

	<p>ITEA2 – Project #11011 Multi-Concerns Interactions System Engineering 01.12.2012 to 31.03.2016</p>
---	--

**Recommendations for Security and Safety Co-engineering
(Release n°3)**

Project Deliverable D3.4.4 – Part A (Stéphane Paul, TRT)

Task 3.4 – Advanced concepts in safety and security co-engineering (Laurent RIOUX, TRT)
 WP3 – Advanced multi-concerns engineering concepts (Sam MICHIELS, KUL)

<p>Status</p> <p><input type="checkbox"/> Draft <input type="checkbox"/> To be reviewed <input checked="" type="checkbox"/> Final</p> <p>Confidentiality</p> <p><input checked="" type="checkbox"/> Public (for public distribution) <input type="checkbox"/> Restricted (only MERgE internal use) <input type="checkbox"/> Confidential (only for individual partner(s))</p>	<p>Document Created : 18.08.2015 Last edited : 22.04.2016 Due date : 28.02.2016 Ready for review : 01.02.2016 Document Version : 1.0 Pages : 166</p>
---	---

Contributors : TRT, ALL4TEC, ONERA, STUK

Executive summary

Nowadays, safety and security are two risk-driven activities that are tackled separately, giving rise to the industrial challenge of efficiently and economically co-engineering these two specialities. It is evident that there is a major opportunity to share on onomastics¹, algorithms, (formal) methods and tools, in particular to reach higher levels of assurance at contained costs.

Deliverable D3.4.4 is split in two parts. Part A (this document) is an extensive state of the art on safety and security co-engineering of software intensive critical information systems. It essentially covers academic publications and industry standards.

Part B (companion document) first reports on two prototype tools dedicated to safety and security co-engineering. The first prototype was designed and developed by MERgE partners based on safety and security requirements from the MERgE software-defined radio test case. The document recalls the requirements and presents the high-level design. Assessment results of this prototype can be found in deliverable D1.1.1d – TCS Evaluation. The second prototype, called AVATAR, is developed by Télécom ParisTech and was identified during our study of the state of the art. We performed an in-depth assessment of this academic tool. Based on the experience we gained during the state of the art work (of which a synthesis is provided in Part B) and tool prototyping work, Part B proceeds with research and development recommendations for new federative approaches, whilst remaining realistic with respect to industrial constraints, i.e. costs, legacy workbenches, training constraints, etc.

Note: the executive summary is common to both parts A and B.

 <p>INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT</p>	
--	---

¹ Study of names and naming.

Version	Content	Resp. Partner	Date
0.01	Creation of the document D3.4.4 based on D3.4.3. Enhancement of the state of the art.	S. Paul (TRT) L. Rioux (TRT) J. de Oliveira (TRT) G. Gailliard (TCS) J.-L. Gilbert (TCS) T. Wiander (STUK) F. Vallée (All4Tec) M. Bakkali (All4tec) A. Faucogney (All4tec) J. Brunel (ONERA) D. Chemouil (ONERA)	18/08/2015
0.02	Extension of the state of the art with the papers from the ISSE'15 workshop.	Stéphane Paul (TRT)	22/09/2015
0.03	Further enhancement of the state of the art.	Stéphane Paul (TRT)	07/10/2015
0.04	Split of the document in two parts.	Stéphane Paul (TRT)	24/11/2015
0.05	Correction of reference errors.	Stéphane Paul (TRT)	04/01/2016
0.06	Correction of the document template.	S. Paul (TRT) L. Rioux (TRT) F. Vallée (All4Tec) M. Bakkali (All4Tec) J. Brunel (ONERA)	07/01/2016
0.07	Extended §6.	Stéphane Paul (TRT)	07/01/2016
0.08	Extended state of the art (academic & standards). Cleaning up of comments & of references. Update of Extended Executive Summary to align with content in Part B.	Stéphane Paul (TRT)	15/01/2016
0.09	Internal review. Minor corrections. Extension of §6.	Philippe Bonnot (TRT) Stéphane Paul (TRT)	01/02/2016
0.99	Peer review.	Grégory Gailliard (TCS)	16/02/2016
1.00	Final submission.	Stéphane Paul (TRT)	16/02/2016

Reviewed & Accepted	Name	Partner
Independent Reviewer (outside WP)	G. Gailliard	Thales Communications & Security
Validation from Management Board	S. Michiels	Katholieke Universiteit Leuven

Contents

Recommendations for Security and Safety Co-engineering (Release n°3)	1
1 Introduction	13
1.1 Purpose of the document	13
1.2 Scope of the document	13
1.3 Motivations	13
1.4 Targeted audience.....	14
1.5 Structure of the document	14
2 State of the art in safety and security co-engineering research	16
2.1 Introduction	16
2.2 Chronological review	16
3 Overview of safety and security standards	91
3.1 Overview of safety standards	93
3.1.1 Transverse safety standards	93
3.1.2 Automotive safety standards	94
3.1.3 Aviation safety standards	95
3.1.4 Space safety standards	101
3.1.5 Railway safety standards.....	101
3.1.6 Medical devices safety standards.....	103
3.1.7 Nuclear safety standards.....	104
3.1.8 Process industry safety standards	105
3.2 Overview of security standards	105
3.2.1 Regulation.....	105
3.2.2 Scope.....	106
3.2.3 Cross-domain standards	108
3.2.4 Aerospace domain specific security standards	110
3.2.5 Nuclear domain specific security standards	111
3.3 Overview of standards transverse to safety and security.....	112
3.4 Analysis of standards w.r.t. safety and security co-engineering concerns.....	113
3.4.1 Analysis of transverse safety standards.....	113
3.4.2 Analysis of automotive safety standards	113
3.4.3 Analysis of aviation safety standards	114
3.4.4 Analysis of space safety standards	114
3.4.5 Analysis of railway safety standards	114
3.4.6 Analysis of medical devices safety standards	114
3.4.7 Analysis of nuclear safety standards	114
3.4.8 Overall analysis	115
3.5 Detailed analysis of the taxonomy of safety and security standards	116
4 A state of the art in safety and security co-engineering in industry	118
4.1.1 Market offers.....	118
4.1.2 Insight on security management in a safety-first industry: Nuclear Energy domain at STUK...	119
4.1.3 Insight on computing safety and security co-engineering at Thales	121
5 A state of the art in safety and security co-engineering in education	123
6 Other safety and security co-engineering focal points	124

7 References..... 127

8 Acronyms..... 147

9 Appendixes..... 151

9.1 Airworthiness Security Process Specification 151

9.2 Airworthiness Security Methods and Considerations 158

List of Figures

Figure 1: Number of safety and security co-engineering related research publications per year.....	10
Figure 2: Identified trends in safety and security engineering	11
Figure 3: Exponential code size evolution on Airbus aircraft	13
Figure 4: On the use of hierarchical structure to achieve safety and security requirements	16
Figure 5: Definitions of safety (left) and security (right) criticality (Burns, et al., 1992).....	17
Figure 6: Understanding security in dependability terms (Jonsson, et al., 1992)	17
Figure 7: Critical system properties versus interactions and coupling (Rushby, 1994)	18
Figure 8: Errors at each of the elements of production, and breach trajectory (Brostoff, et al., 2001)	20
Figure 9: An extended list of guidewords and attributes suitable for identifying security threats (Winther, et al., 2001)	20
Figure 10: Extract of cross-reference between CC class components and DO-178B sections (Taylor, et al., 2002a)	21
Figure 11: Additional guide-words to handle timing issues (Foster, 2002)	21
Figure 12: Reconnaissance fault tree (Helmer, et al., 2002)	22
Figure 13: Revised guide phrase template (Lano, et al., 2002)	22
Figure 14: Rough correspondence between the Common Criteria assurance classes and the DO-178B software processes (Taylor, et al., 2002b).....	23
Figure 15: Defensibility as a kind of dependability (Firesmith, 2003)	23
Figure 16: Example of decomposition of concerns on a medical information system (Sommerville, 2003).....	24
Figure 17: Security-safety lifecycle (Sørby, 2003)	25
Figure 18: Groupings of the means for dependability and security (Avizienis, et al., 2004).....	25
Figure 19: Identifying the best practices in iCMM and CMMI (Ibrahim, et al., 2004)	26
Figure 20: Probabilistic security model structure (Nicol, et al., 2004)	27
Figure 21: Extract of goal structure for the achievement of a dependable system (Altran Praxis, 2006).....	29
Figure 22: An integrated model of security and dependability (Jonsson, 2006)	30
Figure 23: Fault trees and attack trees for a system as interpreted by developers and attackers (Murdoch, et al., 2006)	30
Figure 24: Aircraft Configuration Life Cycle (Olive, et al., 2006).....	31
Figure 25: State transition model of DNS server with game elements identified (Sallhammar, et al., 2006)	31
Figure 26: The unified security/safety risk framework (Stoneburner, 2006)	32
Figure 27: The SeSa method (Grøtan, et al., 2007)	33
Figure 28: Layered model and remote access path to the SIS (Grøtan, et al., 2007)	33
Figure 29: Pre-design of a safe and secure BACS (Novak, et al., 2007)	33
Figure 30: Cases of accidents (left) and Root causes of hazardous incidents (right) (Pan, et al., 2007b).....	34
Figure 31: What-If reviews (Yang, et al., 2007)	34
Figure 32: Conceptual Design for a MILS Workstation (Boettcher, et al., 2008)	35
Figure 33: Genesis of the safety-related security problem: loss of the engineer's paradise (Daniel, 2008)	35
Figure 34: The SafSec approach (Jackson, et al., 2008).....	36
Figure 35: The probability of identifying each failure mode (Stålhane, et al., 2008).....	37
Figure 36: Test derivation efficiency, comparing HazOp with traditional approaches (Daruwala, et al., 2009) ...	38
Figure 37: Integrated fault tree and attack tree (Fovino, et al., 2009).....	39
Figure 38: Safety device attack entry points versus hacker challenges (Hansen, 2009)	40
Figure 39: Key lifecycle alignment points (Hunter, 2009)	41
Figure 40: The FUI 8 PARSC project (PARSEC, 2009)	42
Figure 41: The SEMA framework (Piètre-Cambacédès, et al., 2009)	42

Figure 42: Different domain models of the world (Sun, et al., 2009)	43
Figure 43: Example of parametric diagram using AVATAR (Apvrille, et al., 2010a)	43
Figure 44: AADL processor component extended to model a partition kernel	44
Figure 45: Convergence between ISO 27005 and ISO 15026 (Derock, et al., 2010)	45
Figure 46: Safety-objectives per safety-level according to DO-178B (Gutgarts, et al., 2010)	46
Figure 47: Example of Boolean logic Driven Markov Process (Piètre-Cambacédès, et al., 2010).....	46
Figure 48: Four different types of safety- and security-related requirements (Firesmith, 2010).....	47
Figure 49: Augmenting the attack tree model	47
Figure 50: Threat tree assessment process (Förster, et al., 2010).....	47
Figure 51: Displaying an arbitrary message and a false speedometer reading on the Driver Information Centre, whilst the car is in Park (Koscher, et al., 2010).....	48
Figure 52: Categorization of systems by impact of failure or compromise (Axelrod, 2011)	48
Figure 53: Framework of Information integration of safety and security for high-speed railway (Zhenhai, et al., 2010)	49
Figure 54: Standardized safety profiles (Åkerberg, 2011)	50
Figure 55: Proposed framework for safe and secure communication (Åkerberg, 2011)	50
Figure 56: Challenges of Future Research on Safety and Security in Germany (Gerhold, 2011)	50
Figure 57: Integrating Security Threats to GNSS Architectures within GSN Safety Arguments (Johnson, 2011).....	51
Figure 58: S + IEC 61508 security model for segregation (Mc Guire, 2011)	51
Figure 59: SysML block diagram showing initial shared knowledge, confidentiality and authenticity properties, and classical cryptographic functions (Pedroza, et al., 2011).....	52
Figure 60: Abstract modelling framework for CPS, global CPS (Banerjee, et al., 2012)	53
Figure 61: Relevant existing processes for the SEISES programme (Bieber, et al., 2012)	53
Figure 62: Security level classification (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010)	54
Figure 63: A possible SL / EAL mapping (Blanquart, et al., 2012)	54
Figure 64: Top-down approach threat scenario identification: from feared event to potential causes (Casals, et al., 2012)	54
Figure 65: A roadmap for cyber-safety engineering (Johnson, 2012)	55
Figure 66: MILS virtualisation technique [left] and trustworthy embedded transaction architecture [right] (Kleidermacher, et al., 2012).....	56
Figure 67: Conceptual model (Monakova, et al., 2012)	56
Figure 68: Gateway Software Architecture (Müller, et al., 2012a) (Müller, et al., 2012b).....	57
Figure 69: Gateway modules (Müller, et al., 2012b)	57
Figure 70: Overview of safety-related development assurance in aerospace (Paulitsch, et al., 2012).....	58
Figure 71: Example of FSD usage (Raspotnig, et al., 2012a)	58
Figure 72: The conceptual model for safety and security (Raspotnig, et al., 2013b)	59
Figure 73: Adding SIL in TRVA, for impact calculation (Reichenbach, et al., 2012)	59
Figure 74: Safety and security integrated paradigm (Sadvandi, et al., 2012).....	59
Figure 75: Overview of building blocks (SeSaMo, 2012)	60
Figure 76: Securing information systems and making software systems safe (Axelrod, 2013b)	61
Figure 77: Program synthesis (Fisher, 2013).....	62
Figure 78: Traceability-process model with CHASSIS artefacts, relations & coverage (Katta, et al., 2013a).....	63
Figure 79: Safety/security requirements engineering process (Kornecki, et al., 2013a)	64
Figure 80: Dependency relations for the Security node of the BBN (Kornecki, et al., 2013b).....	64
Figure 81: Conceptual layers (Mattila, 2013)	65
Figure 82: An overall vision of existing cross-fertilizations between safety and security engineering tools and methodologies (Piètre-Cambacédès, et al., 2013).....	66
Figure 83: (a) SEFT modelling elements, and (b) Reactor modelled as a SEFT (Roth, et al., 2013)	67
Figure 84: Quantity of loadable software parts in Boeing aircraft (Rowe, 2013)	67
Figure 85: Standards overlap (Rowe, 2013)	67
Figure 86: Attributes of Building Blocks (SeSaMo D2.1, 2013)	68

Figure 87: The security-informed safety case triangle of assessment (SeSaMo D3.1, 2013).....	68
Figure 88: Conditions for an order of mixed MCSs according to two tuples (Steiner, et al., 2013)	69
Figure 89: Phase 2 of assessment using the NFR approach (Subramanian, et al., 2013)	69
Figure 90: Security vs. non-security fault elimination during operational use (Vouk, 2013)	70
Figure 91: Model transformations for proving safety & security properties (Apvrille, et al., 2014)	70
Figure 92: Security Level Allocation (Bieber, et al., 2014)	71
Figure 93: The onion skin model (Braband, 2014a).....	71
Figure 94: Integrated safety and security verification process (Brunel, et al., 2014b)	72
Figure 95: Mapping safety claims onto NIST security controls (Favaro, et al., 2014)	72
Figure 96: Comparison of selected standards / recommendations (Fruth, et al., 2014).....	73
Figure 97: Protection layers (Gebauer, 2014).....	73
Figure 98: Evolution of the DO-326 standard in time (Joyce, et al., 2014)	74
Figure 99: Safety and security lifecycle activities (Mazzini, et al., 2014)	75
Figure 100: The CHASSIS process diagram (Raspotnig, 2014)	76
Figure 101: Failure Mode, Vulnerabilities and Effect Analysis (Schmittner, et al., 2014a)	77
Figure 102: ConSerts Overview – Engineering Backbone (Schneider, 2014).....	78
Figure 103: Safety vs. security metrics (Schwarz, 2014).....	78
Figure 104: Generic Process Definition (SeSaMo D4.1, 2014)	79
Figure 105: The concept of operations (SeSaMo D4.1, 2014)	80
Figure 106: Runtime Assurance Architecture (Fisher, 2013).....	81
Figure 107: The MILS architectural approach (Tverdyshev, 2014)	81
Figure 108: Proposed extended risk management (Woskowski, 2014)	82
Figure 109: Formal reasoning and platform configuration based on the system architecture (Cimatti, et al., 2015)	83
Figure 110: Analysing railway systems security with an integrative cyber-physical approach (Chen, et al., 2015)	84
Figure 111: Classification of the identified approaches (Kriaa, et al., 2015).....	84
Figure 112: Safety security integrated risk analysis process (Kriaa, et al., 2015)	85
Figure 113: Required resource, required know-how and threat criticality classifications (left), and SecL Determination Matrix (right) (Macher, et al., 2015a)	86
Figure 114: Defining an integrated policy (Netkachova, et al., 2015)	87
Figure 115: Overview of FMVEA method (Schmittner, et al., 2015a).....	88
Figure 116: Comparison of integrity and assurance levels (Schmittner, et al., 2015b)	88
Figure 117: Subordinate case pattern (Taguchi, et al., 2015).....	89
Figure 118: Significant safety standards per application domains.....	92
Figure 119: Functional safety standards based on the IEC 61508 series	93
Figure 120: EU and US Regulation Structures, an avionics point of view (Chevrel, 2014)	96
Figure 121: EASA regulation structure (EASA, 2014)	97
Figure 122: EU Regulation Structures, an Air Traffic Control point of view (Pauly, 2014)	98
Figure 123: US Federal Aviation Regulations (FARs)	98
Figure 124: Relation between standards in the avionics domain (SAE ARP 4754A, 2010).....	99
Figure 125: Mapping of levels between ground and airborne software safety standards	100
Figure 126: Traceability between CENELEC and IEC standards.....	102
Figure 127: The European EN5012x family of railway signalling standards.....	102
Figure 128: Some safety standards for medical devices	104
Figure 129: Some significant security standards	107
Figure 130: Some significant (security) risk management standards	108
Figure 131: Aircraft Network Domains and Interconnections among Domains (ARINC 811, 2005)	111
Figure 132: Overall framework of (IEC 62645, 2014)	112
Figure 133: Taxonomy of security terms in (ISO/IEC 15408-1, 2009).....	117
Figure 134: Model for overall I&C supervision in Finland	120

Figure 135: Airworthiness Security Risk Management Framework (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014).....	151
Figure 136: Airworthiness Security Process Activities (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)	152
Figure 137: Obsolete generic airworthiness security activities as per (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010)	153
Figure 138: Airworthiness Security Process as Part of Aircraft Certification Process (RTCA DO-326, 2010) / (SAE ARP 4754A, 2010) / (EUROCAE ED-79A, 2010).....	154
Figure 139: Security Risk Assessment (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014).....	155
Figure 140: Asset Security Attributes and Threat Conditions (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)	155
Figure 141: Asset Security Effectiveness for the Airworthiness Security Process (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)	156
Figure 142: Simplified example of a security architecture with different types of technical and procedural security measures (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)	156
Figure 143: Security Testing Activities (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)	157
Figure 144: Overview of Airworthiness Security Process Topics (RTCA DO-356, 2014)	158
Figure 145: Trustworthiness Levels (RTCA DO-356, 2014)	159
Figure 146: Examples of Trustworthiness Standards (RTCA DO-356, 2014)	159
Figure 147: Single Stage Threat Scenario (RTCA DO-356, 2014)	160
Figure 148: Two Stages Threat Scenario (RTCA DO-356, 2014)	160
Figure 149: Security Risk Assessment for each stage in the Chain Protection (RTCA DO-356, 2014).....	161
Figure 150: Assets and Failure Condition Classes (RTCA DO-356, 2014)	161
Figure 151: Assets and Threat Condition Classes (RTCA DO-356, 2014).....	162
Figure 152: Likelihood Definitions (RTCA DO-356, 2014)	163
Figure 153: Threat Condition Components (RTCA DO-356, 2014).....	163
Figure 154: Risk Matrix (RTCA DO-356, 2014)	163
Figure 155: Effectiveness Classification of Assurance Level (RTCA DO-356, 2014)	164
Figure 156: Minimum Assurance Levels for Layered Defense-in-Depth Architectures (RTCA DO-356, 2014) .	165
Figure 157: Allocating Assurance Levels to Development or Organizational Trustworthiness (RTCA DO-356, 2014)	165
Figure 158: Layering On-board and Organizational Assurances (RTCA DO-356, 2014).....	165
Figure 159: Alternate Common Criteria EAL Levels for System Level Assurance (RTCA DO-356, 2014).....	166

There will always be engineering failures. But the worst kinds of failures are those that could readily be prevented if only people stayed alert and took reasonable precautions. Engineers, being human, are susceptible to the drowsiness that comes in the absence of crisis. Perhaps one characteristic of a professional is the ability and willingness to stay alert while others doze. Engineering responsibility should not require the stimulation that comes in the wake of catastrophe.

—Samuel C. Florman
The Civilized Engineer

Extended executive summary

Safety and security are two risk-driven activities that are traditionally tackled separately. It is thus possible to distinguish two communities, each working on their own standards, organising their own conferences, publishing in their own journals. Since the 9/11 attacks on the Twin Towers in the Aeronautics domain and the discovery of the Stuxnet computer worm in the Industrial Control Systems domain in June 2010 (cf. Figure 1), it is more and more recognised worldwide that both engineering specialties cannot continue to ignore each other.

