: http://www2.cs.uidaho.edu/~jimaf/papers/compare02b.pdf.

[56] C. Taylor, J. Alves-Foss and B. Rinker, "Towards Common Criteria Certification for DO-178B: Executive Summary," Center for Secure and Dependable Systems, 03 2002a. [Online]. Available: http://www2.cs.uidaho.edu/~jimaf/papers/compare02a.pdf.

[57] C. Taylor, J. Alves-Foss and B. Rinker, "Merging Safety and Assurance: the Process of Dual Certification of Software," in *Software Technology Conference*, 2002.

[58] T. Novak, A. Treytl and P. Palensky, "Common Approach to Functional Safety and System Security in Building Automation and Control Systems," in *Proceedings of Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, 2007, pp. 1141–1148.

[59] J. Ridgway, "Achieving Safety through Security Management," in *The Safety of Systems*, London, Springer, 2007.

[60] A. Derock, P. Hebrard and F. Vallée, "Convergence of the latest standards addressing safety and security for information technology," in *On-line proceedings of Embedded Real Time Software and Systems (ERTS2 2010)*, Toulouse, France, 2010.

[61] J.-P. Blanquart, P. Bieber, G. Descargues, E. Hazane, M. Julien and L. Léonardon, "Similarities and dissimilarities between safety levels and security levels," 03 02 2012. [Online]. Available: http://www.erts2012.org /Default.aspx?Id=1050&Idd=1129.

[62] B. J. Czerny, "System Security and System Safety Engineering: Differences and Similarities and a System Security Engineering Process Based on the ISO 26262 Process Framework," *Journal of Passenger Cars – Electronic and Electrical Systems,* vol. 6, no. 1, 2013.

[63] EUROCAE ED-202, "Airworthiness security process specification," European Organization for Civil Aviation Equipment (EUROCAE), 2010.

[64] EUROCAE ED-202A, "Airworthiness Security Process Specification," European Organization for Civil Aviation Equipment (EUROCAE), 2014.

[65] S. G. Casals, P. Owezarski and G. Descargues, "Risk Assessment for Airworthiness Security," in *Computer Safety, Reliability, and Security, Lecture Notes in Computer Science*, vol. 7612, 2012, pp. 25–36.
[66] J. Rowe, "Software Security & Design Assurance," in *Design & Manufacture Seminar*, 2013.
[67] J. Joyce and L. Fabre, "Integration of security & airworthiness in the context of certification and standardization," in *1st workshop on the Integration of Safety and Security Engineering (ISSE)*, Florence, 2014.
[68] CENELEC EN 20159, "Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems," European Committee for Electro-technical Standardization, 2010.
[69] E. Schoitsch, "Safety and security – what about a joint process?," in *1st Workshop on Safety & Security*, Kaiserslautern, 2014.
[70] S. Brostoff and M. A. Sasse, "Safe and sound: a safety-critical approach to security," in *NSPW'01 Proceedings of the 2001 workshop on new security paradigms*, ACM, Ed., New York, NY, 2001, pp. 41–50.
[71] J. Fruth and E. Nett, "Uniform Approach of Risk Communication in Distributed IT Environments Combining Safety and Security Aspects," in *1st International Workshop on the Integration of Safety and Security Engineering (ISSE), 33rd International Conference on Computer Safety, Reliability and Security (SafeComp)*, Florence, 2014.
[72] P. B. Gutgarts and A. Temin, "Security-Critical versus Safety-Critical Software," in *Proceedings of IEEE International Conference on Technologies for Homeland Security (HST)*, 2010.
[73] J. A. Lynch, "Applying Safety Critical Systems Engineering Techniques to Secure Systems," 2002.
[74] N. L. Foster, "The application of software and safety engineering techniques to security protocol development," University of York, 2002.
[75] K. Lano, D. Clark and K. Androutsopoulos, "Safety and Security Analysis of Object-Oriented Models," in *Computerp. Safety, Reliability and Security – Proceedings of 21st International SAFECOMP Conference, Catania, Italy, September 10–13, 2002*, vol. 2434, S. B. Heidelberg, Ed., 2002, pp. 82–93.
[76] T. Srivatanakul, J. A. Clark and F. Polack, "Effective Security Requirements Analysis: HazOp and Use Cases," in *Information Security, Lecture Notes in Computer Science*, vol. 3225, Berlin/Heidelberg, Springer, 2004, pp. 416–427.
[77] B. Daruwala, S. Mandujano, N. K. Mangipudi and H.-c. Wong, "Threat Analysis for Hardware and Software Products Using HazOp," in *International Conference on Computational and Information Science (CIS'09)*, Stevens Point, Wisconsin: World Scientific and Engineering Academy and Society (WSEAS), 2009, pp. 446–453.
[78] G. Helmer, J. Wong, M. Slagell, V. Honavar, L. Miller and R. Lutz, "A Software Fault Tree Approach to Requirements Analysis of an Intrusion

