On the meaning of security for safety (S4S)

S. Paul
Thales Research and Technology, France

Abstract

Safety engineering traditionally leaves out malevolent behaviour. Recent attacks in safety-critical domains, e.g. 9/11, Stuxnet, have definitely changed the game. The academic safety engineering community is addressing the issue through a significant amount of publications and workshops. The industrial safety standardisation communities are addressing the issue by revisiting safety standards or elaborating new cybersecurity standards to seamlessly cope with IT security threats that can have an impact, direct or indirect, on safety. Regulation is also increasing. However, because the *security for safety* approach is not a simple juxtaposition of safety and cybersecurity processes and techniques, and despite all this hustle and bustle by academic and industrial communities, it is still very difficult to precisely define what is meant by *security for safety*. In this paper we analyse this would-be seamless integration of security engineering activities into the safety engineering world, and we discuss the areas in which a lot of fuzziness still remains.
Keywords: safety, cybersecurity, engineering.

1 Introduction

Safety engineering traditionally left out malevolent behaviour. Typically, the 1998 obsolete version of the Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems standard [1], clause 1.2.j stated that "this standard […] does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems." Recent attacks in safety-critical domains, e.g. 9/11 [2], Stuxnet [3], have changed the game. Typically, the 2010 version of the aforementioned standard [4] reads, in clause 1.2.l: "…requires malevolent and unauthorized actions to be considered during hazard and risk analysis and provides informative guidance on the

WIT Transactions on The Built Environment, Vol 151, © 2015 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE150321

security required for the achievement of functional safety". And indeed, since a couple of decades, multiple safety communities are actively addressing the safety and security co-engineering issue, considering that safety-critical systems may not be as safe as they claim, if they are not also secure.

The academic community has been publishing an impressive amount of papers on the subject of safety and security co-engineering since the early 90's [5], organising their conferences and workshops, discussing commonalities and differences, and showing that there is a significant overlap between both specialties [6]. States are financing large research and development projects on the topic, both in Europe [7–9], and across the Atlantic [10]. The industrial standardisation community is actively revisiting standards (e.g. ED-202 [11], S+IEC 61508 [4], IEC 62645 [12]) to better cope with IT security threats that can have an impact, direct or indirect, on safety-critical systems and/or infrastructures. Industries, large or small, have also invested and are starting to propose services [13, 14] and products [15, 16] on the market to make business out of this growing public concern.

Despite all this hustle and bustle, it is very difficult to precisely define what is meant by *security for safety*, beyond simply stating that safety must be ensured even in case (or in some cases) of malevolent behaviour.

The fuzziness exists at different levels. First, at process level: should safety and security processes be kept apart, simply harmonised or radically fused? The answer to this first question may help answer the following one at standardisation level: should the traditional and generic security standards (e.g. ISO/IEC 27001 [17], Common Criteria [18]) be used to ensure the security of safety-critical systems, or should domain-specific security standards be developed? Standardisation obviously brings to mind regulation, or rather the lack of regulation concerning the security of safety-critical systems and/or infrastructures. Finally, at a finer grain level, questions arise with respect to the (dependability) criteria to consider in *security for safety* studies, the need for security levels, and the use of qualitative versus quantitative approaches, the definition of metrics, etc.

This paper discusses some of these topics, with the aim of clarifying what can be expected under the terms *security for safety*.

2 Security-informed safety, or safety-informed security?

A good example of the fuzziness around *security for safety* is the question whether this approach leads to *security-informed safety* or on the contrary to *safety-informed security*.

Security-informed safety implies that the original safety processes and/or techniques are modified to cope with security concerns. Typical examples of this are, at process level, the obsolete ED-202 standard in which the security activities are embedded inside the safety process [19], or at technical level, an extended safety-case, as proposed in the SeSaMo project [20]. In this approach, safety experts are required to be sufficiently competent in cybersecurity to run their modified safety process and/or use their extended safety techniques to cover

relevant security concerns. Of course, security experts may be involved in the process, but then, it is them who must make the effort of understanding the safety-related jargon, techniques and processes. The work is highly collaborative, and both specialties must learn how to work together.