Early 2014, when we started this state of the art on safety and security co-engineering for software-intensive systems, we thought we would rapidly establish a comprehensive picture of this small community living in the shadows of the big safety community on the one hand, and of the security community on the other hand. In our minds, safety and security co-engineering questions were intimately linked to niche safety-critical systems markets, such as the Integrated Modular Avionics (IMA), Industrial Control Systems (ICS) or similar networked control systems.

Much to our surprise, we discovered a bustling academic community, with a significant number of publications explicitly addressing safety and security co-engineering concerns (cf. part A, §2), and actively organising workshops and conferences on the subject (cf. part A, §6). As illustrated in Figure 1, our state of the art on academic safety and security co-engineering publications comprehends some 160 references (on a total of over 400 references in the deliverable) concentrating essentially on the last 10 years², even if a few references go back to the early 90's. Recent attention to the topic may be related to the explosion of the number of Cyber-Physical Systems (CPS), System of Systems (SoS) and Internet of Things (IoT) in general public markets. We also found an industrial community actively revising existing safety-related standards or elaborating new standards to cope with business security issues with a certain level of rigor (cf. part A, §3). This standardisation activity is all the more surprising that there is a real lack of international regulation concerning security risk management for safety-critical systems. The last but not least of our surprises was in the education domain: there seems to be very few courses addressing both cyber-security and safety engineering, which does not bode well for the future (cf. part A, §5).

Our state of the art was first organised in a chronological order (cf. part A of this deliverable), and then analysed as a whole. This analysis led us to organise the publications in three groups (cf. part B, §5). A first group comprehends the papers that state the issues related to engineering safety and security separately, and assert that there is room for improvement, but do not explain how. The second group comprehends the papers that propose to improve one specialty by adapting techniques from the other specialty, in other words, safety and security cross-fertilisation. Here, one specialty is seen as more important than the other one, giving way to *security for safety* or vice-versa.

The last set of publications relates to novel clean-slate approaches for safety and security co-engineering, considering both specialties as peers. Amongst these publications, one tool, called TTool/AVATAR, caught our attention and was analysed in depth (cf. Part B, §4).

From the mass of aforementioned publications and after an analysis of internal MERgE case test safety and security co-engineering requirements (cf. part B, §2):

- we identified and developed a new formal system modelling and verification framework for security and safety assessment (cf. part B, §3), which extends the classical safety-related dysfunctional modelling with security-related concerns;

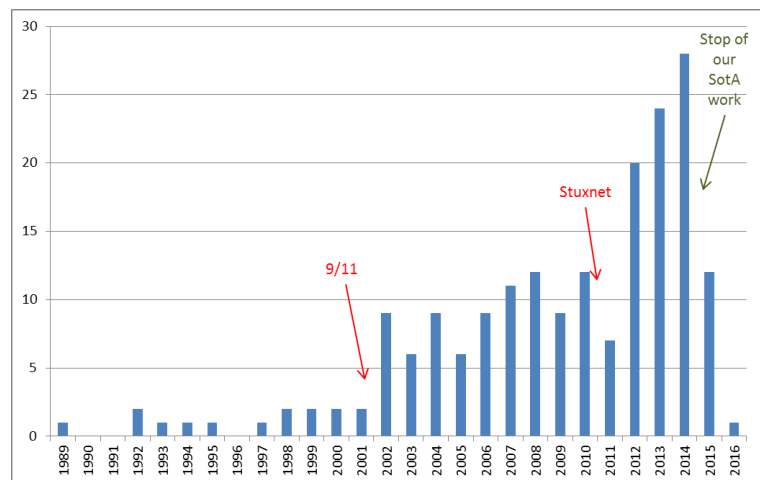


Figure 1: Number of safety and security co-engineering related research publications per year

² The number of references for 2015 is significantly low due to the fact that we stopped our systematic search of publications early 2015, and simply referenced occasional findings.

- we ventured to formulate a couple of facts, and a couple of trends (cf. part B, §6).

The first fact is that safety and security co-engineering seems to be primarily a concern of the safety engineering community. Indeed, the increasing number of cyber-attacks in the world tends to show that safety-critical systems, and in particular the rising number of 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 boogie within the security community: security experts seem to be interested in safety studies in only two cases: (i) to assess if safety-critical systems are more vulnerable when they switch into fail-safe modes; (ii) to re-use safety techniques when availability and integrity are the primary concerns of the security engineering work, by opposition to confidentiality or privacy concerns.

The second major fact is that the security regulation is somehow lagging behind industrial initiatives to produce security standards. This may be explained considering that security is a National sovereignty prerogative, whilst safety regulation has often been transferred to transnational organisations (e.g. European Commission, International Civil Aviation Organisation) since decades. Depending on the domains, National regulation may be seen as too weak or on the contrary an effective means to affect worldwide businesses. In the nuclear domain, renewed national regulation is a driver for unified safety and security considerations as the example of STUK YVL guides suggest. Other industries (e.g. in the aviation domain) have been developing security standards, which cannot be termed as acceptable means of compliance (AMC), since there is no regulation to comply with. This situation is bound to change.

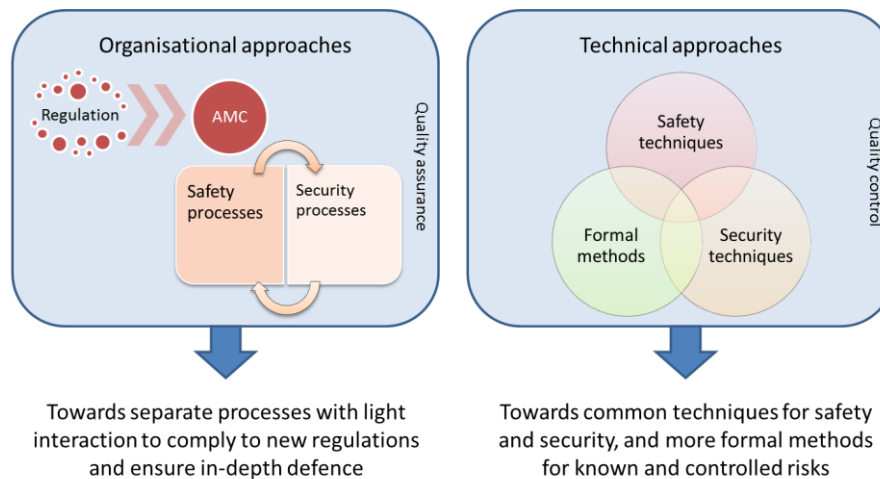


Figure 2: Identified trends in safety and security engineering

Trends (cf. Figure 2) were a bit more difficult to establish. We have formulated two of them based on concordant events happening in multiple domains (e.g. aviation, electronics, nuclear), and on both side of the Atlantic:

- the safety communities thrive to maintain current organizational approaches as stable as possible, because regulations, acceptable means of compliance and standards have proven efficiency records and are extremely difficult to change, technically and / or politically; some minor updates to the processes and methods are however necessary to ensure interaction points, such as safety-aware security in the avionics domain, or security-aware safety in the electrical / electronic / programmable electronic domain; the safety communities seems to be moving away from revolutionising standard safety processes, even if all individual members of those communities do not seem to adhere to this trend;
- the academic and industrial communities are adapting and extending existing, architectures and tools, to cover both safety and security properties; within this trend, the adoption and seamless integration of formal methods and tools occupies a significant part.

These two trends cover quality assurance for the former, to ensure in-depth defence, and quality control for the latter, to cope with known and controlled risks. All of the above is detailed in the current document.

The document concludes on a set of proposals for continued enhanced safety and security co-engineering. The proposals are based on a set of three assumptions:

- industrial safety and security engineering processes / methods are difficult / slow to change;
- safety and security vernacular is difficult / slow to change;
- safety and security tools are diverse, but tend towards a formalisation of their conceptual data model.

Based on these hypotheses, our state of the art and our technical work, the document concludes on three proposals that may feed a safety and security co-engineering research and development roadmap:

- the development of a common pivot model to support artefact sharing between engineering specialties;
- the management of conflicts between safety and security engineering processes seen as independent processes;
- the criteria to be respected by engineering tools to allow for successful cross-fertilisation between engineering domains.

1 Introduction

1.1 Purpose of the document

The purpose of deliverable D3.4.4 is to provide research and development recommendations for safety and security co-engineering of software-intensive safety-critical information and / or embedded systems. The deliverable is split in two parts. This document is the part A.

Part A (this document) is an extensive state of the art on safety and security co-engineering of software intensive critical information systems. It essentially covers academic publications (cf. §2) and industry standards (cf. §3). It marginally covers co-engineering practices in industry (cf. §3.45) and education courses that covers both disciplines simultaneously (cf. §2.4).

1.2 Scope of the document

The scope of the study is the following:

- focus on the safety and security co-engineering of **software-intensive critical information and / or embedded systems**, but not excluding other systems;
- **end-to-end** safety and security **co-engineering**, i.e. from safety and security requirements elicitation, through to the implementation of safety and security solutions, and the verification and validation of those properties;
- safety and security co-engineering **modelling** methods and tools.

This document addresses neither safety and security taken independently, nor safe and secure computing solutions which do not require engineering practices. For a state of the art on safety and security engineering taken as independent disciplines, please refer to (Faucogney, et al., 2014).

1.3 Motivations

There are at least five main motivations for driving this study about safety and security co-engineering.

Motivation n°1: the question is no more *if* your system is going to be subject to a cyber-attack, but *when*.

On Dec. 8th, 2014, the SC Magazine (Stephenson, 2014) makes a title on *Information security in 2014: another year of big events*, and the article starts as follows: *As 2014 draws to a close we can look back over one of the most tumultuous years in recent history. This has been the year of the major security breach. The Target breach was just a warm-up for a laundry list of attacks against large, presumably well-protected, companies and government agencies. Candidly, these organizations – public and private – should be ashamed of themselves. Undeniably, from the cyber-attack point of view, the world is becoming more dangerous every day. As end-users awareness increase, they now consider normal that up to 6% of a safety-critical system's cost may be dedicated to security issues.*

Motivation n°2: safety-critical systems are no more an exception to the rule, being them also subject to cyber-attacks.

As safety-critical systems become more and more complex (cf. Figure 3), and more and more interconnected, cf. (25-356-SC, 2008) and (25-357-SC, 2007), they also become more and more vulnerable to cyber-attacks. A major driver of this evolution is the increasing number of software updates, versus hardware upgrades. This requires ports and protocols for remote maintenance / configuration, which are as many openings for malevolent actions.

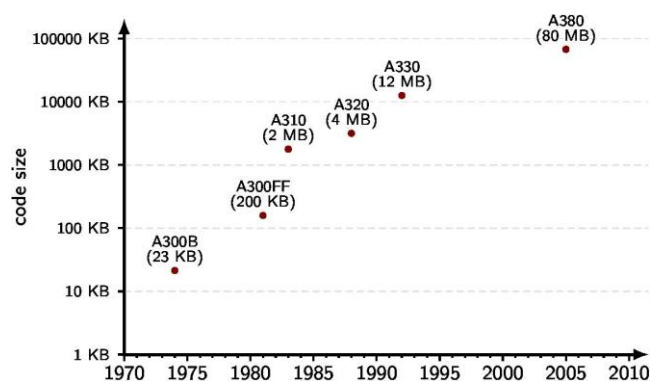


Figure 3: Exponential code size evolution on Airbus aircraft

Motivation n°3: components-off-the-shelf (COTS) have become ubiquitous in software engineering.

The Service and Component Architecture (SCA) has effectively leveraged reuse in the software engineering process, including for safety-critical and/or embedded systems. However, when COTS are massively used in the software design, proving overall safety and security properties is a real challenge. A strategy for COTS selection needs to be defined beforehand, together with guidance on how to use / configure them.

Note: sub-contracted software development fall under the same category as COTS when limited trust is granted to the sub-contractors with respect to the existence of backdoors and / or Trojan horses in the delivered software.

Motivation n°4: system maintenance in secure conditions (MSC) and system maintenance in operational conditions (MCO) go by very different update rates and live cycles.

Safety-critical systems are hard to certify; once certified, modifications are kept minimal in order to avoid running the complete certification process all over again. On the contrary, system maintenance in secure conditions requires frequent updates to keep up with the ever rising new threats and related patches. Living with both these safety and security constraints requires well-thought system architectures.

Motivation n°5: there are no complete and convincing solutions on the market to address simultaneously safety and security engineering, including trade-off decision support.

The safety engineering has a long history of good practices, standards and tools, which have reached a high degree of maturity. The security engineering domain is newer and is subject to constant evolution. Both communities have lived side-by-side with few interactions. One partial exception to this statement is the MILS architecture used for real-time operating systems (RTOS). The MILS architecture assures properties that are relevant to both safety and security, typically *non-bypassable*, *evaluable*, *always invoked*, and *tamperproof*. MILS currently appears in commercial products, e.g. PikeOs by (Sysgo, 2014), Integrity Multivisor by (Green Hills Software, 2014), VxWorks by (Wind River, 2015), LynxOS by (Lynx Software Technologies, 2015)³ or QNX® Hypervisor by (QNX, 2015). However, by itself, MILS is far from being a complete solution, to cover the complete safety lifecycle, from the functional hazard analyses and safety cases, to verification and validation.

1.4 Targeted audience

The targeted audience of this release of the deliverable is the safety and security co-engineering community, without any restriction.

1.5 Structure of the document

This document is structured as follows.

- Chapter 1 is the current introduction.
- Chapter 2 **Erreur ! Source du renvoi introuvable.** is the core part of the document. It provides an academic state of the art in safety and security co-engineering for software intensive critical information systems. Safety and security are often considered as sub-factors of dependability. However, according to (Rushby, 1994), *“the suggestion that system properties such as availability, reliability, safety, and security should be regarded as attributes of dependability does not meet with universal approval”*. Thus, the present state of the art covers publications that address dependability engineering if and only if both safety and security concerns are mentioned explicitly. For a state of the art examining safety and security independently, please refer to D4.3.1 (Faucogney, et al., 2014). The focus here is on differences, similarities, and approaches aiming at the convergence of both specialities.
- Chapter 3 complements the above academic state of the art with an analysis of safety and security standards. By contrast to the academic state of the art, this state of the art addresses safety standards (§3.1) and security standards (§3.2) separately, and then proceeds with transverse standards (§3.3), and an analysis of the former with respect to safety and security co-engineering concerns (§3.4). At the beginning of the project, we thought about building a taxonomy of safety and security terms in the different standards, so as to verify if a common baseline is possible; however, this work was aborted when we felt that there was not much to gain in this significant work. Preliminary results relate to a taxonomy of terms used in the Common Criteria (cf. §3.5).
- The following chapters complement the above state of the art with a small insight within industry practices (Chapter 4), complements the above state of the art with a small review of education courses that address both safety and security concerns (Chapter 5), and a variety of social-networks (Chapter 6).

³ Previously known as “LinuxWorks”.

- Chapters 7 and 8 provide respectively the references and definitions of acronyms.
- Chapter 9 is a set of appendixes providing extended descriptions of some key referenced documents.

2 State of the art in safety and security co-engineering research

2.1 Introduction

(Axelrod, 2011) points out that “*there exist two distinct groups of software engineers, namely: those concentrating on security-critical information-processing systems, and those focusing on safety-critical process control systems. While there seems to be considerable information sharing among members within each group, as indicated by the volume of publications, there is relatively little communication across groups. Hardly any research and few publications appear to bridge that gap*”. This chapter provides a state of the art in safety and security co-engineering for software intensive critical information systems. It covers publications that address safety and security explicitly⁴. To our surprise, we found the literature to be quite extensive, especially in the recent years. This state of the art focuses on research papers (cf. §2), but also includes a significant analysis of standardisation work (cf. §3), as well as some insight into industry practices (cf. §3.4), education (cf. §5) and a variety of social-networks (cf. §6).

2.2 Chronological review

(Rushby, 1989) proposes to use the concept of *security kernel*, or its extension, the Trusted Computing Base (TCB) comprising a separation kernel and zero or more resource managers, to enforce negative properties other than security, e.g. domain segregation in safety engineering. This gives the author the opportunity of discussing the differences between safety and security in terms of hierarchical structure (cf. Figure 4): the most dependable service is achieved at the top, whilst the most dependable component is located at the bottom of a hierarchical structure. A security kernel enforces security on the system as a whole without requiring the rest of the system to cooperate towards that end. The author argues that a security kernel can influence the behaviour of the whole system through the selection of functions it *does not* provide. By denying the ability to achieve certain behaviours, the kernel can prevent certain faults of commission⁵. An abstract characterization of the class of behaviours that can be enforced in this way is given by a simple second-order formula: $\forall \alpha \in \text{op}^*, P(\alpha)$, where op^* denotes the set of all sequences of invocations of functions provided by the kernel and $P(\cdot)$ is a predicate over the input/output behaviour of that set. Special cases of this formula are non-interference specifications and invariants on (parts of) the system state. A Trusted Computing Base comprising a separation kernel and zero or more resource managers is appropriate for both cases. The separation kernel enforces the non-interference requirement (causing otherwise isolated *domains* to be *wired up* appropriately), while the resource managers maintain certain properties invariant.

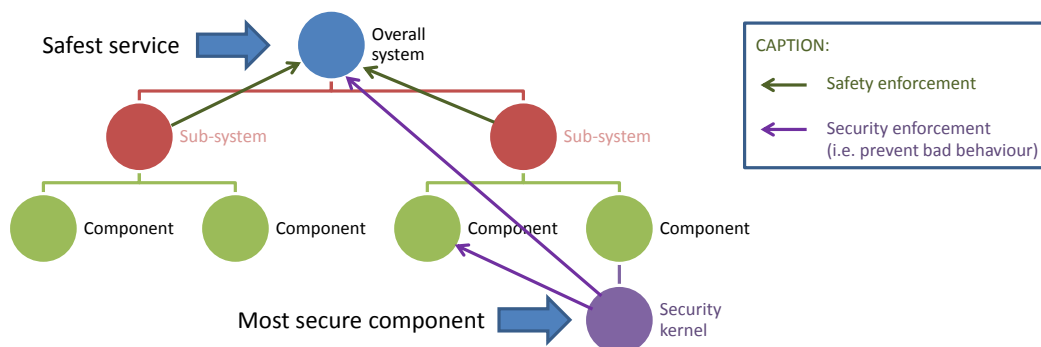


Figure 4: On the use of hierarchical structure to achieve safety and security requirements

(Burns, et al., 1992) extensively discusses the distinction between safety and security in terms of the differences in causal structure and in the degree of harm caused. The paper starts with an informal characterisation of safe-

⁴ Meaning that many publications dealing implicitly with safety and security under the umbrella of dependability may not be included.

⁵ Basili makes a distinction between something that is missing (faults of omission) and something that is incorrect (faults of commission).

ty and security, and proceeds with a formal⁶ notation for representing the concepts (cf. Figure 5). In substance, a computer system (CS) is said to be safety-critical if a failure F_{CS} of the computer system combined with the standing conditions C_{OE} in the operational environment (OE) is sufficient to cause a harmful state H_{CR} for a critical resource (CR). This simple definition of safety-criticality is then extended by modelling the causes of the F_{CS} state, for example by expressing that it is caused by a failure F_O on the part of the operator (O), which the computer system does not prevent or render nugatory, or a legal but inappropriate action A_O by the operator which is not defended against due, for example, to a computer design failure (Dcs). The definition of security-criticality is similar to the safety-criticality one, except that there is an indirection in the causal chain. In the case of security-criticality, a failure F_{CS} of the computer system or an operator malfeasance F_O produces a vulnerability D_{OE} , which can be exploited by an attack A_{FA} by free agents (FAs). An appealing feature of these definitions is the similarity with, respectively fault trees and attack trees, whereby the minimal sufficient conditions (MSCs) have the structure of AND-gates and the disjunction of MSCs have the structure of OR-gates. Finally, it is worth mentioning that this research was supported by the British Admiralty Research Establishment (ARE), now part of the MOD's Defence Research Agency (DRA).

$$H_{CR} \leftarrow \langle C_{OE} \mid F_{CS} \mid \rangle$$

$$\text{with: } F_{CS} \leftarrow \langle C_{CS} \mid F_O \mid \rangle \vee \langle C_{CS} \mid A_O \mid D_{CS} \rangle$$

$$H_{CR} \leftarrow \langle C_{OE} \mid A_{FA} \mid D_{OE} \rangle$$

$$\text{with: } D_{OE} \leftarrow \langle C_{CS} \mid F_{CS} \mid \rangle \vee \langle C_{OE} \mid F_O \rangle$$

Figure 5: Definitions of safety (left) and security (right) criticality (Burns, et al., 1992)

Following the definition of dependability by Jean-Claude Laprie (Laprie, 1992) in which security appeared as an attribute of dependability, (Jonsson, et al., 1992) presents a novel approach to security, intended to facilitate and improve this integration. This is accomplished by taking a dependability viewpoint on traditional security and interpreting it in terms of system behaviour and fault prevention (cf. Figure 6: Understanding security in dependability terms). The author provides some models for dependability and defines security as a concept for fault prevention with respect to intentional external faults or attacks against the system with no specific relation to behavioural attributes, such as privacy or reliability/availability.