Detection System," *Requirements Engineering,* vol. 7, no. 4, pp. 207–220, 2002.
[79] P. J. Brooke and R. F. Paige, "Fault trees for security system design and analysis," *Computers & Security,* vol. 22, no. 3, pp. 256–264, 2003.
[80] J. Murdoch, J. Allen, F. Anderson, M. Ashford, N. Bartol, M. Campbell, P. Caseley, V. Cocca, E. Fitzsimmons, P. Flora, J. Gaffney, G. Hafen, J. Janigan, J. Jarzombek, C. Jones, M. Kass and G. Larsen, "Security Measurement," Practical Software and Systems Measurement, 2006.
[81] D. M. Nicol, W. H. Sanders and K. S. Trivedi, "Model-based evaluation: from dependability to security," *IEEE Transactions on Dependable and Secure Computing,* vol. 1, no. 1, pp. 48–65, 2004.
[82] A. Rushdi and O. Ba-Rukab, "A doubly-stochastic fault-tree assessment of the probabilities of security breaches in computer systems," in *Proceedings of the 2nd Saudi Science Conference*, vol. 4, 2004, pp. 1–17.
[83] A. Rushdi and O. Ba-Rukab, "Fault-tree modelling of computer system security," *International Journal of Computer Mathematics,* vol. 82, pp. 805–819, 2005.
[84] C. W. Axelrod, "Applying Lessons from Safety-Critical Systems to Security-Critical Software," in *IEEE Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY, USA, 2011.
[85] W. Young and N. G. Leveson, "Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory," *Communications of the ACM,* vol. 57, no. 2, pp. 31–35, 2014.
[86] A. Burns, J. McDermid and J. Dobson, "On the meaning of safety and security," in *The Computer Journal – Special issue on safety and security parallel*, 1st ed., vol. 35, Oxford, Oxford University Press, 1992, pp. 3–15.
[87] V. Stavridou and B. Dutertre, "From Security to Safety and Back," in *Computer Security, Dependability and Assurance: From needs to Solutions. Proceedings*, IEEE, Ed., York, 1998, pp. 182–195.
[88] A. G. Ramirez, J. Schmaltz, F. Verbeek, B. Langenstein and H. Blasum, "On Two Models of Noninterference: Rushby and Greve, Wilding, and Vanfleet," in *33rd International International Conference on Computer Safety, Reliability, and Security (SAFECOMP)*, Florence, 2014.
[89] C. Boettcher, R. DeLong, J. Rushby and W. Sifre, "The MILS Component Integration Approach to Secure Information Sharing," in *Proceedings o fthe 27th IEEE/AIAA Digital Avionics Systems Conference (DASC)*, St. Paul, MN, 2008.
[90] EURO-MILS EC FP7 Project, "EURO-MILS," 01 10 2012. [Online]. Available: http://www.euromils.eu/. [Accessed 16 09 2014].
[91] K. Müller, M. Paulitsch, R. Schwarz, S. Tverdyshev and H. Blasum, "MILS-Based Information Flow Control in the Avionic Domain: a Case Study on Compositional Architecture and Verification," in *31st Digital Avionics Systems Conference (DASC)*, Williamsburg, 2012.
[92] S. Tverdyshev, "MILS – Architecture for Safety and Security," in *1st workshop on safety and security*, Kaiserslautern, 2014.