By contrast, *safety-informed security* implies that the security process is defined independently from the safety process, but that it is run using inputs coming from the safety process, limiting its scope of application to a frontier defined by safety experts. A typical example of this, at process level, is the new ED-202A standard [11], in which both safety and security processes interact as peers with the mainstream system engineering process [21]. At technical level, a typical example would be an attack tree analysis which would use for attack tree roots (a.k.a. attacker top-level goals or feared events) all the hazards resulting from the Functional Hazard Analysis (FHA) performed by safety experts, and nothing more. In this approach, safety experts are simply required to provide defined sets of data to security experts and the security experts can then work, more or less independently, according to their usual practices, in terms of standards, methods and tools. The negative side-effect of this approach are the possible resulting conflicts between the safety and security objectives; the difficulty is then not so much solving those conflicts, because the *safety-first* principle usually applies, but rather in identifying and consistently managing those conflicts, to avoid doing and undoing.

Based on the evolution of the ED-202 standard [11, 19], the aeronautical safety community seems to have opted for a *safety-informed security* approach, although, considering the discussions within the EUROCAE and RTCA standardisation groups, all individuals of that community do not seem to adhere. The executive summary of ED-202 even states that: "As an alternative, when considered practical, compliance may be accomplished through a blended process – documented by the applicant – that would integrate safety and security […]". Thus, it is difficult to state if this experience will set a trend in other domains, as the question seems to be as much political, as practical.

Our prognostic is that the safety communities will thrive to maintain their current safety organizational approaches as stable as possible, because safety standards, often used as acceptable means of compliance to regulation, have proven efficiency records, and are extremely difficult to change, technically and politically, especially considering the rate of occurrence of new types of cyber-attacks. Some minor updates to the safety standards may however be necessary to ensure interaction points, reduce overlaps and provide guidance for conflict management between the safety and security specialties. For example, in the space domain, section §5.3 of ECSS-Q-ST-40C [22] reads: "The implementation of safety requirements shall not be compromised by other requirements. NOTE *For example: security requirements*".

3 Towards domain-specific security standards?

The compartmentalised safety standardisation communities have created nearly as many safety standards as business domains. If, as discussed above, the trend

of *security for safety* is towards *safety-informed security*, then the traditional and generic security standards (e.g. ISO/IEC 27000 series [17, 23–25], Common Criteria [18, 26–28], NIST SP 800 series [29–31], NIST Cybersecurity Framework [32]) should have home court advantage to be selected to ensure the security of safety-critical systems. Initial publications do not confirm this hypothesis.

Indeed, the Nuclear Power Plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems [12] has been developed using the ISO/IEC 27000 series, IAEA and country specific guidance as sources of information, but in §1.1, this standard states that "Standards such as ISO/IEC 27001 and ISO/IEC 27002 are not directly applicable to the cyber-protection of nuclear I&C CB&HPD systems. This is mainly due to the specificities of these systems, including the regulatory and safety requirements inherent to nuclear facilities." The standard proceeds with a list of particular differentiators that justify a targeted security standard, all of which more or less related to the potential for much greater impact of a cyber-attack than that occurring at other industrial facilities.

Likewise, the aforementioned ED-202A aeronautical security standard [11] goes down the same pathway, with no qualms: it references the ISO/IEC 27k series as well as the NIST SP 800 framework, but fails to justify why the generic standards are not suited for securing aeronautical safety-critical systems.

In the automotive domain, the 10 parts Road Vehicles – Functional Safety Standard [33, 34] does not yet include security considerations. However, this point is becoming a hot topic, and the need for a new standard is frequently mentioned, e.g. in Czerny [35] and Gebauer [36].

Slightly more cross-domain, the new Industrial Communication Networks – Network and System Security series (IEC 62443) is a set of eleven documents currently elaborated by the International Society for Automation. The individual parts of the standard are at different stages of development, some being published [37–40], while others are still drafts. There currently is a German initiative to apply the IEC 62443 series to railway.

From the above, it can be seen that the safety standardisation communities seem keen to repeat their multiplication of domain-specific standards. One may ask if that will set the trend for the other domains. However, the key question remains why the traditional and generic security standards did not (yet) make it? Is the reason that the term *security* does not have quite the same meaning when used standalone, or when used in the *security for safety* expression? Or is it simply a question of appropriation of the security specialty by the safety community?

4 About regulation

A reason behind the fuzziness surrounding the elaboration of *security for safety* standards might be the lack of clear international regulation.

