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
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 Piètre-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], Knorrecker 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 whilst 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], Srivathanakul 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