[93] K. Fisher, "High Assurance Cyber Military Systems (HACMS): Making sure you are in control of your vehicle," 2013.
[94] A. Tiwari, D. Jovanovic, P. Lincoln and D. Sadigh, "Safety Envelope for Security," in *3rd international conference on High Confidence Networked Systems (HiCoNS)*, Berlin, 2014.
[95] DARPA I2O HACMS, "High-Assurance Cyber Military Systems (HACMS)," DARPA, 06 11 2014. [Online]. Available: http://www.darpa.mil/opencatalog/HACMS.html. [Accessed 21 11 2014].
[96] J. Delange, "Security and dependability integration for the construction of critical middleware (in French)," TELECOM ParisTech, Paris, 2010.
[97] H. Garavel and S. Graf, "Formal Methods for Safe and Secure Computers Systems," Federal Office for Information Security, 2013.
[98] L. Piètre-Cambacédès and C. Chaudet, "Disentangling the relations between safety and security," in *AIC'09 Proceedings of the 9th WSEAS international conference on Applied informatics and communications*, Stevens Point, Wisconsin, 2009.
[99] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," in *IEEE Trans. Dependable Secur. Comput.*, 2004, pp. 11–33.
[100] E. Jonsson, "Towards an integrated conceptual model of security and dependability," in *First International Conference on Availability, Reliability and Security (ARES)*, 2006.
[101] E. Jonsson and T. Olovsson, "On the Integration of Security and Dependability in Computer Systems," in *International Conference on Reliability, Quality Control and Risk Assessment*, Washington DC, 1992.
[102] G. Stoneburner, "Toward a Unified Security-Safety Model," vol. 39, IEEE Computer, 2006, pp. 96–97.
[103] D. G. Firesmith, "Tutorial: Engineering safety- and security-related requirements for software-intensive systems," in *6th International Workshop on Software Engineering for Secure Systems (SESS'10) Workshop at the 32nd ICSE Conference*, Cape Town, South Africa, 2010.
[104] D. G. Firesmith, "Common concepts underlying safety, security, and survivability engineering," 2003.
[105] M. Mattila, "Different Views on Defining Safety, Security and Social Responsibility," *Interdisciplinary Studies Journal – Special Issue on Security, Safety and Social Responsibility,* vol. 3, no. 1, pp. 7–20, 2013.
[106] N. Chapon and L. Piètre-Cambacédès, "Vers une ingénierie système intégrant sûreté et sécurité (in French)," in *Génie Logiciel*, 100th ed., 2012, pp. 16–21.
[107] S. Sadvandi, N. Chapon and L. Piètre-Cambacédès, "Safety and Security Interdependencies in Complex Systems and SoS: Challenges and Perspectives," in *Complex Systems Design and Management (CSDM)*, Springer Berlin Heidelberg, 2012, pp. 229–241.
[108] I. N. Fovino, M. Masera and A. De Cian, "Integrating Cyber Attacks within Fault Trees," *Reliability Engineering and System Safety,* vol. 94, no. 9, pp. 1394–1402, 2009.

[109] M. Förster, R. Schwarz and M. Steiner, "Integration of modular safety and security models for the analysis of the impact of security on safety," Fraunhofer IESE, 2010.
[110] M. Steiner and P. Liggesmeyer, "Combination of Safety and Security Analysis – Finding Security Problems that Threaten the Safety of a System," in *ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems (DECS)*, 2013.
[111] L. Pièrre-Cambacédès and M. Bouissou, "Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes)," in *IEEE International Conference Systems Man and Cybernetics (SMC)*, Istanbul, 2010.
[112] F. Reichenbach, J. Endresen, M. M. R. Chowdhury and J. Rossebø, "A pragmatic approach on combined safety and security risk analysis," in *IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Dallas, IEEE, 2012, pp. 239–244.
[113] C. Raspotnig and A. L. Opdahl, "Comparing risk identification techniques for safety and security requirements," *Journal of Systems and Software,* vol. 86, no. 4, pp. 1124–1151, 2013a.
[114] K. Sallhammar, B. E. Helvik and S. J. Knapskog, "Towards a Stochastic Model for Integrated Security and Dependability Evaluation," in *1st International Conference on Availability, Reliability and Security*, Washington, 2006.
[115] T. Aven, "Identification of safety and security critical systems and activities," in *Reliability Engineering & System Safety*, 2009, pp. 404–411.
[116] A. J. Kornecki, N. Subramanian and J. Zalewski, "Studying Interrelationships of Safety and Security for Software Assurance in Cyber-Physical Systems: Approach Based on Bayesian Belief Networks," in *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Kraków, 2013.
[117] M. A. Vouk, "Differences and Similarities between Software Reliability and Software Security Engineering," in *Software Reliability in 2013: Theory & Practice*, Levallois-Perret, 2013.
[118] MAFTIA, "Malicious-and Accidental-Fault Tolerance for Internet Applications," IST MAFTIA Project n°11583, 01 01 2000. [Online]. Available: http://webhost.laas.fr/TSF/cabernet/maftia/.
[119] A. G. Hessami, "A systems framework for safety and security: The holistic paradigm", chez *Systems Engineering*, 2nd éd., vol. 7, Wiley Periodicals, 2004, pp. 99–112.
[120] Altran Praxis, "SafSec Methodology, Issue 3.1," 2006.
[121] D. Jackson and B. Dobbing, "Changing Regulation in Safety and Security – Implications and Opportunities," in *The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop*, 2008.
[122] L. Ibrahim, J. Jarzombek, M. Ashford, R. Bate, P. Croll, M. Horn, L. LaBruyere, C. Wells and al., "Safety and Security Extensions for Integrated Capability Maturity Models," 2004.