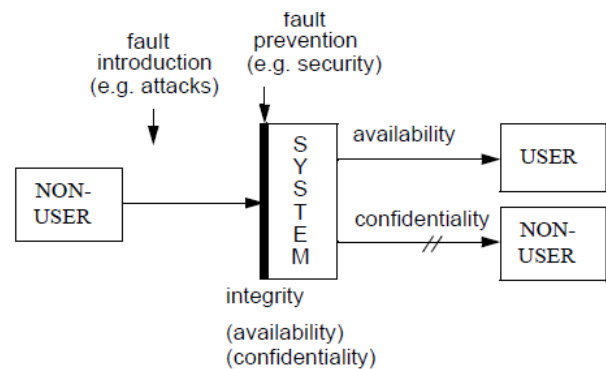


Figure 6: Understanding security in dependability terms (Jonsson, et al., 1992)

(Brewer, 1993) describes a number of security techniques, recalling the history of their evolution. The author recalls that whilst the security engineers have come to appreciate that security must be achieved through a combination of fault preventive and fault tolerance techniques, this approach is newer to safety engineers. The author concludes that safety engineers have much to gain by adopting the security principles of the “reference monitor concept” and the security policy modelling.

(Rushby, 1994) starts by presenting an extensive survey (22 pages) of dependable, safe, secure and real-time systems, concentrating on the critical properties addressed and the mechanisms employed to safeguard them. The author then extensively examines (15 pages) the formal specifications and assurance techniques that have been proposed and used in the four approaches⁷. He points out that the requirement for ultra-criticality⁸ is so many orders of magnitude removed from the failure rates that can be determined empirically in feasible time on test, that essentially all assurance has to come from subjective factors such as examination of the lifecycle processes of its development, and review and analysis of the software itself. The author recalls that the available evidence indicates that very few serious faults are introduced (or remain undetected) in the later stages of the development lifecycle under the very disciplined processes used for critical systems; instead, evidence points to the early lifecycle and to faults in requirements specification as the primary source of catastrophic failures. Rushby assumes that, if formal methods, or any other techniques, are to make major contributions to critical systems, then it seems that they should concentrate on the early lifecycle and on the hardest aspects of a design. Amongst many interesting topics, the paper addresses the topic of verification of safety and security properties in the context of hierarchical refinement versus architectural refinement. The paper concludes on a taxonomy of critical systems founded on two attributes, interaction and coupling, with the aim of identifying compatible

⁶ (Rushby, 1994) mentions that it is not clear in what sense this model is formal, as it does not appear to provide any deductive apparatus.

⁷ I.e. dependability, safety, security and real-time.

⁸ I.e. systems for which the required failure rates range between 10^{-7} and 10^{-12} per hour.

/ incompatible critical system properties. In short (cf. Figure 7), security requires an environment with few and controlled interactions, and leads to tightly coupled systems, safety-critical systems benefit by having few, linear and known interactions, and from loose coupling, whilst the conflicts between security and real time are most sharp when the most flexible and dynamic forms of real-time resource allocation and the strictest notions of security (i.e. no covert channels), are considered.

Interactions	Coupling	
	Loose	Tight
Linear	Weak [†] security Safety	Strict [†] security Fault masking Static real time
Complex	Dynamic real time Fault tolerance	Global coordination

[†] Strict security requires absence of covert channels.

Figure 7: Critical system properties versus interactions and coupling (Rushby, 1994)

(Elliott, et al., 1995) presents a review of safety engineering prior to a perspective on how advances in computer security concepts and techniques may assist in enhancing the current best practice approach to safety assurance. These early findings are from current challenging research involving a comparison between the two domains of safety and security in developing and applying the concept of Safety Policy and deriving suitable Safety Models. The ultimate goal is to develop a Safety Policy Method for application to all types of safety sectors to be utilised throughout any safety systems life cycle.

(Braband, 1997) discusses safety and security aspects of a safety-critical railway application: a future harmonised European Train Control System (ETCS), which utilises public networks for safety-critical train control data transmission. The author mainly focuses on the derivation of (quantitative) safety and security requirements, in particular for the data transmission.

(Stavridou, et al., 1998) examines the relevance of the security concept of non-interference to safety-related properties, and conversely, the applicability of fault-tolerance mechanisms usually applied to provide safety and reliability in the security domain. The paper suggests promising lines of research in the intersection of safety and security, in the application of security concepts and models to different classes of safety or fault-tolerance properties, and in the theory and practice of fault-tolerant systems applied to intrusion tolerance.

(Simpson, et al., 1998) illustrates that the concept of non-interference, used in theories of security, may also be used to reason about safety. It presents a technique for modelling safety properties in terms of communicating sequential processes, and develops a practical theory of system protection from failures. The authors rigorously model fail-safe, i.e. fault with no impact on safety, fail-stop, i.e. fault and associated repairs with no impact on safety, and fail-operational, i.e. fault and associated repairs with no impact on safety nor on functional aspects of the system, behaviours.

The Security, Safety and Quality Evaluation for Dependable Systems (SQUALE) project performed an analysis of existing safety and security standards, namely (ITSEC, 1991), IEC 61508 series⁹, (IEC 60880, 1986), (CENELEC EN 50128, 1997), (ETR 367, 1997) and (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992). Based on this study, (Corneillie, et al., 1999) defines investigation, proofing and assessment activities, applicable within any life cycle and system environment, that are necessary to gain confidence that a system, including its hardware and software components, meets its dependability objectives. To reduce costs, correspondences are established between the SQUALE criteria and the aforementioned standards, whereby the SQUALE Criteria can adopt confidence providing techniques from industrial domain-specific standards. To support these correspondences, a harmonised terminology is defined. The document is rather extensive (190 pages).

(Eames, et al., 1999) investigates safety and security requirements specification methods, and proposed techniques for the integration of methodologies. The nature of interaction between safety and security requirements, and problems relating to their independent development, are discussed. The requirements specifications of an Air Traffic Control system are used to highlight the problems inherent in the independent approach to requirements development. From investigation of the literature and the case study, the authors identify several areas

⁹ Seven parts : (IEC 61508-1, 1998), (IEC 61508-2, 2000), (IEC 61508-3, 1998), (IEC 61508-4, 1998), (IEC 61508-5, 1998), (IEC 61508-6, 2000) (IEC 61508-7, 2000).

that can cause problems when attempting to harmonize safety and security requirements techniques. The most important of these are: different system models used for safety and security; different documentation structures for the analyses and their results; the interaction of safety and security requirements; isolation of safety and security requirements processes.

The authors identify that there is a danger that conflicts can arise if safety and security requirements are developed in isolation. They consider the integration of safety and security requirements processes suggesting that this can be achieved through either unification or harmonisation of the requirements processes. They conclude that while there are significant similarities between the fields of safety and security, each has developed specific tools and skills, that if unified could result in compromises that would result in safety and security risks going unobserved. Harmonisation of the approaches on the other hand, while resulting in two sets of requirements, would ensure that safety and security, and their interrelationships were considered at design time without the potential for requirements to go unobserved.

(Brewer, 2000) recalls that (ISO/IEC 15408-1, 1999) and (ISO/IEC 17799, 2000) are the two most important information Security standards, concluding that they have complementary approaches, the Common Criteria being predicated on the absence of vulnerabilities, whilst the Code of Practice for Information Security Management focuses on managing the risk should exploitable vulnerabilities exist.

The goal of the FP5 IST Malicious-and Accidental-Fault Tolerance for Internet Applications project (MAFTIA, 2000) was to investigate the *tolerance paradigm* for security systematically, with the aim of proposing an integrated architecture built on this paradigm, and realising a concrete design that can be used to support the dependability of many applications. MAFTIA used fault tolerance techniques to build dependable systems that are intrusion tolerant, that is, able to continue providing a secure service, despite the presence of malicious faults, i.e. deliberate attacks on the security of the system. The project's major innovation was a comprehensive approach for tolerating both accidental faults and malicious attacks in large-scale distributed systems, including attacks by external hackers and by corrupt insiders. MAFTIA uniformly applied the tolerance paradigm to the dependability of complete large-scale applications in a hostile environment and not just to single components of such systems. There were three main areas of work: (i) the architecture of MAFTIA: providing a framework that ensures the dependability of distributed applications in the face of a wide class of faults and attacks; (ii) the design of dependability mechanisms and protocols; (iii) the verification and assessment of the work.

(Brostoff, et al., 2001) starts by recalling that information security should be considered and designed as a socio-technical work system, rather than just a technological system. This gives the authors the opportunity of discussing the differences between safety and security from a societal viewpoint, e.g. violations of safety rules are usually not applauded, whereas flaunting petty security regulations is a badge of seniority in many organizations. Based on this socio-technical focus assumption, the authors argue that the traditional safety models can be adapted to security engineering, in particular the Generic Error Modelling System (GEMS¹⁰) and the famous Swiss Cheese model. The models' adaptation to security is ensured by: (i) defining mistakes, lapses, slips and computer security violations as active failures; (ii) defining latent failure as something that predisposes a system to security breaches; (iii) describing a system as *decision-makers*, who direct the organization at a strategic level, *line managers* who implement the strategies, which in turn create *preconditions* for *productive activities*, and *defences*, which protect the organization (cf. Figure 8). The causes of a disaster, or security breach, can be traced to failures at all levels listed in this model. The proposed model has a number of advantages, but the authors recognise that there are also disadvantages, i.e. the model is not easy to operationalise.

¹⁰ Reason's GEMS integrates, within the same framework, the three stages of cognitive processing for tasks (i.e. planning, storage and execution), the different error mechanisms (i.e. mistakes, lapses and slips) and the three levels of performance (i.e. skill, rule and knowledge).

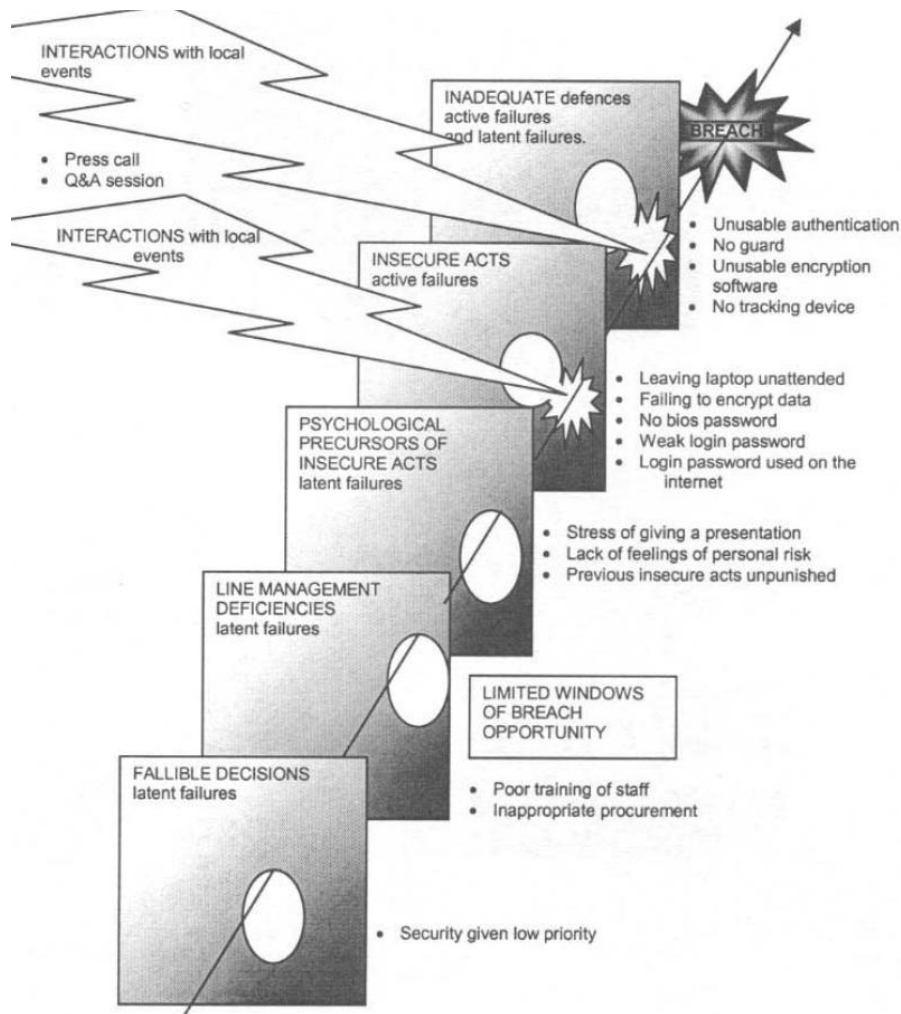


Figure 8: Errors at each of the elements of production, and breach trajectory (Brostoff, et al., 2001)

(Winther, et al., 2001) recalls that the emphasis placed on security issues when developing safety-critical systems is too often inadequate, possibly due to the lack of safety-compliant security methods. The authors report on an adaption of the safety-related HAZard and OPerability (HazOp) principle to the security context, which is well-suited for handling security issues in a safety context. The main modification of the method consists in establishing new guidewords and attributes.

Attributes	Post-Guidewords
disclosure, manipulation, disconnection, fabrication, delay, corruption, deletion, removal, stopping, destabilisation, capacity reduction, destruction, denial	insider, outsider, technical failure, virus, ignorance, fire, faulty auxiliary equipment, sabotage, broken cable, logical problems, logical attack, planned work, configuration fault, spamming, social manipulation

Figure 9: An extended list of guidewords and attributes suitable for identifying security threats (Winther, et al., 2001)

(Alves-Foss, et al., 2002) provides a mapping of the Common Criteria assurance evaluation criteria (ISO/IEC 15408-1, 1999) - (ISO/IEC 15408-3, 1999) to the criteria found in (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992). Specifically, the purpose of this extensive (38 pages) and draft document is to provide guidance for developers of (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992) compliant software on the activities necessary to make their systems also compliant with CC Evaluation Assurance Level (EAL) 5. The Target of Evaluation (ToE) is an airborne software system, and all comments contained within this document refer to only these types of systems. To that end, it is important to understand the context in which these criteria have been creat-

ed, how their requirements are presented and how they can be interpreted. A summary (12 pages) of this document is provided in (Taylor, et al., 2002a). See also (Taylor, et al., 2002b) below.

ACM – Configuration Management ACM_Aut CM Automation ACM_CAP Advanced support ACM_SCP Development Tools	<table border="1"> <tr> <th colspan="2">Software Configuration Management</th> </tr> <tr> <th>Activities</th> <th>Data Control Processes</th> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td>X</td> <td></td> </tr> </table>	Software Configuration Management		Activities	Data Control Processes	X		X		X		Life Cycle Data Sect. 11.4 Sect. 11.18 Sect. 11.4, 11.18																		
Software Configuration Management																														
Activities	Data Control Processes																													
X																														
X																														
X																														
ADO – Delivery and Operation ADO_Del Prevention Modification ADO_IGS Installation and Start-up	(No correspondence with DO-178B Areas) (No correspondence with DO-178B Areas)																													
ADV – Development ADV_FSP Functional Specification ADV_HLD High Level Design ADV_IMP Implementation of TSF ADV_INT Minimization Complexity ADV_LLD Low Level Design ADV_RCR Correspondence Demo ADV_SPM Security Policy Model	<table border="1"> <tr> <th colspan="4">Software Development Process</th> </tr> <tr> <th>Requirements</th> <th>Design</th> <th>Code Integrate</th> <th>Trace</th> </tr> <tr> <td>X</td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>X</td> <td>X</td> <td></td> </tr> <tr> <td></td> <td></td> <td>X</td> <td></td> </tr> <tr> <td></td> <td></td> <td>X</td> <td></td> </tr> <tr> <td>X</td> <td></td> <td></td> <td></td> </tr> </table>	Software Development Process				Requirements	Design	Code Integrate	Trace	X					X	X				X				X		X				Life Cycle Data Sect. 11.6, 11.9, 11.14 Sect. 11.7, 11.10, 11.14 Sect. 11.14, 11.11 Sect. 11.7, 11.10 Sect. 11.14 Sect. 11.9, 11.14
Software Development Process																														
Requirements	Design	Code Integrate	Trace																											
X																														
	X	X																												
		X																												
		X																												
X																														

Figure 10: Extract of cross-reference between CC class components and DO-178B sections (Taylor, et al., 2002a)

(Foster, 2002) reports on a practical case of adaptation of safety engineering techniques to the development of security protocols. To improve the elicitation and analysis of security protocol requirements, the author of this PhD thesis selected and adapted two safety-related techniques. The HAZard and OPerability (HazOp) technique was used as the basis of a new Vulnerability Identification and Analysis (VIA) method – adding new guide-words (cf. Figure 11), and the Fault Tree (FT) technique was used as the basis of a new Requirements Analysis and Elicitation (RAE) tree method. The report concludes that, although the proposed techniques require considerable effort, they result in a more thorough analysis of the protocol scenario.

ADDITIONAL GUIDE WORDS (to handle timing issues)	GENERIC MEANING
Early	Something happens earlier, in (absolute) time, than intended.
Late	Something happens later, in (absolute) time, than intended.
Before	Something happens earlier, in an order or sequence, than intended.
After	Something happens later, in an order or sequence, than intended.

Figure 11: Additional guide-words to handle timing issues (Foster, 2002)

(Helmer, et al., 2002) starts by recalling that requirements analysis for an Intrusion Detection System (IDS) involves deriving requirements for the IDS from analysis of the intrusion domain. When the IDS is a collection of mobile agents that detect, classify, and correlate system and network activities, the derived requirements include what activities the agent software should monitor, what intrusion characteristics the agents should correlate, where the IDS agents should be placed to feasibly detect the intrusions, and what countermeasures the software should initiate. The paper describes the use of software fault trees for requirements identification and analysis in an IDS. Intrusions are divided into seven stages, and a fault sub-tree is developed to model each of the seven stages (reconnaissance, penetration, etc.) Two examples are provided (cf. Figure 12). This approach was found to support requirements evolution (as new intrusions were identified), incremental development of the IDS, and prioritization of countermeasures.

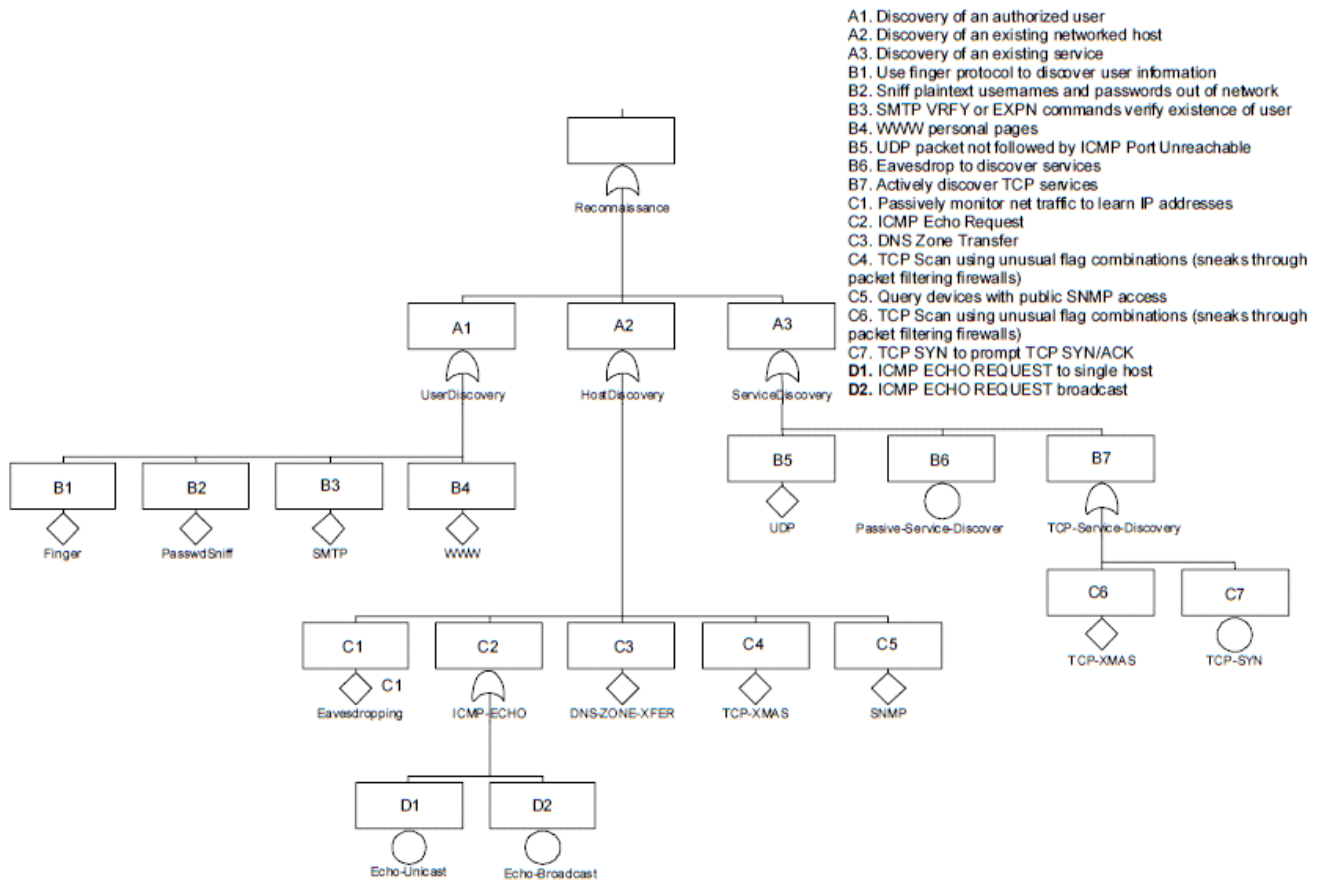


Figure 12: Reconnaissance fault tree (Helmer, et al., 2002)

(Lano, et al., 2002) reviews existing approaches for the safety and security analysis of object-oriented software designs, and identifies ways in which these approaches can be improved and made more rigorous. More precisely, the authors examine how safety analysis techniques such as HAZard and Operability (HAZOP) studies and Fault Tree Analysis (FTA) can be adapted to object-oriented system and software modelling notations, particularly UML. New guide-words (cf. Figure 13) and revised interpretations are extensively presented.