For example, in the aeronautical domain, aircraft type certification currently acts in the absence of comprehensive rules and guidance for how cyber-security

affects safety. The FAA and EASA use ad-hoc processes, typically in the form of Special Conditions to address specific security concerns for specific aircraft models, e.g. for the Boeing 787-8 [41, 42].

In Europe, in contrast with safety, security is a National sovereignty prerogative. Therefore, to our knowledge, there is no relevant transnational regulation. This makes life difficult for international standardisation bodies. It is interesting to see however that a number of industrial standards (as discussed above) are emerging, either in advance to the regulation, or in compliance to National regulations only, e.g. YVL A.12 [43] in the nuclear domain.

In the US, President Obama has very recently established that it is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties [44]. This Executive Order is at the origin of the creation of the NIST Cybersecurity Framework [32], with significant impacts on the overall security engineering domain, e.g. in the aerospace domain [45].

In a context of cyber-warfare [46, 47], chance is that regulation will increase in the coming years, clearing up the overall picture with the emergence of acceptable means of compliance. For example, in the medical domain, since it was shown that some medical devices, e.g. pacemakers and insulin pumps, can be remotely controlled, engendering concern about privacy and security issues [48], the Food and Drug Administration (FDA) released over 20 regulations [49] aiming to improve the security of data in medical devices. But until this regulatory work is generalized in all safety-critical domains, some confusion is to be expected.

5 Security criteria to be considered in Security for Safety

In section §3 above, we asked ourselves if the term *security* had the same meaning when used standalone, or when used in the *security for safety* expression. Classically, information security is defined as a composite of Confidentiality, Integrity and Availability (CIA), whereby Confidentiality is the absence of unauthorized disclosure of information, Integrity is the absence of unauthorised IT system state alteration, and Availability the readiness for correct IT system service for authorized users.

Safety being usually understood as the absence of catastrophic consequences on the user(s) and the environment, the question here is whether the three CIA criteria make sense in a *security for safety* approach. The question is particularly pregnant for the Confidentiality criterion, the compromising of which usually has only indirect consequences on safety. Another pregnant question is whether denial-of-service attacks are in the scope.

In the railway domain, EN 20159 [50] includes provisions for intentional attacks by means of messages to safety-related applications, but it does not cover general IT security issues and in particular it does not cover IT security issues

concerning the confidentiality of safety-related information, and the overloading of the transmission system.

By contrast, the obsolete ED-202 [51] defined airworthiness security as "the protection of the airworthiness of an aircraft from the information security threat: an adverse effect on safety due to human action (intentional or unintentional) using access, use, disclosure, denial, disruption, modification, or destruction of data and/or data interfaces. This includes the consequences of malware and forged data and access by other systems to aircraft systems". Here, access, use and disclosure clearly relate to the Confidentiality criterion; denial, disruption and destruction clearly relate to the Availability criterion, and modification to the Integrity criterion. ED-202 excluded a number of areas from its scope, and in particular security sensitive handling of security assessment results, national rules on confidentiality, privacy or key escrow regulations. Nevertheless, this ambitious challenge seems to have been dramatically reduced in the new edition, ED-202A [11], in which airworthiness security is now defined as: "the protection of the airworthiness of an aircraft from intentional unauthenticated electronic interaction: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data [etc., as above]". It is to be noted that the term *denial* has disappeared from the definition, and the information threat limited to intentional unauthenticated interaction.

The above tends to show that indeed the term Security is not well defined in the Security for Safety context. This may explain why the industrial safety communities are chary about recommending generic security standards, which would possibly engage them beyond what they can reasonably achieve.

6 Conclusion

Safety and security co-engineering seems to be primarily a concern of the safety engineering communities. Indeed, the increasing number of cyber-attacks in the world tends to show that safety-critical systems, and in particular cyber-physical systems, which are particularly exposed by nature, may not be as safe as they claim, if they are not also secure. The multiplication of security-related workshops in conjunction to safety-related conferences, and the multiplication of safety standards updates that include security concerns, both provide significant testimonies of this growing interest for safety and security co-engineering by the safety community. There is no similar booing within the security community with respect to safety engineering.

Nevertheless, despite all the papers and standards published by the different academic and industrial safety engineering communities, we have shown that it is still very difficult to precisely define what is meant by *security for safety*.

In terms of overall engineering process definition, certain options, such as *security-informed safety* may have tremendous impacts on the competencies required by safety experts, whereas other options, such as *safety-informed security* may require specific trade-off support. The different safety communities do not seem very clear on the directions to take, even if the aeronautical community has recently opted for a *safety-informed security* approach.