[123] C. Raspotnig, P. Karpati and V. Katta, "A Combined Process for Elicitation and Analysis of Safety and Security Requirements," in *Enterprise, Business-Process and Information Systems Modeling (EMMSAD), Lecture Notes in Business Information Processing*, vol. 113, Springer Berlin Heidelberg, 2012b, pp. 347–361.
[124] C. Raspotnig, "Requirements for safe and secure information systems," 2014.
[125] V. Katta, C. Raspotnig and T. Stålhane, "Requirements management in a combined process for safety and security assessments," in *8th International Conference on Availability, Reliability and Security (ARES)*, Regensburg, Germany, 2013a.
[126] T. Aoyama, M. Koike, I. Koshijima and Y. Hashimoto, "A unified framework for safety and security assessment in critical infrastructures," in *Safety and security engineering V*, vol. 134, F. Garzia, C. A. Brebbia and M. Guarascio, Eds., WIT Press, 2013.
[127] C. W. Axelrod, Engineering Safe and Secure Software Systems, Artech House Publishers, 2012.
[128] C. W. Axelrod, "Securing Cyber-Physical Software," 18–21 Nov. 2013b. [Online]. Available: http://2013.appsecusa.org/2013/wp-content/uploads/2013/12/APPSEC2013-Presentation-Final.ppt.
[129] C. W. Axelrod, "Managing the risks of cyber-physical systems," in *IEEE Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY: IEEE, 2013c, pp. 1–6.
[130] E. Schoitsch, "Design for safety and security of complex embedded systems: a unified approach," in *Cyberspace Security and Defense: Research Issues, NATO Science Series II: Mathematics, Physics and Chemistry*, vol. 196, Springer Netherlands, 2005, pp. 161–174.
[131] M. B. Line, O. Nordland, L. Rostad and I. A. Tondel, "Safety vs. Security?," in *International Conference on Probabilistic Safety Assessment and Management (PSAM 8)*, New Orleans, USA, 2006.
[132] T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security," in *Proceedings of Reliability Engineering & System Safety*, 2007, pp. 745–754.
[133] T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security," 4th ed., vol. 39, IEEE, 2011, pp. 123–134.
[134] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainabilityof Mission-Critical Cyber–Physical Systems," *IEEE Proceedings,* vol. 100, no. 1, pp. 283–299, 2012.
[135] SeSaMo, "Security and Safety Modelling," 2012. [Online]. Available: http://sesamo-project.eu/. [Accessed 20 05 2014].
[136] S. Mazzini, S. Mazzini, A. Martelli and L. Baracchi, "Security and Safety Modelling in Embedded Systems," in *Embedded Real Time Software and Systems (ERTS)*, Toulouse, 2014.

[137] J. Favaro and R. Stroud, "ARTEMIS SESAMO Project: Work Achieved and Perspectives," in *1st International Workshop on the Integration of Safety and Security Engineering (ISSE), 33rd International Conference on Computer Safety, Reliability and Security (SafeComp)*, Florence, 2014.
[138] S. Kriaa, C. Raspotnig, M. Bouissou, L. Pietre-Cambacedes, P. Karpati, Y. Halgand and V. Katta, "Comparing two approaches to safety and security modelling: BDMP technique and CHASSIS method," in *OECD Halden Reactor Project, 37th Enlarged Halden Programme Group (EHPG) meeting*, Storefjell, 2013.
[139] ISO 31000, "Risk management – Principles and guidelines," International Organization for Standardization, 2009.
[140] IEC 31010, "Risk management – Risk assessment techniques," International Electrotechnical Commission, 2009.
[141] ISO/IEC 15026-2, "Systems and software engineering – Systems and software assurance – Part 2: Assurance case," International Standards Organization/International Electrotechnical Commission, 2011.
[142] OMG SACM, "Structured Assurance Case Meta-model," 2 2013. [Online]. Available: http://www.omg.org/spec/SACM. [Accessed 23 05 2014].
[143] J. Åkerberg, "On Safe and Secure Communication in Process Automation," Mälardalen University Press Dissertations, Västerås (Sweden), 2011.
[144] J. Braband, "Towards an IT security protection profile for safety-related communication in railway automation," in *Embedded Real-Time Software and Systems (ERTS2)*, Toulouse, 2014a.
[145] J. Braband, "IT security for functional safety in railway automation," in *1st Workshop on Safety and Security*, Kaiserslautern, 2014b.
[146] H. R. Nielson and F. Nielson, "Safety versus Security in the Quality Calculus," in *Theories of Programming and Formal Methods, Lecture Notes in Computer Science*, vol. 8051, Springer, 2013, pp. 285–303.
[147] C. Labreuche and F. Lehuédé, "MYRIAD: a tool suite for MCDA," in *4th Conference of the European Society for Fuzzy Logic and Technology (EUSFLAT)*, Barcelona, 2005.
[148] MERgE, 2012. [Online]. Available: http://www.merge-project.eu/.
[149] S. Paul, L. Rioux, T. Wiander and F. Vallée, "Recommendations for security and safety co-engineering (v2)," ITEA2 MERgE project, 2015.