(Pre) Guideword	Attribute	(Post) Guideword
Deliberate	Disclosure Manipulation of COMPONENT by	Insider Outsider
Unintentional	Denial Mis-authentication Repudiation	Technical behaviour/ functionality

Figure 13: Revised guide phrase template (Lano, et al., 2002)

(Lynch, 2002) investigates the similarities and differences between the engineering processes and techniques applied to safety critical systems and those applied to secure systems. It also evaluates some of the potential opportunities for cross-fertilisation between the domains. The technique of developing a safety argument is applied to security, to demonstrate the use of security argument. Several safety hazard identification and assessment techniques (hazard identification checklists, HAZOPS, FMEA, zonal analysis) are applied to security, to demonstrate security hazard identification and analysis. Experiments are carried out to determine how applicable and effective the safety techniques are when applied to secure systems.

(Prentice, 2002) starts by recalling that the US President signed the final version of the Aviation and Transportation Security Act on November 19, 2001, and that he details of this fast-paced legislation are now coming out. The Act established The Transportation Security Administration (TSA). The author states that this law will have a profound effect on the aviation business, our jobs, and the way they are perform.

(Schaefer, 2002) reviews safety and security issues as they relate to technology, both for individuals and for the institution.

(Taylor, et al., 2002b) describes a process of dual certification for software that meets both FAA safety requirements and NIST/NSA security requirements. The two sets of requirements from (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992) and the Common Criteria (ISO/IEC 15408-1, 1999) are assessed for similarity of function with non-corresponding parts identified. Each certification process is outlined and a merged certification procedure is presented. In generating a high-level map between DO-178B and the Common Criteria assurance requirements, the authors made the assumption that all DO-178B requirements would be completed, thus, they identified Common Criteria assurance classes that would not map to any DO-178B processes (cf. Figure 14), for separate inclusion in a final merged process. The work showed that there is a great deal of overlap between DO-178B and the Common Criteria requirements: for many DO-178B requirements, simply incorporating security considerations or following a more rigid methodology is enough to meet both DO-178B and Common Criteria requirements. Three Common Criteria assurance classes did not map. These classes were: Guidance Documents (AGD), Delivery and Operation (ADO) and Vulnerability Assessment (AVA) classes. These requirements need to be added to the merged development process in order to meet both FAA and NIST/NSA certification.

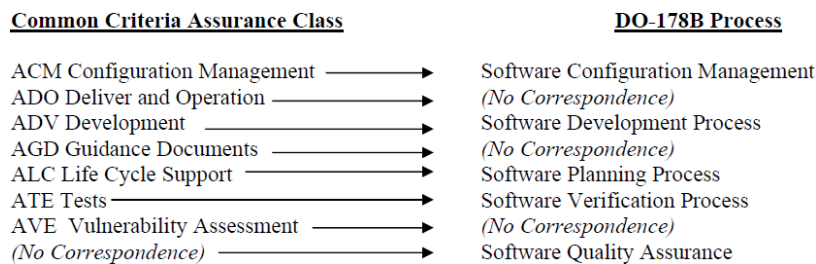


Figure 14: Rough correspondence between the Common Criteria assurance classes and the DO-178B software processes (Taylor, et al., 2002b)

(Brooke, et al., 2003) briefly reviews Fault Tree Analysis (FTA) techniques and explains how similar techniques can be applied to the design and analysis of security-critical systems. The application of this technique is illustrated in an example inspired by a public-key cryptosystem. According to the authors, the major benefit of fault tree analysis applied to security is the identification of the relationship between events, not a quantitative evaluation of security.

(Firesmith, 2003) presents a consistent set of information models that identify and define the foundational concepts underlying safety, security, and survivability¹¹ engineering (cf. Figure 15), and can later be used to define a co-engineering process. In addition, the technical note shows how quality requirements are related to quality factors, sub-factors, criteria, and metrics, and it emphasizes the similarities between the concepts that underlie safety, security, and survivability engineering. The information models presented in this technical note provide a standard terminology and set of concepts that explain the similarities between the asset-based, risk-driven methods for identifying and analysing safety, security, and survivability requirements as well as a rationale for the similarity in architectural mechanisms that are commonly used to fulfil these requirements.

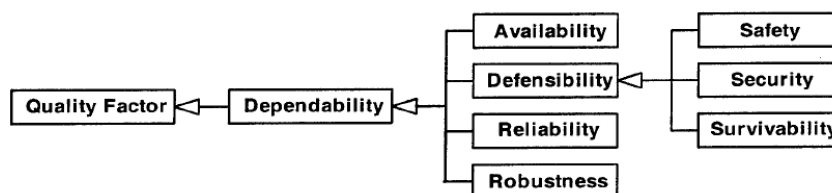


Figure 15: Defensibility as a kind of dependability (Firesmith, 2003)

(Smith, et al., 2003) discusses safety in the rail domain, in terms of concepts, processes, operational challenges, formal methods, standards. The paper builds upon (Eames, et al., 1999) to recall the importance of securing safety-critical systems. The authors then introduce a practical case of application: securing safety-critical communications for the Australian rail network.

¹¹ Here, survivability is defined as the degree to which both accidental and malicious harm to essential, mission-critical services is prevented, detected, and reacted to.

(Sommerville, 2003) has a slightly larger scope than safety and security engineering. The paper discusses an approach to system requirements elicitation that integrates safety requirements elicitation and analysis with more general requirements analysis. The author proposes to organise the analysis round pervasive *concerns*, such as safety and security, which are based on business goals and can drive the system requirements engineering process, thus filling the gap between the operational and system views. Concerns are not about what to *do* but a way of explicitly identifying the key issues around a business / operational goal. The overall method is called DISCOS and illustrated on a medical information system (cf. Figure 16).

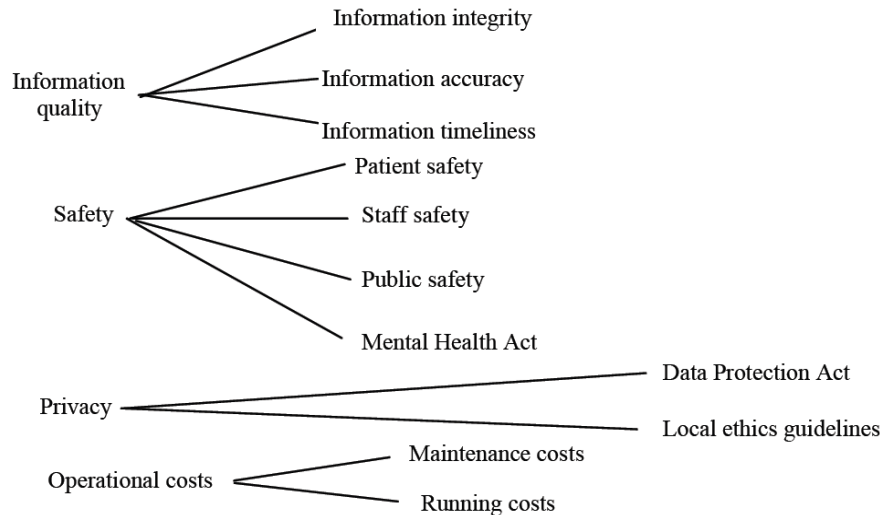


Figure 16: Example of decomposition of concerns on a medical information system (Sommerville, 2003)

(Sørby, 2003) is an impressive master thesis (185 pages) that starts by: (i) providing a brief introduction to the concepts of safety (resp. security) and safety-critical (resp. security-critical) systems, including a safety (resp. security) terminology and its ontology; (ii) recalling the risk management process defined in the Australian risk management standard (AS/NZS 4360, 1999), and briefly describing the most important risk analysis methods; (iii) recalling some basics about wireless networking, with emphasis on security issues in wireless LANs. The report then proposes a development process (cf. Figure 17) for security-safety critical systems, which is based on the safety lifecycle defined in (IEC 61508-1, 1998) and the CORAS integrated risk management and system development process (Braber, et al., 2003). The approach, including a security-HAZOP¹², is extensively illustrated on a toy example of: (i) an industrial robot, represented by a LEGO Mindstorms cutting robot, located into a safety zone whose entrance is controlled by a LEGO Mindstorms gate; and (ii) a monitoring system represented by a Sony AIBO robot. Finally, the author discusses the relationship between safety and security based on experiences gained during the development of the aforementioned system, together with existing definitions and related work in the security and safety domains. Amongst the conclusions, it is stated that the security attribute “confidentiality” is irrelevant in terms of safety: this is because only direct harm was considered, and not events that might open up for other harmful events benefiting from a loss of confidentiality.

¹² HAZard and Operability.

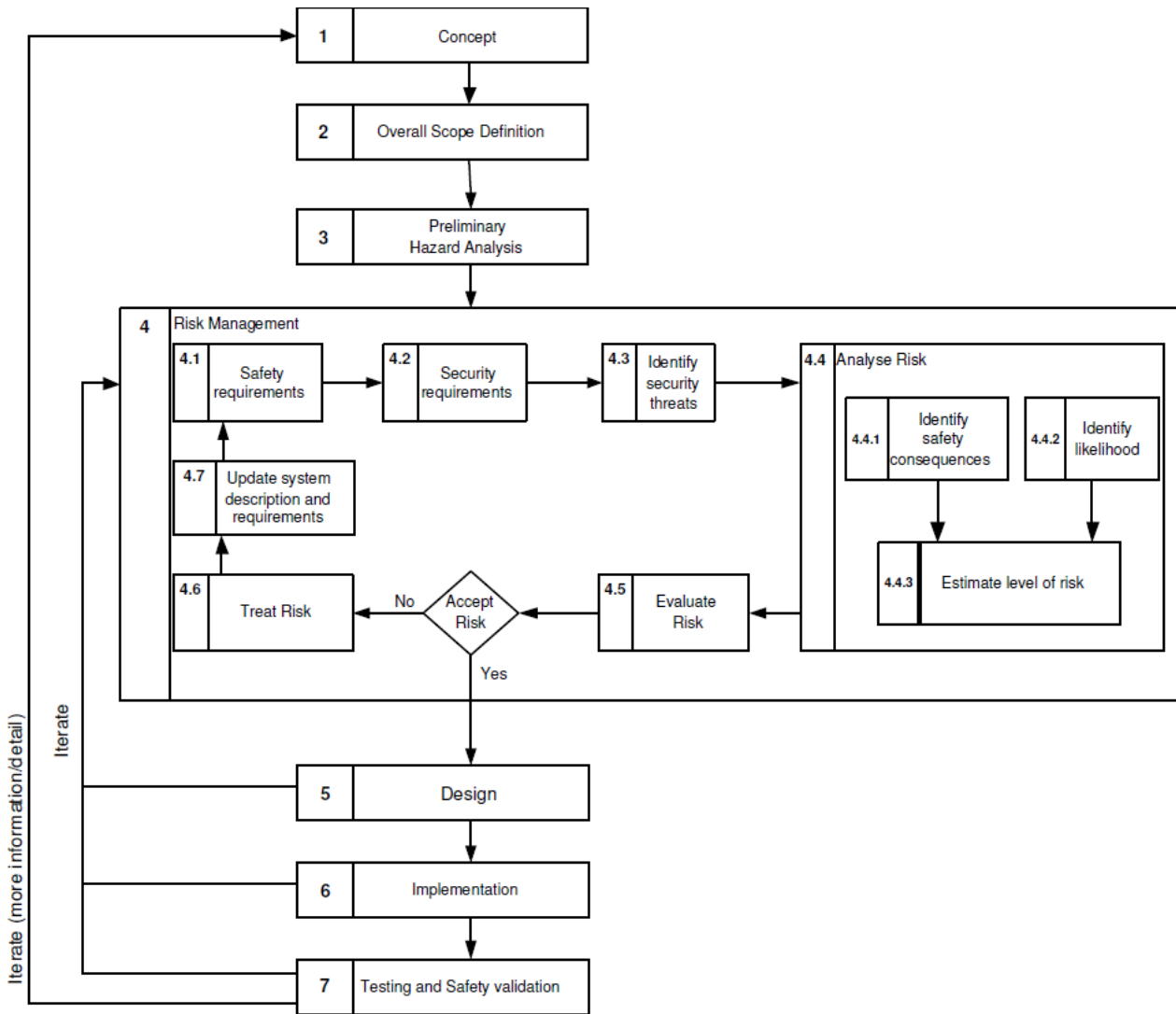


Figure 17: Security-safety lifecycle (Sørby, 2003)

(Avizienis, et al., 2004) gives the main definitions relating to dependability, a generic concept including such attributes as reliability, availability, safety, integrity, maintainability, etc. Security¹³ brings in concerns for confidentiality, in addition to availability and integrity. Basic definitions are given first. They are then commented upon, and supplemented by additional definitions, which address the threats to dependability and security (faults, errors, failures), their attributes, and the means for their achievement (i.e. fault prevention, fault tolerance, fault removal, fault forecasting – cf. Figure 18).

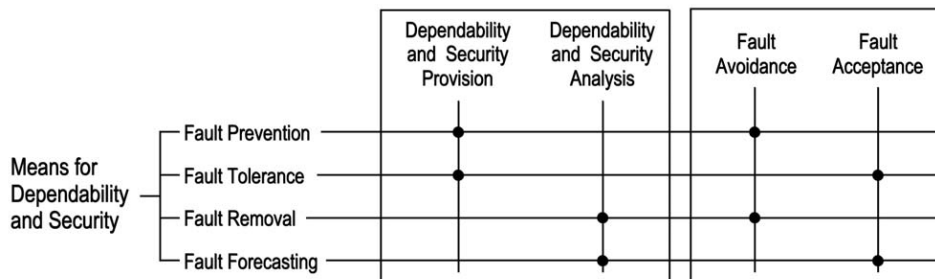


Figure 18: Groupings of the means for dependability and security (Avizienis, et al., 2004)

(Johnson, 2004) starts by recalling that safety and security share numerous attributes and recalls that there are three main ways to attempt to improve security, i.e. security surveys, risk assessment and vulnerability assess-

¹³ By contrast with (Corneillie, et al., 1999), (Firesmith, 2003) and (Altran Praxis, 2006), (Avizienis, et al., 2004) does not consider security as a sub-factor of dependability.

ments, the latter being usually the most effective. The author argues that vulnerability assessment techniques, traditionally used to improve security, can be applied to safety analysis: thinking like a malicious adversary can have benefits in identifying safety vulnerabilities. The attributes of an effective safety vulnerability assessment are discussed, and recommendations are offered for how such an adversarial assessment might work. The author concludes that a safety vulnerability assessment can potentially provide new insights, a fresh and vivid perspective on safety hazards, and increased safety awareness.

(Hessami, 2004) proposes a new paradigm for holistic systems assurance, of which safety performance and security/vulnerability are key aspects. While principally focused on safety assurance, the proposed paradigm is broadly applicable to any facet of a system's performance and goes beyond the current horizons of systems safety landscape. It develops and proposes a more inclusive approach and extension of current systems safety domain, comprising scope and issues beyond accident causation and consequential loss. It further advocates a more extensive view of loss, encompassing harm to people and damage to the natural habitat as well as detriment to a business enterprise or society at large.

Safety and security are critical to the US Department of Defence (DoD) and the Federal Aviation Authority (FAA), as well as to many other government and industry organizations. Both the Capability Maturity Model Integration (CMMI) and the FAA integrated Capability Maturity Model (iCMM) provide process improvement frameworks in which safety and security activities can take place. Yet some practices specific to safety and security were not necessarily addressed in these models, nor was there sufficient guidance for interpreting the models' practices in a safety and security context.

(Ibrahim, et al., 2004) identifies best safety and security practices for process improvement and appraisal use in combination with the two integrated capability maturity models: the iCMM, and the CMMI for systems engineering, software engineering, integrated product and process development, and supplier sourcing. The safety and security practices produced are based on widely recognized safety and security standards and sources, and harmonized to represent the commonality among the safety and security disciplines, where possible. A mapping is provided to (MIL-STD-882C, 1993), (MIL-STD-882D, 2000), (IEC 61508-1, 1998) - (IEC 61508-7, 2000) standard series and (DEF STAN 00-56, 1996) for safety, and (ISO/IEC 17799, 2000), (ISO/IEC 15408-3, 1999), (ISO/IEC 21827, 2002)¹⁴ and (NIST SP 800-30, 2002)¹⁵ for security.

<i>iCMM Implementing Practices</i>	<i>CMMI Implementing Practices</i>
<p><i>PA 13 Risk Management</i></p> <p>BP 13.02 Identify project risks by examining objectives, alternatives, and constraints in the context of established sources of risk.</p> <p>BP 13.03 Assess risks to determine their likelihood of occurrence and the consequences if they occur.</p>	<p><i>Risk Management (RSKM)</i></p> <p>RSKM SP 2.1-1 Identify and document the risks.</p> <p>RSKM SP 2.2-1 Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority.</p>

Figure 19: Identifying the best practices in iCMM and CMMI (Ibrahim, et al., 2004)

(Nicol, et al., 2004) starts by reviewing measures and existing techniques that are pertinent to dependability and security evaluation, giving examples of how those techniques are currently being applied to the evaluation of certain security properties. While these applications suggest that there is merit to using stochastic techniques to evaluate security properties, they also suggest that significant new work is necessary to create a sound, model-based framework for quantifying system security. At the highest level, the authors believe that this work falls into two categories: (i) modelling attacker behaviour – cf. Figure 20; and (ii) creating a single, comprehensive methodology for evaluating whether a design meets one or more high-level requirements related to security. The issues and challenges related to each of these needs are described. The authors conclude that stochastic evaluation techniques inspired by dependability evaluation methods have the potential to be used, with appropriate extension, for security evaluation, however, there are still significant obstacles to the creation of a comprehensive, integrated approach to the evaluation of multiple security properties, largely due to fundamental differences between the accidental nature of the faults and the intentional, human nature of cyber-attacks.

¹⁴ Now revised under (ISO/IEC 21827, 2008).

¹⁵ Now revised under (NIST SP 800-30, 2012).

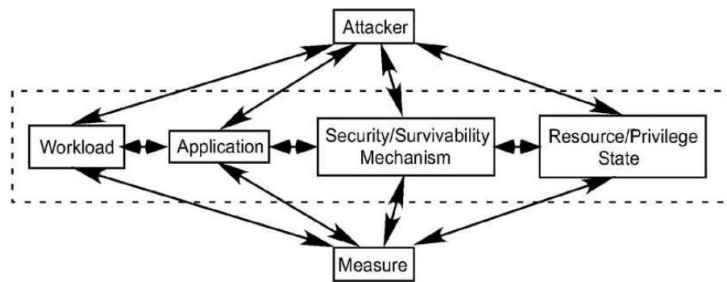


Figure 20: Probabilistic security model structure (Nicol, et al., 2004)

(Pfitzmann, 2004) recalls that in the past, IT-systems were at most either safety-critical or security-critical. The author asserts that in the future, more and more IT-systems will be both, safety- and security-critical. The paper provides the reasons behind that, but the author concludes that he can say neither how fast, nor at what levels (i.e. system specification, system architecture, or mechanisms) safety and security will merge.

(Rushdi, et al., 2004): see (Rushdi, et al., 2005) below.

(Srivatanakul, et al., 2004) demonstrates on an e-commerce case, that it is possible and beneficial to adapt the safety-related HAZard and OPerability (HazOp) approach to the traditional Use Cases modelling, so as to provide a more systematic approach for security analysis. Amongst the benefits, the authors assert that the HazOp approach: helps the derivation of security requirements and policy, highlights issues, can be applied to all Use Case elements, allows dealing with abstraction from communications that hides threats, and helps in the elicitation of attack patterns.

(Winther, 2004) addresses the necessity of including security aspects when assessing reliability and safety of critical systems. The integration of security in qualitative analysis is demonstrated and the possibility of probabilistically modelling security is discussed. Methods of particular interest are HAZard and OPerability (HazOp) and Petri-Nets.