In terms of standards, we have shown that the safety standardisation communities seem keen to create their own domain-specific security standards, rather than use the traditional and generic security standards. This may be because the meaning of *security* is not very clear when used in conjunction to safety engineering, in particular with respect to the *confidentiality* criteria and *denial of service* attacks.

In terms of regulation, we have shown that the current standardisation effort is made difficult by the absence of international regulatory bodies, and thereof, the multiplication of National regulations. Chance is that this situation will evolve towards more regulation, and thus clarify the picture.

7 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 engineering specialities. This paper represents a snapshot of the collaborative work realised as part of the MERgE project. Beyond the big picture given herein, work is ongoing on more focused technical questions. In this context, recommendations for security and safety co-engineering are under preparation [52].

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 author wishes to acknowledge Frédérique Vallée and Anthony Faucogney (ALL4TEC), Timo Wiander (STUK), Julien Brunel (ONERA), and Laurent Rioux (TRT).

References

[1] IEC 61508-1, "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements," International Electrotechnical Commission, 1998.

[2] Wikipedia 9/11, "September 11 attacks," Wikipedia, the free encyclopedia, 21 12 2014. [Online]. Available: http://en.wikipedia.org/wiki/September_ 11_attacks. [Accessed 22 12 2014].

[3] N. Fallière, "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems," Symantec, 06 08 2010. [Online]. Available: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices. [Accessed 12 05 2014].

[4] S + IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission, 2010.

[5] S. Paul, "Over 20 Years of Research in Safety and Cybersecurity Co-Engineering: a Bibliography," submitted at the *6th International Conference on Safety and Security Engineering* (*SAFE*), Opatija, 2015.
[6] L. Piètre-Cambacedes and M. Bouissou, "Cross-fertilizations between safety and security engineering," *Reliability Engineering & System Safety,* vol. 110, p. 110–126, 2013.
[7] SeSaMo, "Security and Safety Modelling," 2012. [Online]. Available: http://sesamo-project.eu/. [Accessed 20 05 2014].
[8] MERgE, 2012. [Online]. Available: http://www.merge-project.eu/. [Accessed 27 11 2014].
[9] ARTEMIS EMC2, 2014. [Online]. Available: http://www.artemis-emc2.eu/. [Accessed 30 09 2014].
[10] 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].
[11] EUROCAE ED-202A, "Airworthiness Security Process Specification," European Organization for Civil Aviation Equipment (EUROCAE), 2014.
[12] IEC 62645, "Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems," International Electrotechnical Commission, 2014.
[13] A. G. Hessami, "Surety: Atkins Integrated Safety, Security and Environmental Assurance, Product Sheet," [Online]. Available: http://www.atkinsglobal.com/. [Accessed 2014].
[14] SafeRiver, "Safe River, Safety & Security Forge," Safe River, 2014. [Online]. Available: http://www.saferiver.fr/?setlang=en. [Accessed 22 12 2014].
[15] Sysgo, "PikeOS Hypervisor," 2014. [Online]. Available: http://www.sysgo.com/products/pikeos-rtos-and-virtualization-concept/. [Accessed 16 12 2014].
[16] Green Hills Software, "Integrity Real-Time Operating System," 2014. [Online]. Available: http://www.ghs.com/products/rtos/integrity.html. [Accessed 16 12 2014].
[17] ISO/IEC 27001, "Information technology – Security techniques – Information security management systems – Requirements," International Standards Organization/International Electrotechnical Commission, 2013.
[18] ISO/IEC 15408-1, "Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model," International Standards Organization/International Electrotechnical Commission, 2009.
[19] EASA, "Regulations," European Aviation Safety Agency , 2014. [Online]. Available: http://easa.europa.eu/regulations. [Accessed 27 09 2014].
[20] 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.