(Horn, 2005) is an extension of the work proposed in (Sørby, 2003).

(ICAO, 2005) emanates from the work of the 5th Worldwide Air Transport Conference and draws four main conclusions: (i) economic liberalization as well as the evolution of business and operating practices have implications for safety and security regulation, which need to be addressed properly; (ii) existing International Civil Aviation Organisation (ICAO) provisions and guidance material regarding States' responsibility for aviation safety and security are generally adequate in addressing various situations resulting from liberalization, but more work could be undertaken to improve the existing Standards And Recommended Practices (SARPs) and/or guidance material to adapt to the evolution of business practices; (iii) safety and security must remain of paramount importance in the operation and development of international air transport and should at no time be compromised by economic considerations; and (iv) there is a need for all parties, governments and service providers, to realize the importance of having a clear understanding of their respective responsibilities for safety and security compliance and oversight.

Quantitative assessment of the effect of security breaches on a computer system can be based on the following: specification of all foreseeable types of basic events and estimation of their probabilities of occurrence over a stated period of time; observation of the various types of security measures employed by the system; definition of the undesired top events resulting from security breaches, and estimation of the system's vulnerability to each of these events as the cost incurred by the system if that event took place; mathematical modelling of the logical relations between the aforementioned entities. (Rushdi, et al., 2005) presents an adaptation of the fault-tree methodology to the quantification of security exposure of computer systems. In this context, a fault tree is described as a logic diagram whose input represents breach events at various system levels, and whose vertices represent logic operations or gates. The root or output of the fault tree can be any of the undesired top events. The authors briefly survey algorithms for converting the switching (Boolean) expression of the indicator variable for the top event into a probability expression. Once the top event probability is determined, it can be multiplied by the system's vulnerability to that event to yield a quantified value of the system's exposure to it. The authors also handle the doubly stochastic problem of estimating the uncertainty in the top event probability by using an analytic exact formula relating the variance of the top event probability to the variances of the basic

event probabilities. An example of a typical computer system is presented wherein numerical estimates are obtained for the top event probabilities and their variances and for the importance ranking of the various breach events.

(Schoitsch, 2005) starts by recalling that: (i) safety has a long tradition in many engineering disciplines, noting in particular that standards / methods of risk and hazard analysis, and certification methods have evolved long before IT; (ii) security has evolved quite recently with networked IT-systems and concerns about privacy, data integrity, authenticity and protection; (iii) both communities have developed their own standards, methods and system views; neither in standardization nor in application areas do they cooperate well. The paper takes a holistic view of critical systems and proposes a unified approach to system dependability, integrating both safety and security, arguing that in case of massively deployed embedded systems, security issues have severe safety impact and vice versa.

(Srivatanakul, 2005) investigates well-defined and systematic approaches from the safety domain that would potentially improve the security analysis process and thus the security of developed systems. This thesis takes inspiration from deviational techniques from the safety domain (such as HAZOP, FMEA, and software fault injection) and seeks to show that such techniques can be adapted for use in security, based on the Flaw Hypothesis Method framework. The techniques proposed are applied to different aspects of system design and to different levels on design notation rigour. The first technique of Rigorous Analysis of Security Requirements is based on use cases and HAZOP technique. It aims to provide a more rigorous approach to security requirement analysis at the start of the development. The second technique is the Security Zonal Analysis, which focuses on security problems arising from unfortunate interactions. The concept is derived from the zonal analysis technique used in safety, with the use of HAZOP-based guide words for possible channel identification. The third technique, Security Analysis of Formal Elements, challenges a formal specification to address issues of specification validation and the effects of failure. It applies the mutation method to derive potential deviants. Evaluation of the three techniques is illustrated through real-world case studies.

The SafSec project was funded by the MoD Defence Procurement Agency who wished to reduce the cost and effort of safety certification and security accreditation for future military avionics systems and in-service upgrades. The SafSec Standard does not supersede existing safety and security standards, but it helps to achieve the certifications with the minimum of duplicated work and the maximum of re-use of evidence between the different certifiers. SafSec focuses on dependable¹⁶ systems, therefore adding reliability and maintainability attributes to the baseline safety and security attributes.

The SafSec Standard (Altran Praxis, 2006) establishes a well-defined terminology, and defines the top-level goal "*The system is demonstrably dependable*" as the goal to be achieved to be compliant with the standard. The top-level goal is decomposed using the Goal Structuring Notation (GSN) into 17 requirements directed towards the demonstration of dependability (cf. Figure 21). SafSec is non-prescriptive and rather concise (44 pages). The associated Guidance expands on the objectives set out in SafSec with indications of how the objectives may be met while conforming to existing safety, e.g. (DEF STAN 00-56, 1996), and security standards, e.g. Common Criteria (ISO/IEC 15408-1, 2005).

¹⁶ Like (Corneillie, et al., 1999) and (Firesmith, 2003).

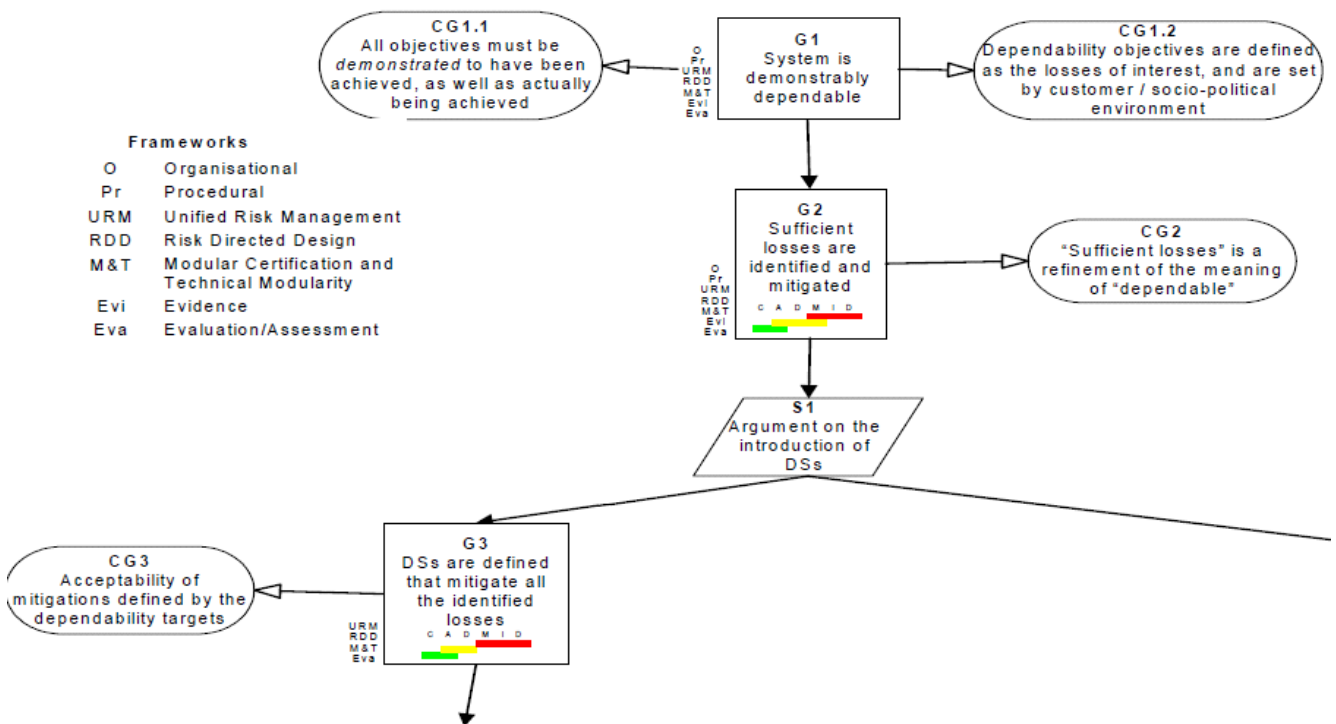


Figure 21: Extract of goal structure for the achievement of a dependable system (Altran Praxis, 2006)

(Contini, et al., 2006) starts by recalling that non-coherent fault trees characterised by non-monotonic structure functions allows easier modelling of complex top events. The availability of tools based on the Binary Decision Diagrams approach allows extending the fault tree analysis to applications requiring the construction of non-coherent functions as well as high basic events probabilities. Two examples are described. The first one, from the field of safety, shows that the possibility to use non coherent trees reduces the modelling effort for complex top events. The second example refers to a simple problem in the new field of security where the need of dealing with intentional actions implies the modelling of mutually exclusive events to which high probability values are associated. Some considerations about the interpretation of the importance indexes of basic events are also briefly described.

(Gorbenko, et al., 2006) gives results of a web services dependability analysis using standardized FMEA (Failure Modes and Effects Analysis) technique and its proposed modification IMEA (Intrusion Modes and Effects Analysis) technique. Obtained results of the FMEA-technique application were used for determining the necessary means of error recovery, fault prevention, fault-tolerance ensuring and fault removal. Systematization and analysis of web service intrusions and means of intrusion-tolerance were fulfilled by use of IMEA-technique. The authors also propose the architectures of the fault and intrusion-tolerant web services based on the components diversity and dynamical reconfiguration, and discuss principles and results of dependable and secure web services development and deployment by use of the F(l)MEA-technique and multiversion approach. See also (Babeshko, et al., 2008).

(Jonsson, 2006) is a position paper suggesting a high-level conceptual model that is aimed to give a novel approach to security and dependability definitions and terminology. The model defines security and dependability characteristics in terms of a system's interaction with its environment via the system boundaries and attempts to clarify the relation between malicious environmental influence, e.g. attacks, and the service delivered by the system (cf. Figure 22). The model is intended to help reasoning about security and dependability and to provide an overall means for finding and applying fundamental defence mechanisms. Since the model is high-level and conceptual it must be interpreted into each specific sub-area of security/dependability to be practically useful.

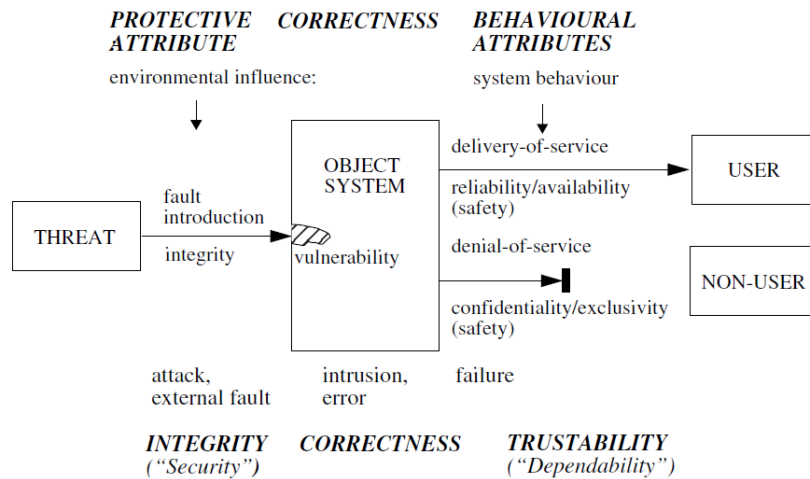


Figure 22: An integrated model of security and dependability (Jonsson, 2006)

(Line, et al., 2006) discusses some of the common properties and differences between terms and techniques in the safety and security communities with the aim of reconciling potential conflicts and exploring potential for cooperation, convergence and mutual benefits. This requires reaching an agreement on which terms to use and how to interpret them, and also on what techniques to use. The authors conclude that although the safety field has a longer track record, to be able to cover both aspects, one needs to adopt techniques from both fields — or possibly *merge* existing techniques or create new ones.

(Murdoch, et al., 2006) is a tailoring of the Practical Software and Systems Measurement (PSM) and ISO/IEC-15939 measurement framework to serve information needs relating to the security of software-intensive systems. Within this extensive document (67 pages), the authors introduce the concept of “aggregated security” of a system, which takes into account all the possible failures of components and services, in order to evaluate the overall security of the system, using a mix of attack trees and fault trees.

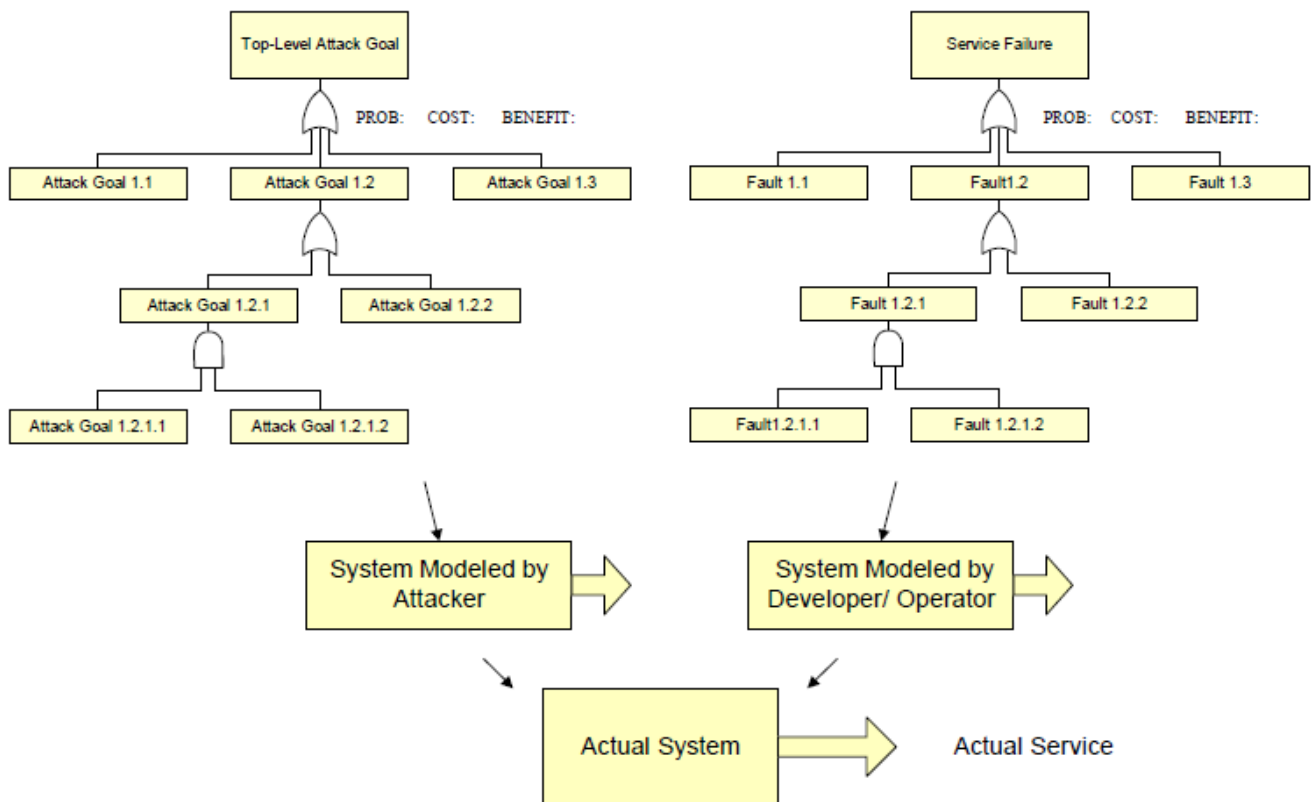


Figure 23: Fault trees and attack trees for a system as interpreted by developers and attackers (Murdoch, et al., 2006)

(Olive, et al., 2006) starts by recalling that in today's highly competitive air travel market, there is a growing demand among commercial airlines for on-aircraft systems, applications, and services that reduce airline operating costs, increase revenue opportunities, and improve the passenger experience. While many of these "new" aircraft functions may appear routine to users of the Internet, the inter-networking that is required both on and off the aircraft poses significant technical and operational challenges for airlines and their suppliers. Aircraft information security is one of the key challenges. This paper provides an overview of the Commercial Aircraft Information Security Concepts of Operation and Process Framework (ARINC 811, 2005) whose purpose is to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts. In a few pages, the paper summarizes the impact of information technology on airlines and aircraft systems, the need for aircraft information security, the need for standardisation, the aircraft information security concepts of operations (cf. Figure 24) including a reference architecture for the networked aircraft, and the three steps of the aircraft information security process framework.

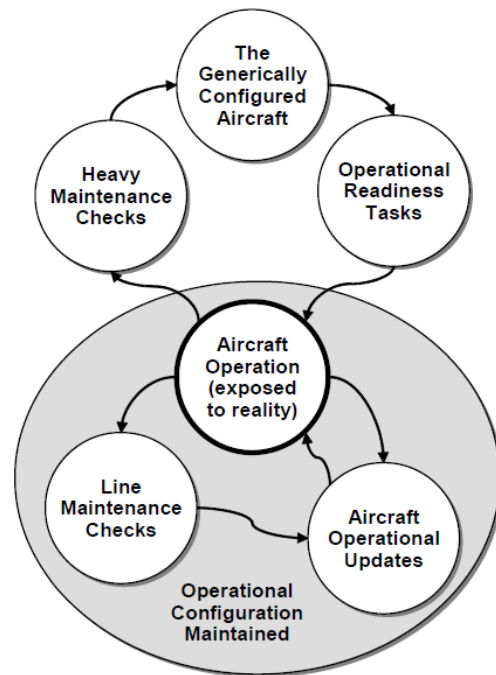


Figure 24: Aircraft Configuration Life Cycle (Olive, et al., 2006)

(Sallhammar, et al., 2006) presents a new approach to integrated security and dependability evaluation, which is based on stochastic modelling techniques. The proposal aims to provide operational measures of the trustworthiness of a system, regardless if the underlying failure cause is intentional or not. By viewing system states as elements in a stochastic game, the authors can compute the probabilities of expected attacker behaviour, and thereby be able to model attacks as transitions between system states (cf. Figure 25). The proposed game model is based on a reward-and-cost concept. A section of the paper is devoted to the demonstration of how the expected attacker behaviour is affected by the parameters of the game. The model opens up for the use of traditional Markov analysis to make new types of probabilistic predictions for a system, such as its expected time to security failure.

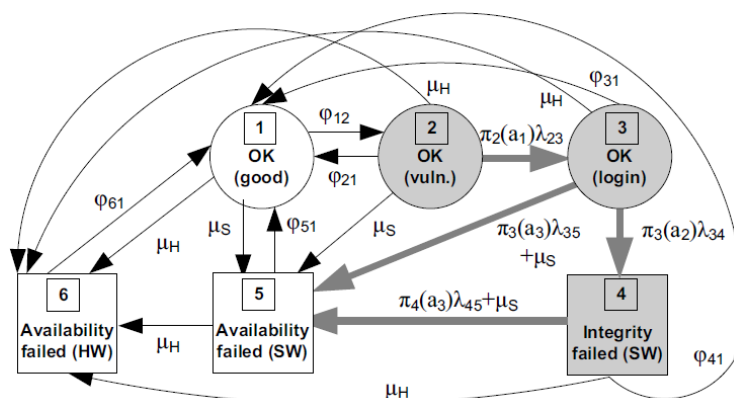


Figure 25: State transition model of DNS server with game elements identified (Sallhammar, et al., 2006)

(Stoneburner, 2006) is a very short paper (2 pages) proposing a common risk taxonomy for the National Institute of Standards and Technology (NIST) security risk framework and the Federal Aviation Authority (FAA) safety risk framework, in particular with a unified definition of mishap and an extended definition of hazard (cf. Figure 26).

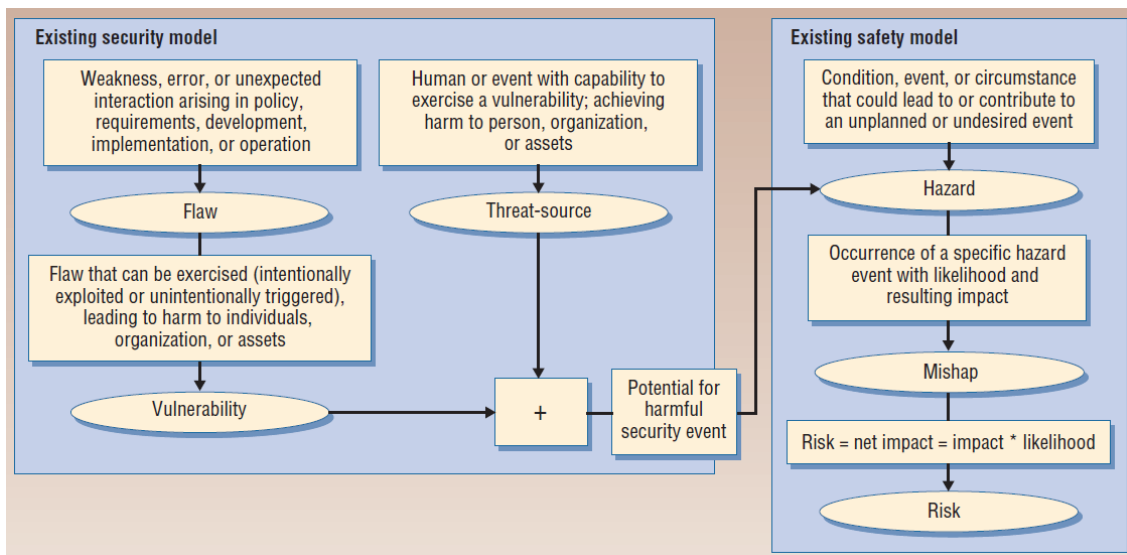


Figure 26: The unified security/safety risk framework (Stoneburner, 2006)

(Aven, 2007) and its re-edition in (Aven, 2011), starts by recalling that there have recently been several attempts to establish adequate risk and vulnerability analyses tools and related management frameworks dealing not only with accidental events but also security problems. These attempts have been based on different analysis approaches and using alternative building blocks. In this paper, the author discusses some of these and shows how a unified framework for such analyses and management tasks can be developed. The framework is based on the use of probability as a measure of uncertainty, as seen through the eyes of the assessor, and defines risk as the combination of possible consequences and related uncertainties. Risk and vulnerability characterizations are introduced.

(Cockram, et al., 2007) provides a practical case of application of the SafSec methodology, cf. (Altran Praxis, 2006) on a sanitised version of a command and control system that allocates the deployment of personnel within a battle-space. The example described in the paper applies this approach at a detailed level, using aspects of security to support the safety argument, and safety techniques to support security accreditation. The authors show an argument, which uses the dependability by contract approach, and how this is used. They show that module boundary contracts provide the process of specifying both types of attributes, and conclude that the goal structure notation is an appropriate method to demonstrate both safety and security arguments.

(D-MILS, 2007) is a Specific Targeted Research Project (STREP) of the 7th Framework Programme for research and technological development (FP7). Distributed MILS uses a Time-Triggered Ethernet (TTE) network to extend the MILS separation kernel into a distributed separation kernel.

(Grøtan, et al., 2007) describes a systematic approach, called SeSa for SecureSafety (cf. Figure 27), to assess whether a given technological solution for (non-diode) remote access to the Safety Instrumented Systems (SIS) of Norwegian offshore installations implies an unacceptable risk in terms of jeopardizing the Safety Integrity Level (SIL) of the SIS. The approach requires a “pre-structuring” of the remote access path (cf. Figure 28) and a few other hypotheses related to good engineering practices, but should be easily adaptable to other industrial domains. The approach extensively uses existing threat lists, the HAZard and OPerability (HAZOP) analysis and a mapping between the SILs defined in (IEC 61508-1, 1998) and Evaluation Assurance Levels (EALs) defined in (ISO/IEC 15408-1, 2005).

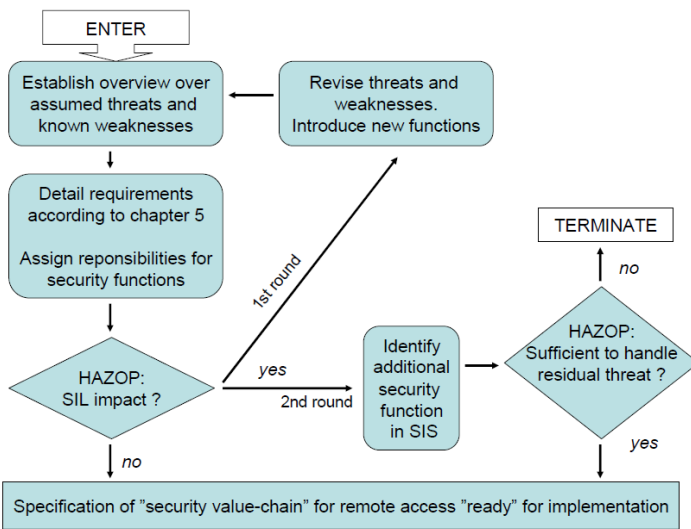


Figure 27: The SeSa method (Grøtan, et al., 2007)

(Novak, et al., 2007) presents a life cycle model which intends to harmonize safety and security for Building Automation and Control Systems (BACS). The authors start by presenting separately the main ideas of the safety (IEC 61508-1, 1998) - (IEC 61508-7, 2000) standard series, relative to electronic or programmable safety-related systems, on the one hand, and of the Common Criteria (ISO/IEC 15408-1, 2005), on the other hand. The paper builds upon (Stoneburner, 2006) but slightly differs from the latter in that Stoneberger specifies that the “potential for harmful security event” should be considered as a safety hazard (cf. Figure 26); here, the approach starts with IEC 61508 safety-related activities, and then addresses the security concern (cf. Figure 29). This is justified by the fact the safety standard is more precise and restrictive than the security standard, and also because safety requirements can have an irrevocable impact on the system architecture. In the end of the proposed life cycle, the dependencies, possible conflicts and trade-off between the concerns are addressed, without any specific technique, but simply using common sense.

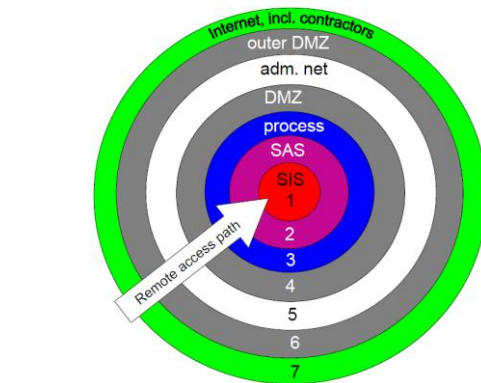


Figure 28: Layered model and remote access path to the SIS (Grøtan, et al., 2007)

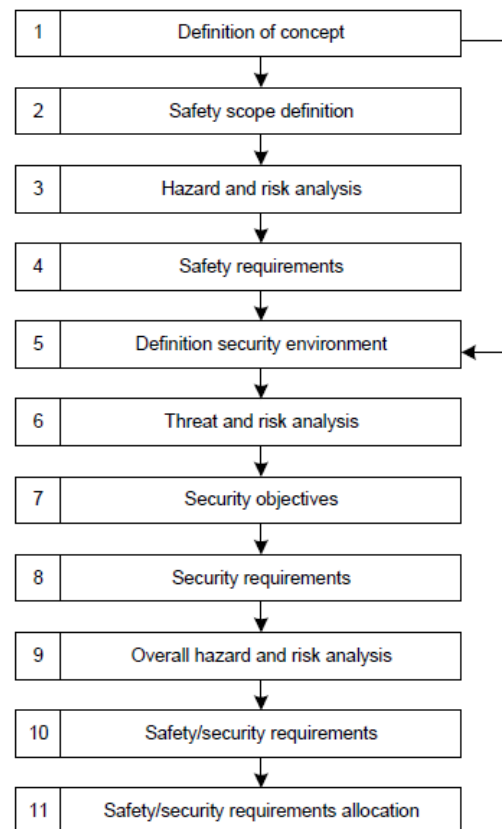


Figure 29: Pre-design of a safe and secure BACS (Novak, et al., 2007)

(Pan, et al., 2007a) is a short paper (3 pages) that defines functional safety and security, and studies the relationship (in terms of similarities, differences and dependencies) and influences (in terms of antinomy, homology and dependence) between the two.

(Pan, et al., 2007b) is slightly out of scope of this state of the art in that it addresses operation-time engineering activities to keep a system safe & secure during system operation and system maintenance (i.e. start-up, shut-

down, abnormal conditions, alarm management, etc.) rather than design-time engineering activities. It naturally covers human factors, cf. Figure 30.

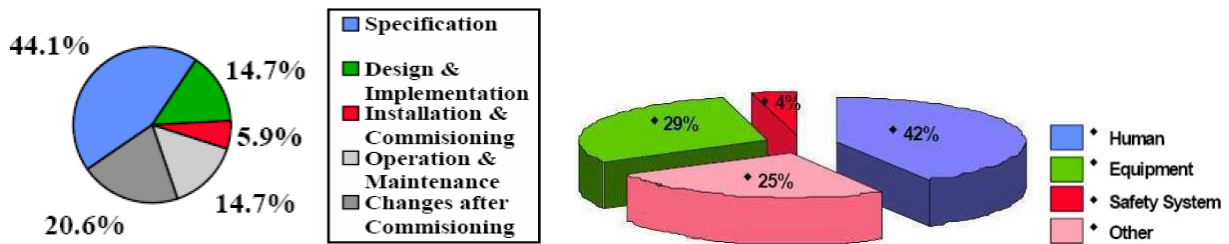


Figure 30: Cases of accidents (left) and Root causes of hazardous incidents (right) (Pan, et al., 2007b)

(Ridgway, 2007) recalls that whilst the achievement of safety objectives may not be possible purely through the administration of an effective Information Security Management System (ISMS), one’s job as safety manager will be significantly eased if such a system is in place. The paper seeks to illustrate the point by drawing a comparison between two of the prominent standards within the two disciplines of security and safety management, i.e. (ISO/IEC 17799, 2005) and (BS EN 61508-1, 2002).

Many papers tend to present safety-engineering as more mature than security-engineering, and thus propose to adapt safety-engineering techniques and processes to the security field. Taking the opposing view, (Sindre, 2007) looks at misuse cases, originally proposed for security, with the purpose of investigating whether they are also useful for safety, and to what extent they can complement existing diagrammatic modelling techniques in the safety domain. Misuse cases are thus compared to several traditional techniques for safety analysis, such as fault trees, cause-consequence diagrams, HAZard and OPerability (HazOp), and Failure Mode, Effects and Analysis (FMEA), identifying strengths and weaknesses of either.

(Wiander, 2007) analyses the implementation experiences of four organisations that have implemented the (ISO/IEC 17799, 2005) standard¹⁷. The core topic of the paper is out of scope of this state of the art, but it is worthwhile stating that two of the five interviewees “mentioned that the ISO/IEC 17799 (2005) standard does not adequately cover the corporate safety issues and there is no link to them.”

(Yang, et al., 2007) explores a framework of safety and security checking for internet-based control systems. After identifying the similarity between safety and security, the authors applied the safety-related *What-If* method to security risk analysis (cf. Figure 31). A modified Process Control Event Diagram¹⁸ (PCED)-based HAZard and OPerability¹⁹ (HAZOP) analysis is proposed.

<i>If</i>	<i>What</i>	<i>Actions</i>
Scenario 1: Firewall and password control are broken.	Attackers obtain the access to the control system	Action 1: Disconnect the external link of the local control system with the internet if the intrusion is detected
Scenario 2: Attackers have modified control parameters	Disturbances have been introduced into the process	Action 2: A safeguard system filters out any abnormal change to the local control system
Scenario 3: Attackers have created safety critical conditions	A fatal accident might be happening	Action 3: An emergency SIS is required to be automatically activated

Figure 31: What-If reviews (Yang, et al., 2007)

(Babeshko, et al., 2008) presents results of a SCADA-based ICS dependability and security analysis using a modification of standardized FMEA (Failure Modes and Effects Analysis)-technique. The technique mentioned

¹⁷ (ISO/IEC 27002, 2013) has developed from BS 7799, published in the mid-1990s. The British Standard was adopted by ISO/IEC as (ISO/IEC 17799, 2000), revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27k-series standards.

¹⁸ A PCED is an abstract and qualitative model of the communication between processes, controllers and operators.

¹⁹ As in (Foster, 2002).

takes into account possible intrusions and is called F(I)MEA (Failure (Intrusion) Modes and Effects Analysis). The F(I)MEA technique is applied for determining the weakest parts of ICS and the required means of fault prevention, fault detection and fault-tolerance ensuring. An example of F(I)MEA-technique applying for SCADA vulnerabilities analysis is provided. The solutions of SCADA-based ICS dependability improvement are proposed. See also (Gorbenko, et al., 2006).

(Boettcher, et al., 2008) describes the Multiple Independent Levels of Security (MILS) approach developed as part of the Multiple Independent Levels of Security / Safety initiative of the Air Force Research Laboratory (AFRL). MILS is a high-assurance architecture for secure information sharing that builds on and extends a long tradition of work on architectural approaches to security and safety. Its mechanisms are closely related to the *robust partitioning* employed for safety in Integrated Modular Avionics (IMA), and to the *separation kernels* employed in some secure systems. MILS is characterized by a two-level approach to secure system design: (i) at the policy level, a decomposition to a virtual architecture is performed while identifying the trusted components, the local policies and the communications channels; (ii) at the resource sharing level, implementation of components is considered, which includes the allocation of components to shared physical resources. Security is seldom identified with a single, simple policy; the two-level approach of MILS was introduced as a rational way to organize the multiple cooperating components and sub-policies that realize a complete secure system (cf. Figure 32).

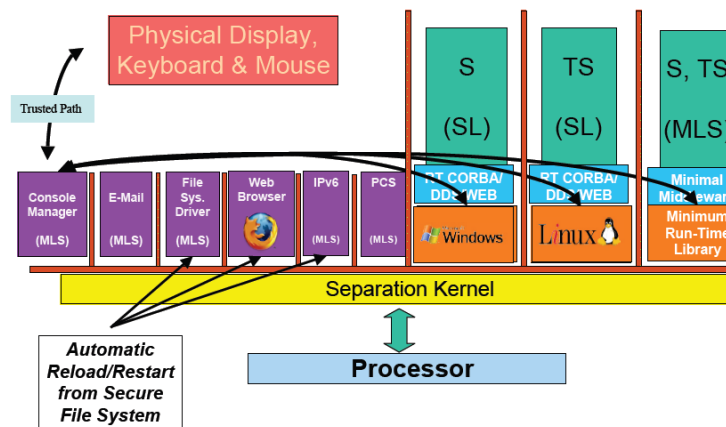


Figure 32: Conceptual Design for a MILS Workstation (Boettcher, et al., 2008)

(Daniel, 2008) is a humorous and cartoon-illustrated history of safety and security convergence, from the 1940's to present time (cf. Figure 33). However, beyond the humour, the author raises 12 fundamental points, all with a strong "think different" baseline:

(1) security, by principle, is human factors related; (2) an engineering solution to security is an illusion; (3) security is an eternal process comprising varying activities, using varying mechanisms, with evolving technologies; (4) policies help keep decision-makers straight; (5) applying mathematics to security may be dangerous; (6) catalogues, forms, check-lists... are good to know for the attacker; (7) the safety-related "proven-in-use" concept is like 9/11 when applied to security; (8) good practice is common sense, but is not enough; (9) never underestimate attacker imagination; (10) manufacturer, integrator and operator issues are a market side-issue; (11) an appropriate threat-risk-analysis method is still missing; and (12) a "good" industrial security standard is still missing.



Figure 33: Genesis of the safety-related security problem: loss of the engineer's paradise (Daniel, 2008)

(Deleuze, et al., 2008) addresses the issues resulting from the concomitant allocation of safety and security objectives to an industrial facility. The authors analyse the liaison between the concepts of security and safety. They attempt to describe the possible disconnections or even contradictions between them, as well as the benefits expected from increased disciplinary exchanges between safety and security studies. The first section of the paper introduces to key security challenges and threats in industrial facilities. The second section briefly reviews, on the basis of available literature, the major differences between a safety study and a security assessment for a given industrial facility. The third section discusses the boundary conditions for security-related application of probabilistic and deterministic risk assessment methodologies usually applied in safety studies. The

fourth section presents situations where safety and security objectives appear to have been inconsistent. Examples include: risks caused by false alarms, increased complexity of operating procedures, risks caused by active security measures, negative effects of barriers accumulation, competing rationalities or paradigms... The authors conclude that safety and security objectives are not easily compatible on an industrial facility and those innovative scientific paradigms and methods need to be developed so that operators of industrial facilities can consider a more integrated approach.

(Dewar, 2008) is the introduction to the *Relationship between Safety and Security in Software-Based Systems* workshop. It starts by recalling some basics on safety-critical systems, with a safety focus on (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992), and a security focus on the Common Criteria, i.e. (ISO/IEC 15408-1, 2005), (ISO/IEC 15408-2, 2008), and (ISO/IEC 15408-3, 2008). The paper then compares the two. To catch the reader's attention on the implications of Evaluation Assurance Levels (EAL), the author raises a striking example: various versions of Microsoft Windows (e.g. Windows 2000 at SP3) are certified at EAL4, i.e. in some respects equivalent to DO-178B Level A. The author then analyses the relations between safety and security, and compares the merit of testing with respect to safety and security properties, with a focus on formal methods and object-oriented techniques, with in particular the Liskov Substitutability Principle (LSP²⁰). He concludes that things are starting to move in terms of safety and security co-engineering.

(Jackson, et al., 2008) presents the SafSec Standard (cf. (Altran Praxis, 2006) and Figure 34), and the safety and security regulatory shifts that occurred in parallel to the elaboration of SafSec.

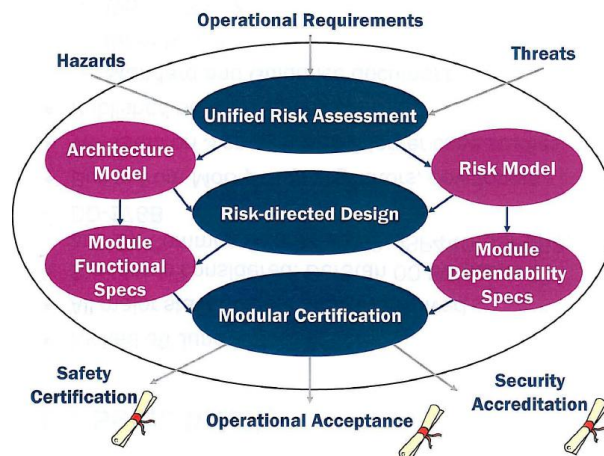


Figure 34: The SafSec approach (Jackson, et al., 2008)

The European Modular Urban Transport Safety and Security Analysis (MODSafe, 2008) project was launched in September 2008 with the goal of undertaking research on the safety life cycle of urban guided transport systems in Europe, taking on board some security considerations.

(Nordland, 2008) recalls that safety engineers tend to regard security as outside the scope of their task, and presents multiple examples of safety-critical systems that are increasingly exposed to malevolent attacks. The paper does not present any approach or solution, but simply suggests that engineers take the bull by the horns.

(Saglietti, 2008) briefly summarizes the classical differences and historical trends in analysing safety and security demands. After a brief survey on terminology, the paper proposes a uniform view to both safety and security attributes on which to base common verification and validation activities; one of the means to achieving that goal is by recommending an effect-driven engineering approach rather than a cause-driven approach. In contrast with (Dewar, 2008), the author feels that both safety and security-critical systems require extensive testing, achieving high white-box and integration coverage measures, preferably supported by an automatic generation of test data capable of achieving as high (i.e. control flow / data flow / interaction) coverage as possible, with as little validation effort as possible.

²⁰ Substitutability is a principle in object-oriented programming, which states that, in a computer program, if S is a subtype of T, then objects of type T may be replaced with objects of type S without altering any of the desirable properties of that program. The Liskov Substitution Principle (LSP) is a particular definition of a subtyping relation, which intends to guarantee semantic interoperability of types in a hierarchy [Wikipedia].

(Stålhane, et al., 2008) builds upon (Sindre, 2007), assessing the efficiency of misuse cases²¹ applied to safety hazard identification, based on an experiment with students. The respective merits of the textual and diagrammatical parts of misuse cases are compared, showing that the textual part of misuse cases is better for producing more failure modes (cf. Figure 35).

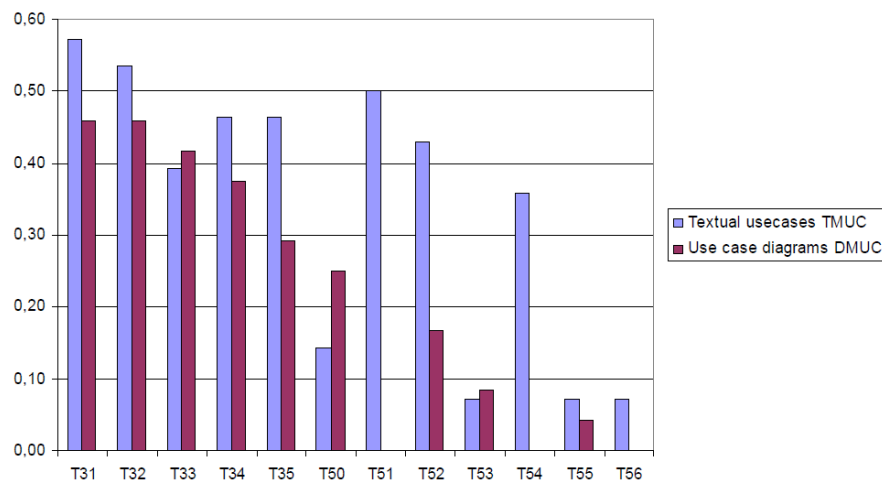


Figure 35: The probability of identifying each failure mode (Stålhane, et al., 2008)

The French FUI SEISES²² project (SEISES, 2008) was defined regarding a context, challenges and needs that are specific to computerized on-board systems, in particular those integrated in aeronautical, space, transport systems and / or critical infrastructure. The SEISES project has been implemented in order to offer the relevant industries a standard that integrates safety and security alike. The English terms “safety” and “security” have been chosen in order to avoid ambiguity in their understanding by the various business areas involved in the project for which the French translations may differ. These terms are understood as follows:

- safety: operational safety and security of goods and people;
- security: information security against malicious intent.