[21] 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.
[22] ECSS-Q-ST-40C, "Space product assurance – Safety," European Cooperation on Space Standardization (ECSS), Noordwijk, 2009.
[23] ISO/IEC 27000, "Information technology – Security techniques – Information security management systems – Overview and vocabulary," International Standards Organization/International Electrotechnical Commission, 2014.
[24] ISO/IEC 27002, "Information technology – Security techniques – Code of practice for information security controls," International Standards Organization/International Electrotechnical Commission, 2013.
[25] ISO/IEC 27005, "Information technology – Security techniques – Information security risk management," International Standards Organization/International Electrotechnical Commission, 2011.
[26] ISO/IEC 15408-2, "Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components," International Standards Organization/International Electrotechnical Commission, 2008.
[27] ISO/IEC 15408-3, "Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components," International Standards Organization/International Electrotechnical Commission, 2008.
[28] ISO/IEC 18045, "nformation technology – Security techniques – Methodology for IT security evaluation," International Standards Organization/International Electrotechnical Commission (ISO/IEC), 2008.
[29] NIST SP 800-30, "Risk Management Guide for Information Technology Systems, Special Publication 800-30," National Institute of Standards and Technology, Gaithersburg, 2002.
[30] NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems Federal Information Systems, Special Publication 800-53, Revision 4," National Institute of Standards and Technology, Gaithersburg, 2013.
[31] NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, Revision 1," National Institute of Standards and Technology, Gaithersburg, 2013.
[32] NIST Cybersecurity Framework, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2014.
[33] ISO 26262-1, "Road vehicles – Functional safety – Part 1: Vocabulary," International Organization for Standardization, 2011.
[34] ISO 26262-10, "Road vehicles – Functional safety – Part 10: Guideline on ISO 26262," International Organization for Standardization, 2012.
[35] 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.

[36] C. Gebauer, "Safety and security as drivers for future system development," in *1st Workshop on Safety and Security*, Kaiserslautern, 2014.

[37] IEC/TS 62443-1-1, "Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models," International Electrotechnical Commission, 2009.

[38] IEC 62443-2-1, "Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program," International Electrotechnical Commission, 2010.

[39] IEC/TR 62443-3-1, "Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems," International Electrotechnical Commission, 2009.

[40] IEC 62443-3-3, "Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels," International Electrotechnical Commission, 2013.

[41] 25-356-SC, "Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Isolation or Protection From Unauthorized Passenger Domain Systems Access," Federal Aviation Administration, 01 02 2008. [Online]. Available: https://federalregister.gov/a/E7-25467. [Accessed 12 11 2014].

[42] 25-357-SC, "Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Protection of Airplane Systems and Data Networks from Unauthorized External Access," Federal Aviation Administration, 28 12 2007. [Online]. Available: https://federalregister.gov/a/E7-25075. [Accessed 10 10 2014].

[43] STUK Guide YVL A.12, "Information security management of a nuclear facility," Radiation and Nuclear Safety Authority (STUK), 22 11 2013. [Online]. Available: http://www.finlex.fi/data/normit/41822-YVL_A.12e.pdf. [Accessed 23 12 2014].

[44] B. Obama, *Improving Critical Infrastructure Cybersecurity,* Washington: The White House, Office of the Press Secretary, 2013.

[45] Boeing Cybersecurity Framework, "Developing a Framework to Improve Critical Infrastructure Cybersecurity," Boeing, 2013.

[46] E. Bumiller and T. Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," The New York Times, 11 10 2012. [Online]. Available: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0. [Accessed 23 12 2014].

[47] K. Calamur, "Lengthy, Widespread Internet Outage Reported In North Korea," NPR, 22 12 2014. [Online]. Available: http://www.npr.org/blogs/thetwo-way/2014/12/22/372531702/widespread-internet-outage-reported-in-north-korea. [Accessed 23 12 2014].

[48] Wikipedia Medical Device, "Medical device," 01 09 2014. [Online]. Available: http://en.wikipedia.org/wiki/Medical_device#cite_note-4. [Accessed 06 10 2014].
[49] FR-78-151-47712, "Federal Register/Vol. 78, No. 151, p 47712," 06 08 2013. [Online]. Available: http://www.gpo.gov/fdsys/pkg/FR-2013-08-06/pdf/2013-19020.pdf. [Accessed 06 10 2014].
[50] CENELEC EN 20159, "Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems," European Committee for Electro-technical Standardization, 2010.
[51] EUROCAE ED-202, "Airworthiness security process specification," European Organization for Civil Aviation Equipment (EUROCAE), 2010.
[52] S. Paul, L. Rioux, T. Wiander and F. Vallée, "Recommendations for security and safety co-engineering (release n°2)," ITEA2 MERgE project, 2015.
[53] IEC 61508-7, "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures," International Electrotechnical Commission, 2000.