SEISES is to develop a framework integrating the safety and security practices and processes within the life cycle of the on-board computerised systems, single components and related resources. This framework designed for the on-board systems is based on the Common Criteria, and gives it a practical application in this field. The project objectives are to ensure the coherence of practices and to facilitate the activities of design, development, evaluation, validation and maintenance of safe and secure systems (including security functions). The main goal with respect to the existing literature (SAE ARP 4761A, 2004), (SAE ARP 4754A, 2010) / (EUROCAE ED-79A, 2010), (RTCA DO-254, 2000) / (EUROCAE ED-80, 2000), (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992), (ISO/IEC 15408-1, 2009), etc. can be summed up with the idea to integrate security within the safety practices. SEISES also aims at completing and harmonizing the existing standards in both areas by providing a platform of integrated and toolled practices, directly applicable to the aeronautical and space domains. This approach enables, throughout the different life-cycle phases of the on-board systems, an optimized implementation of the provisions that enable the control of hazards and threats and the management of risks, also taking into account the notion of impact (human, material, economic, image, legal and regulatory, terrorism, etc.)

In 2008, the German Federal Ministry of Education and Research (BMBF) launched the Virtual and Augmented Reality for Maximum Embedded System Safety, Security and Reliability project (ViERforES, 2008). Virtual reality (VR) and augmented reality (AR) technologies are employed in the ViERforES project to reproduce and experience non-physical properties of distributed embedded systems in virtual environments. New tools and methods provide engineers support to test and perfect products safely in every phase of the life cycle.

²¹ Misuse cases extend standard UML use cases. Misuse cases were developed to address security concerns through the specification of behaviour that the system should avoid, and the modelling of how a misuser can damage the system.

²² SEISES is a French acronym for Systèmes Embarqués Informatisés, Sûrs Et Sécurisés. In English: On-board Safe and Secure Computerized Systems Platform. The description provided herein for the SEISES project is extracted from the *State of the Art of Security and Privacy Policies – Standardisation*, deliverable D11.1.3, FP7 SECUR-ED project, June 2013.

(Aven, 2009) discusses the rationale for the different initiatives taken to identify safety and security critical systems and activities, at different levels and in different contexts, ranging from infrastructures at the societal level to equipment on the production plant level. These different approaches are implemented to define the critical systems and activities. Some of these relate to vulnerabilities, others incorporate the probability dimension and are risk based, whilst yet others take into account values of the decision-maker and relevant stakeholders. The paper discusses: (i) if vulnerability is an adequate measure to be used as a basis for determining criticality; (ii) if it is meaningful to specify safety and security critical systems and activities without addressing risk; (iii) how the limitations of the risk assessments should be accounted for; (iv) if the concept of criticality should be extended to also cover utility aspects. The author brings new insights into the discussion by being precise on the key risk concepts, including uncertainty, probability and expected value, and considering alternative risk perspectives. The author's main concern is activities with potential severe consequences and large uncertainties. A novel approach is suggested based on expected values and uncertainties in underlying phenomena and processes. In order to account for uncertainties, the author suggests the following method: (1) identify a list of systems for evaluation; (2) identify possible initiating events A; (3) define categories of consequences C (i.e. severity classification); (4) rank the systems according to vulnerability using $E[C|A]$, i.e. the expected consequences given the occurrence of A; assign probabilities for the events A, calculate the unconditional expected consequences, EC, by $EC = P(A) \times E[C|A]$, and rank the systems according to EC; (5) assess uncertainties in underlying phenomena and processes that could result in surprises relative to EC, and adjust the ranking based on this assessment. Steps 4 and 5 are based on a traditional risk description. It is only when the uncertainties are added that "true" risk is revealed, e.g. an event with a presumed low risk based on EC, may be reclassified as high risk if the uncertainties regarding the underlying assumptions are high. Uncertainties may be related to e.g. new technology, future events, customer demand or political stability.

(Daruwala, et al., 2009) presents a case of practical implementation of a recommendation found in many other papers, i.e. apply safety-related techniques to security engineering. The authors successfully applied the HAZard and OPerability (HazOp) technique to security threat identification on Intel hardware and software. The paper reports significant efficiency²³ gains compared to traditional approach based on brainstorming, interface exposure and analysis of privilege levels, as used on equivalent systems (cf. Figure 36).

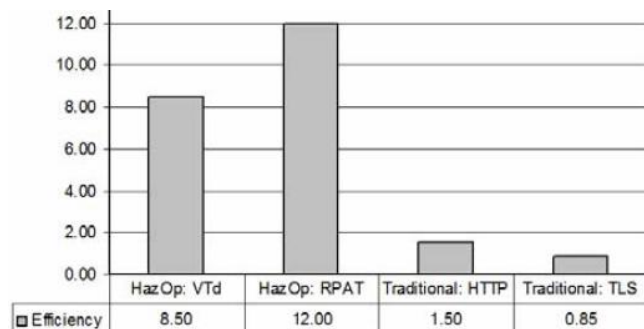


Figure 36: Test derivation efficiency, comparing HazOp with traditional approaches (Daruwala, et al., 2009)

It is to be regretted that (Daruwala, et al., 2009) does not reference (Foster, 2002), in which it is reported that the HazOp technique has already been successfully applied to security protocol development, especially since both papers report somehow contradictory results, i.e. increased efficiency for (Daruwala, et al., 2009), versus considerable effort but increased coverage for (Foster, 2002). Positive feedback about HazOp is also provided in (Winther, et al., 2001), (Srivatanakul, et al., 2004), (Yang, et al., 2007), (Cusimano, et al., 2010), (Raspotnig, 2014).

²³ Efficiency is expressed in terms of number of test cases identified per week.

(Fovino, et al., 2009) presents a new method for quantitative security risk assessment of complex systems combining fault-tree analysis, traditionally used in reliability analysis, with attack-tree analysis, proposed for the study of malicious attack patterns. Formal definitions of fault tree and attack tree are provided.

Tree integration is realised through the equation *Attack tree goal = Fault tree event*, showing the fact that a top goal of an attack tree coincides with an event contained in a fault tree. The resulting tree is called Extended Fault Tree (EFT).

According to the authors, the combined use of fault trees and attack trees helps the analyst to effectively face the security challenges posed by the introduction of modern ICT technologies in the control systems of critical infrastructures. The proposed approach allows considering the interaction of malicious deliberate acts with random failures.

The quantitative analysis is possible under the precondition that probabilities are available for both safety and security events. A mathematical model for the calculation of system fault probabilities is presented.

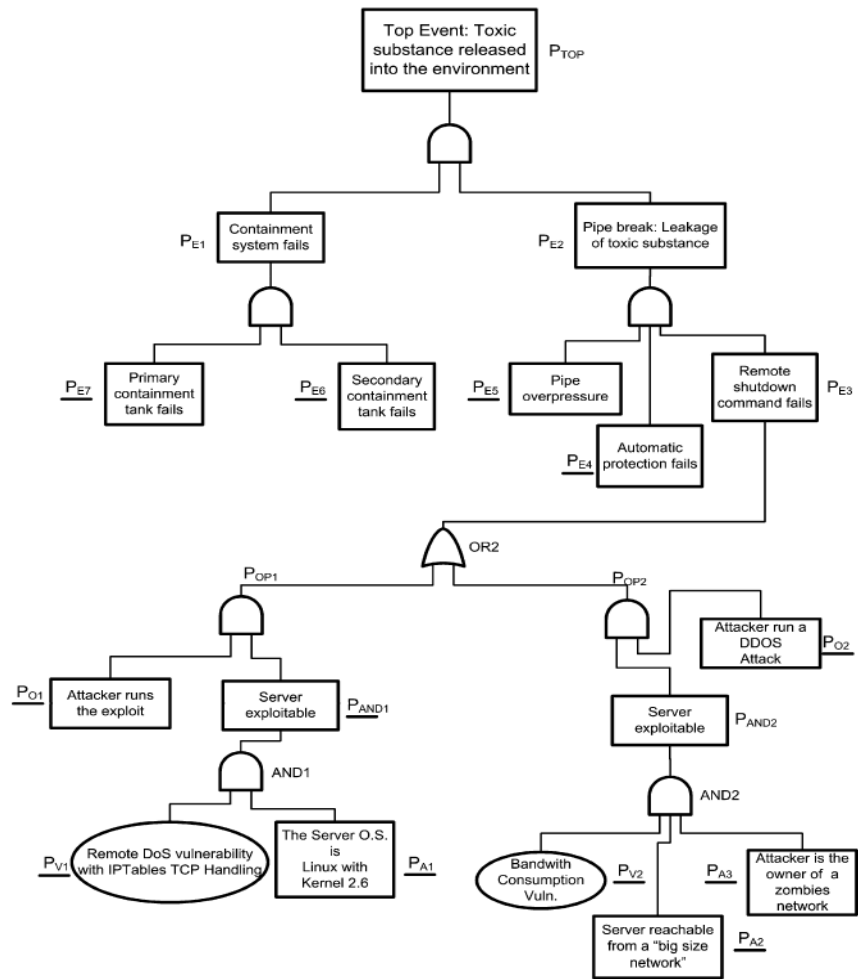


Figure 37: Integrated fault tree and attack tree (Fovino, et al., 2009)

(Goertzel, et al., 2009) recalls that security concerns, long recognized and addressed for information systems and networks, have only recently emerged as relevant to safety-critical software-intensive systems. As these systems move away from closed environments and architectures to network connectivity and open and commodity technologies, they are exposed as never before to security threats that are familiar in the information systems realm. Security has become as necessary a property as high-reliability and fault-tolerance. On the information systems side, in Department of Defence parlance, fought on current terms, the information war is not only being lost, it is unwinnable. The “detect-protect-respond” paradigm is “broken”, and there is a new strategy that shifts information assurance, computer network defence, and cyber security from attack prevention and pre-emption towards the ability to “fight through”, i.e. survive attacks. Survivability (resilience) is now the common thread running through both security-critical and safety-critical software engineering. Secure software developers need to adopt and adapt reliability and safety engineering techniques and tools to achieve survivability objectives in their larger, more complex information system programs and applications. Software safety engineers need to strike the balance between the emerging need for security and the unique imperatives of safety-critical software, and leverage tools and best practices originating in the information and software assurance communities.

(Hansen, 2009) shows that most standardized safety protocols do not provide sufficient security measures, and represent a weak link in the design of safety systems. The author assumes that safety systems are designed and used according to the (IEC 61508-1, 1998) - (IEC 61508-7, 2000) standard series. A systematic overview of the possibilities and difficulties of attacking safety devices is provided (cf. Figure 38). The paper shows that the probability that a hostile hacker obtains access to a safety device and compromises the safety function in the device is small; the most likely outcome is bringing the system to a failsafe state, harming the availability, rather than the safety.

	Find bug	Avoid timeout	Find exploit	Access SIL code from non-SIL code	Find dual fault	Find dual exploit
(1) Black Channel	x	x	x	x		
(2) Other protocols	x		x	x		
(3) Normal application	x		x	x		
(4) Safe protocol	x	x	x		x	x
(5) Safe application	x	x	x		x	x

Figure 38: Safety device attack entry points versus hacker challenges (Hansen, 2009)

(Hunter, 2009) starts by recalling that treating safety and security activities independently in the system lifecycle can lead to unexpected and unwanted outcomes, illustrated by the Maroochy Cyber Attack real-life example. The author stresses that before attempting to integrate two value-based systems, it is important that their value systems are aligned. When it comes to safety and security the values and priorities that drive the methodologies are not the same, typically assets versus people, and safety integrity versus security priorities. Then, the paper highlights two key issues that limit the success of integrating safety and security in the systems lifecycle: incompatibility with risk management; and possible conflicts with mitigating controls. The author recommends using the safety Layer-Of-Protection Analysis (LOPA) technique to allow the determination of probability of security control failure and resulting dangerous failure probability, as well as the use of Goal Structuring Notation (GSN) or similar techniques where safety and security controls may conflict. Rather than combining disparate methodologies for safety and security, the paper proposes Lifecycle Attribute Alignment to ensure effective and compatible safety and security controls are established and maintained at key lifecycle stages. In Figure 39, interaction in these phases is shown in terms of alignment attributes (A), requirement allocation attributes (R) and verification effectiveness attributes (V). The author's hope is to influence the upcoming (S + IEC 61508, 2010).

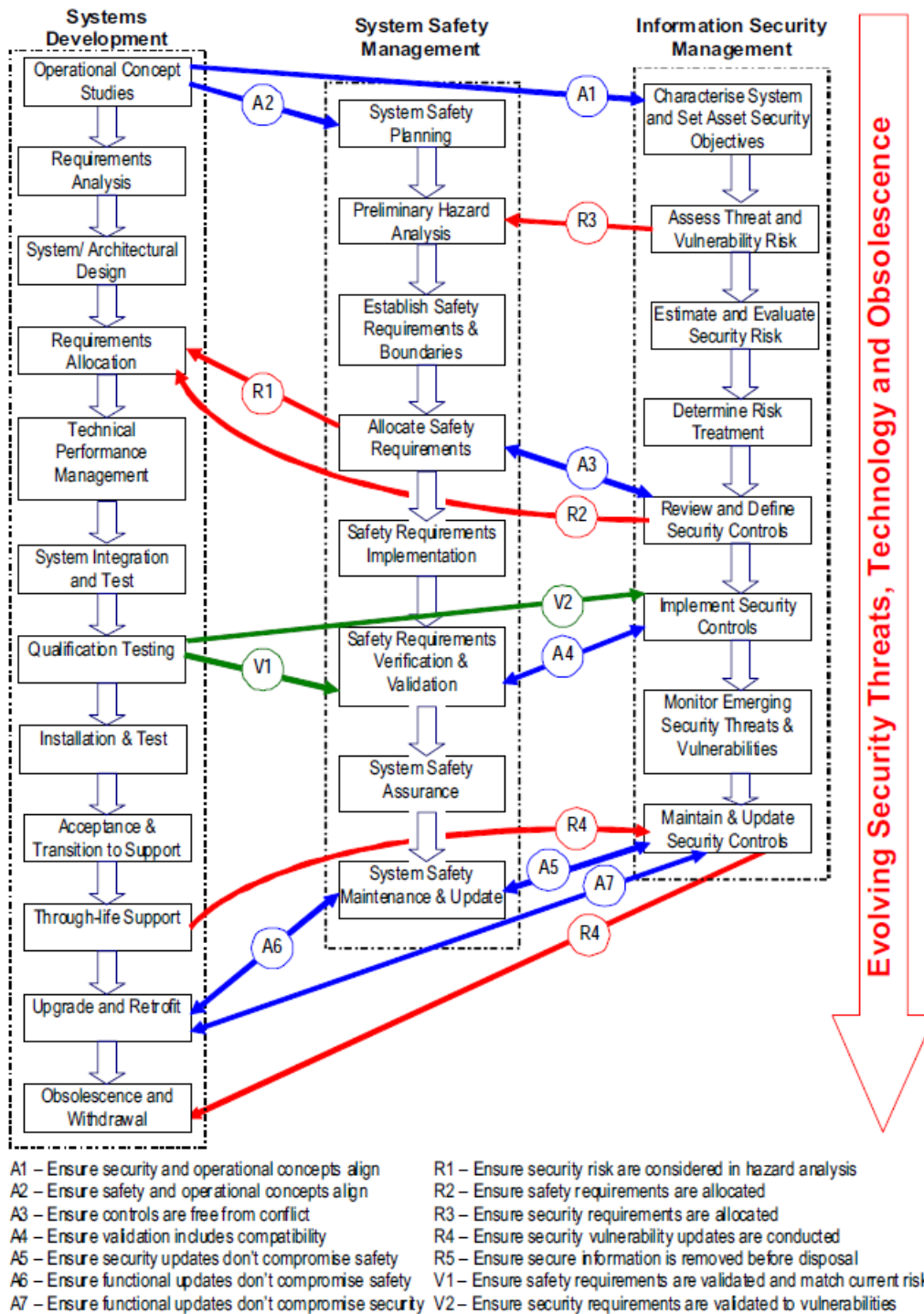


Figure 39: Key lifecycle alignment points (Hunter, 2009)

(Jalouneix, et al., 2009) compares nuclear safety and security, discussing goals and context, organisational principles, including the higher weight of the State in security affairs with respect to safety, and application principles.

The French *Production d'Applications Réparties Sûres pour l'Embarqué Critique*²⁴ FUI 8 project (PARSEC, 2009) aimed at providing development tools for critical real-time distributed systems requiring certification according to the most stringent standards such as the (RTCA DO-178B, 1992) in avionics, the (IEC 61508-1, 1998) - (IEC 61508-7, 2000) standard series in transportation or the Common Criteria (ISO/IEC 15408-1, 2009) - (ISO/IEC 15408-3, 2008) for Information Technology Security Evaluation. In more detail, PARSEC aimed at meeting the following specific requirements of these systems (cf. Figure 40):

²⁴ French for "Production of Secure Distributed Applications for Critical Embedded Systems".

- proven specification of the system (→ Event-B approach);
- means to translate this proven specification to a component model (→ MyCCM-HI technology describing the application and its non-functional requirements, e.g. real-time characteristics or description of the projection of the on a partitioned platform);
- correct-by-design code (→ the synchronous approach using the SynDEX tool and the asynchronous approach using the Ocarina tool);
- integration of the PathCrawler test scenario generation and execution tool, and definition of a requirement traceability survey tool.

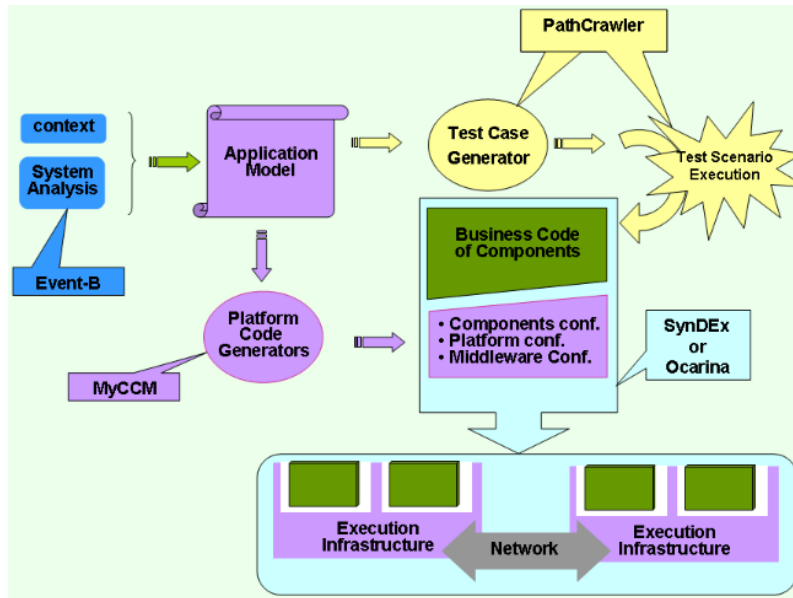


Figure 40: The FUI 8 PARSC project (PARSEC, 2009)

Building upon (Line, et al., 2006), (Piètre-Cambacédès, et al., 2009) aims at a finer understanding of the relations between safety and security, introducing a conceptual framework to better capture their moving perimeters. The framework is called SEMA for System vs. Environment & Malicious vs. Accidental (cf. Figure 41). The framework characterizes safety and security interactions, varying from their reinforcement to their strong antagonism. In following papers, the framework was extended, as security and safety were broken down into 6 concepts: defence, safeguards, self-protection, robustness, containment ability and reliability, cf. (Piètre-Cambacédès, 2010f) (Piètre-Cambacédès, et al., 2010c).

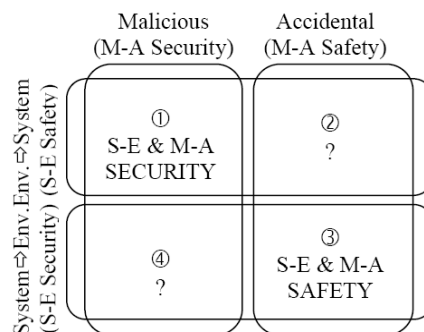


Figure 41: The SEMA framework (Piètre-Cambacédès, et al., 2009)

(Sun, et al., 2009) recognises that modern cyber-physical systems (CPSs) are increasingly prone to security violations, often as a result of contradictory requirements between the safety / real-time properties and the security needs of the system. The authors propose a formal framework that assists designers in detecting such conflicts early, thus increasing both, the safety and the security of the overall system. The framework (cf. Figure 42) includes: (i) an extensible global language to specify the system and environment; (ii) mechanisms to specify domain requirements; (iii) mechanisms to relate requirements across classes; (iv) brute force search through all

possible valid models of the world that satisfy the initial assumption to find conflicts between requirement classes. The paper focalises on CPSs, but the formal framework seems applicable to any type of complex system.

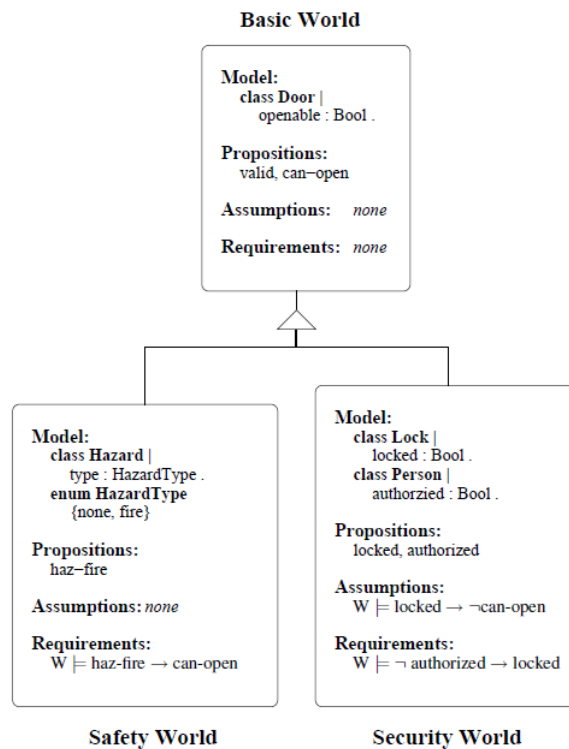


Figure 42: Different domain models of the world (Sun, et al., 2009)

(Aprville, et al., 2010a) presents the AVATAR SysML profile. The set of slides recalls the history of the AVATAR language, presents its syntax and semantics, and illustrates the verification of safety, confidentiality and authenticity properties on a simple coffee machine example. See also (Knorreck, et al., 2010), (De Saqui-Sannes, et al., 2011), (Pedroza, et al., 2011) and (Aprville, et al., 2014).

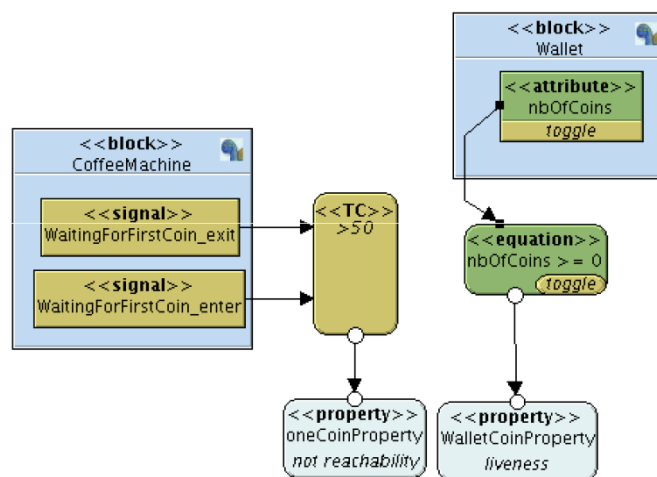


Figure 43: Example of parametric diagram using AVATAR (Aprville, et al., 2010a)

(Carter, 2010) is the minutes of a “safety-critical versus security-critical software” workshop. The aim of the workshop was to bring relevant British experts from industries, universities, government and associated organisations, and professional bodies together in order to debate real-life problems of safety and security-critical software, technical similarities and differences between safety and security, how processes and working practices can be combined, how skills can be swapped, what are the barriers to implementing safety-security systems as one discipline, and what is needed to change standards. The workshop concluded on three main recommendations: (i) the security domain would benefit from using software development techniques from the

safety domain; (ii) the safety domain would benefit from considering malicious attack on its systems; and (iii) safety and security-critical systems should be considered as one. An action plan was drafted, but as yet, we have found no evidence of its execution.

(Cusimano, et al., 2010)²⁵ is a pragmatic feedback on safety and security co-engineering in the Industrial Automation and Control Systems (IACS) domain. The approach, applied on a major U.S. refinery, combines, amongst other techniques, a HAZard and OPerability (HAZOP) analysis, a Control HAZard and OPerability (CHAZOP) analysis, a Failure Modes and Effect Analysis (FMEA), and a Layer-Of-Protection Analysis (LOPA).

(Delange, 2010) starts by explaining the need to cope with security in dependable systems and proceeds with a review of the basic approaches currently used in each specialty, i.e. Multiple Independent Levels of Security (MILS)²⁶, security policy models (e.g. Bell-Lapadula, Biba), cryptography and Common Criteria (ISO/IEC 15408-1, 2009) for security engineering versus Failure Propagation and Transformation Calculus (FPTC) / HAZard and OPerability (HAZOP), partitioning and health monitoring as of ARINC 653²⁷, and (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992) for dependability. The thesis highlights the commonalities of the mechanisms developed in each specialty for different purposes, notably partitioning, but also code analysis and code generation techniques. A critical review points out four issues: (i) absence of a common framework for safety and security; (ii) inconsistencies & spread-out of system specifications in different documents; (iii) absence of relation between validated specifications and code; (iv) lack of automation during the development cycle. Based on this critical review, the author introduces a new method to build dependable systems whilst ensuring their security requirements. The approach is based on: (a) the Architecture Analysis and Design Language (AADL) as unique representation language, cf. Figure 44; (b) automated validation of the specifications; (c) code generation for execution on an open-source partitioned operating system (POK Community, 2011); (d) automated certification, which verifies that specification requirements are met in the implementation by analysing the system during its execution and also evaluates its compliance against certification standards. The author provides AADL extensions to model partitions (cf. Figure 44) and the propagation of errors, as well as validation rules that operate on those extensions.

```
processor kernel
end kernel;

processor implementation kernel.i
subcomponents
p1 : virtual processor environnementpartition.i;
p2 : virtual processor environnementpartition.i;
properties
Slots      => (100ms,200ms);
SlotsAllocation => (reference(p1),reference(p2));
Major Frame      => 300ms ;
end kernel.i;
```

Figure 44: AADL processor component extended to model a partition kernel

(Derock, et al., 2010) proposes a high-level comparison of the safety-related (ISO/IEC 15026, 1998) and the security-related (ISO/IEC 27005, 2008) standards. The paper also presents an overview of a generalized safety process developed at DCNS that covers all the activities mandated in the two aforementioned standards (cf. Figure 45).

²⁵ See similitude of title with (Dewar, 2008).

²⁶ See (Boettcher, et al., 2008).

²⁷ Cf. (ARINC 653P0, 2013), (ARINC 653P1-3, 2010), (ARINC 653P2-2, 2012), (ARINC 653P3A, 2014) and (ARINC 653P4, 2012).

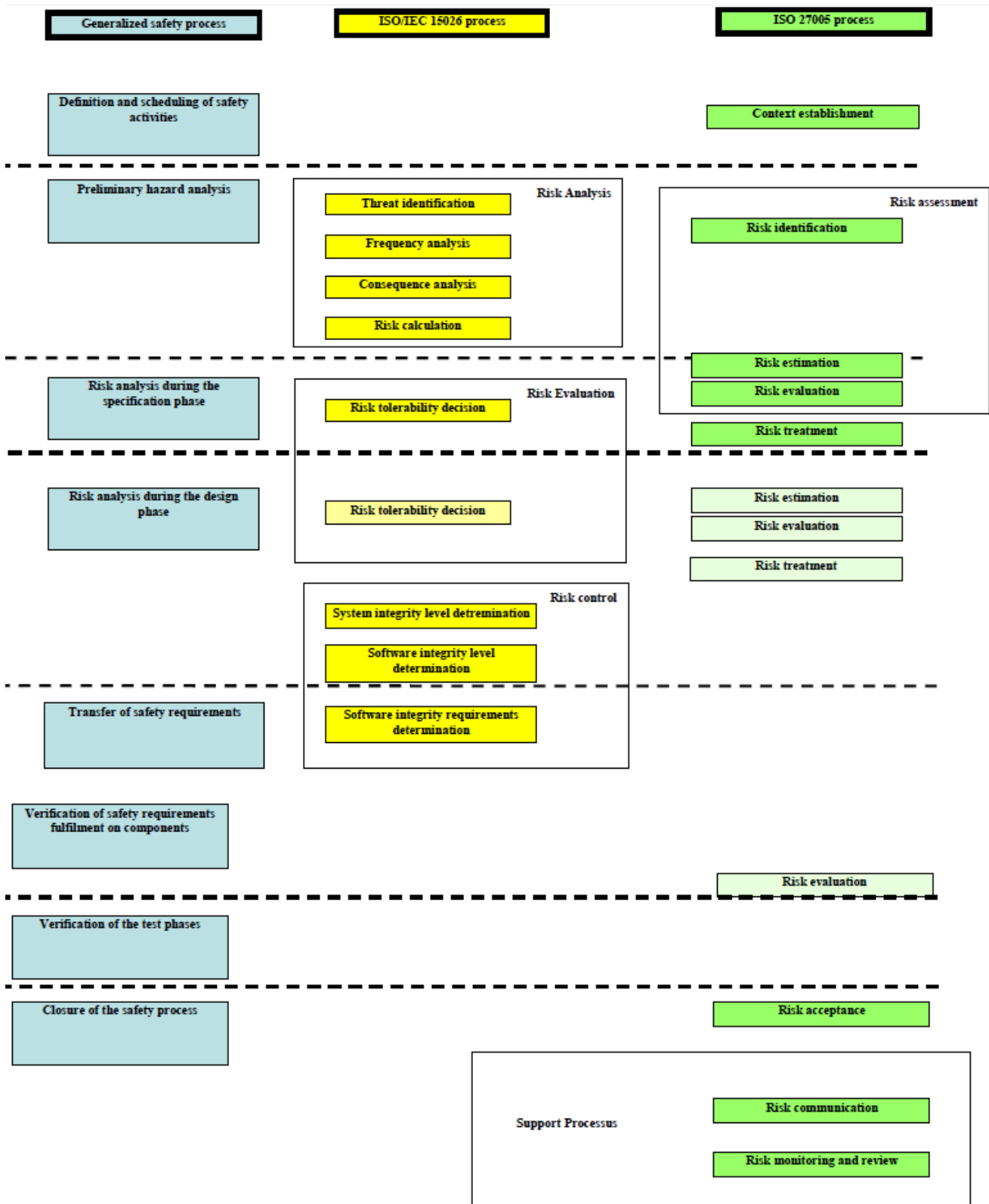


Figure 45: Convergence between ISO 27005 and ISO 15026 (Derock, et al., 2010)

(Gutgarts, et al., 2010)²⁸ recalls that the low failure rate of the safety-critical software is achieved due to the mandatory requirement for certification based on standards, which emphasize rigorous verifications of the process outputs throughout the software life cycle. This is aided by ability to use, in some cases, formal methods to positively prove that requirements have been met. By contrast, difficulties in defining security-critical software requirements to allow for unambiguous verification paved a way for emerging practice of static source code

²⁸ For a smile, do compare the titles of (Carter, 2010) and (Gutgarts, et al., 2010).

analysis, and indirectly to the development of the Common Weakness Enumeration (CWE) by the MITRE. The author suggests, by analogy to (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992), cf. Figure 46, the creation of security-critical levels (e.g. A-E) and associated methods for assuring achievement of those levels, with the twist that each sub-factor of security (i.e. confidentiality, integrity and availability) are likely to have different levels of requirement for a given system.

Level	Objectives	With independence
A	66	25
B	65	14
C	57	2
D	28	2
E	0	0

Figure 46: Safety-objectives per safety-level according to DO-178B (Gutgarts, et al., 2010)

Building upon previous work²⁹ by Marc Bouissou, (Piètre-Cambacédès, et al., 2010) proposes an adaptation of the safety-related Boolean logic Driven Markov Processes (BDMP) to security risk analysis in an integrated formalism covering both specialties (cf. Figure 47). According to the authors, BDMPs are as readable as traditional attack trees, but with dependency and dynamic characteristic capabilities, allowing for the computation of new security indicators (e.g. attack success probability, mean time to attack). Full details can be found, in French, in (Piètre-Cambacédès, 2010f).

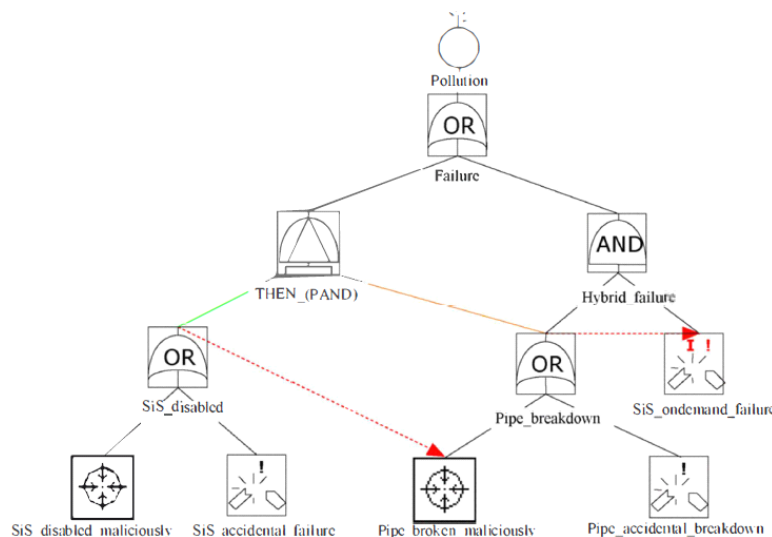


Figure 47: Example of Boolean logic Driven Markov Process (Piètre-Cambacédès, et al., 2010)

(Firesmith, 2010) is a full-day tutorial (i.e. 150 slides), which introduces the attendee to the engineering of safety- and security-related requirements for software-intensive systems. It provides a consistent, effective, and efficient method for identifying, analysing, specifying, verifying, and validating the four different types of safety- and security-related requirements, i.e. safety and security quality requirements, safety- and security-significant requirements, safety and security function / sub-system requirements and safety and security constraints (cf. Figure 48). The author concludes that: (i) these requirements need to be identified, analysed and specified differently; (ii) the processes for requirements engineering, safety engineering and security engineering need to be properly interwoven, consistent and performed collaboratively in parallel.

²⁹ M. Bouissou, Automated Dependability Analysis of Complex Systems with the KB3 Workbench: the Experience of EDF R&D, International Conference on Energy and Environment (CIEM), Bucharest, Romania, October 2005, and, M. Bouissou, A generalization of dynamic fault trees through Boolean logic Driven Markov processes (BDMP), 16th European Safety and Reliability Conference (ESREL'07), Stavanger, Norway, June 2007.

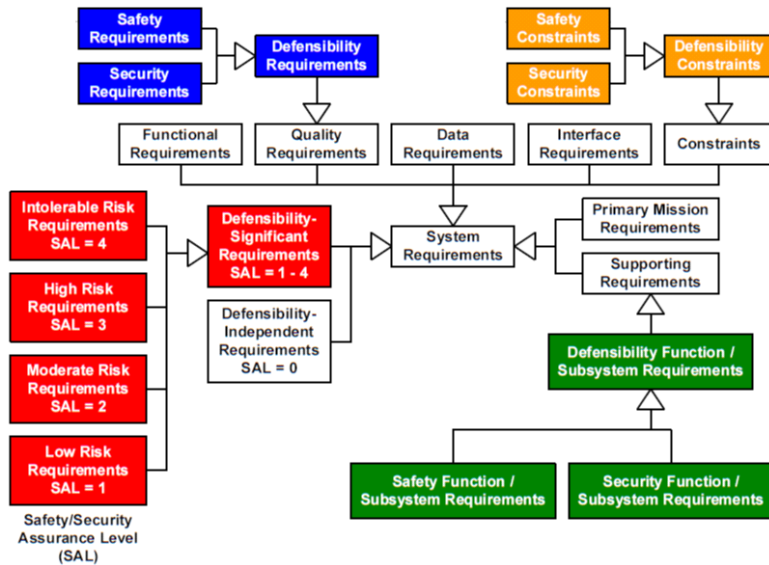


Figure 48: Four different types of safety- and security-related requirements (Firesmith, 2010)

(Förster, et al., 2010) describes the results of Fraunhofer’s research in the ViERforES project (ViERforES, 2008) with respect to dependability models that can be used to arrive at an integrated and analysable model for safety and security issues of a system, and their interdependence. This extensive report (53 pages) starts by recalling the main fault tree and attack tree models, together with some of the proposals made for their integration. The authors then propose a combinatorial model based on the integration of a Component Logic Model (CLM³⁰) and an adapted³¹ attack tree model, cf. Figure 49. This combinatorial model enables qualitative (i.e. assigning priorities to minimal cut sets) and quantitative (i.e. computing minimal cut sets probabilities or weights) safety/security analyses. Multiple options are proposed for quantitative analyses, e.g. pseudo-probabilities, random sampling, sub-set analysis with cost functions, top-level event analysis, etc. The authors also briefly discuss the visualisation of the results to support root cause analysis. The report concludes on a safety / security assessment process (cf. Figure 50).

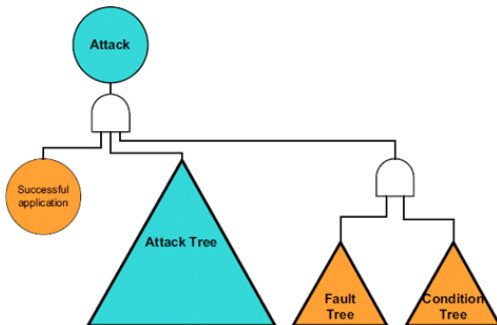


Figure 49: Augmenting the attack tree model

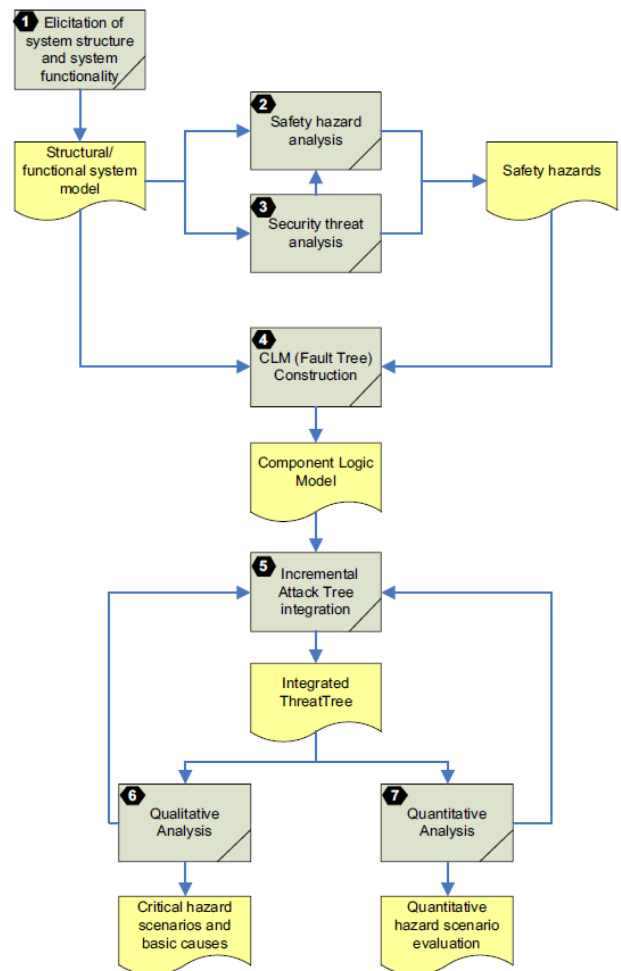


Figure 50: Threat tree assessment process (Förster, et al., 2010)

³⁰ The CLM is an extension of the Component Fault Tree (CFT), which is itself an adaptation of the traditional Fault Tree (FT).

³¹ A semantic shift of the tree nodes is required, from *attack goal* to *impact of a successful attack*.

(Koscher, et al., 2010) reports on an experimental evaluation of security issues on a modern automobile and demonstrates the fragility of the underlying system structure of this safety-critical system. Beyond the fact that the authors are at the origin of the famous Car-Shark tool – a custom CAN bus analyser and packet injection tool – we wish to highlight the paper’s ending discussion on some complex challenges for the industry to address the raised security issues.

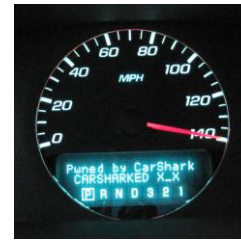


Figure 51: Displaying an arbitrary message and a false speedometer reading on the Driver Information Centre, whilst the car is in Park (Koscher, et al., 2010)

Building upon (Gutgarts, et al., 2010), and based on the fact that security-related standards are much less stringent than safety-related standards, (Axelrod, 2011) advocates for more exchanges between the safety and security communities, and claims that the approaches used for safety-critical process control systems could greatly benefit security-critical information systems (cf. Figure 52). Nine safety-related best practices, which span across the full system / software development lifecycle, are cited for use during security-critical system engineering: (a) security features should be added at the requirements and specifications stages of developing information systems and information-security specialists should be included in the team creating requirements; (b) prior to connecting security-critical systems to networks, a careful analysis should be done to determine whether there might be ways to eliminate or limit connectivity; (c) programming languages that force discipline on the developer should be favoured; (d) hardened versions of operating systems should be favoured; (e) designers and developers should be trained in secure coding practices, and then adequate procedures should be put in place to catch any lapses; (f) verification and validation should be applied to security-critical information systems; (g) deployment should be limited to a small number of platforms; (h) operational and support staff should be trained in the functionality of the information systems that they run, and management should resist the pressure to frequently update current systems and introduce new ones; and (i) sensitive data should not be stored in the applications themselves, and the frequency of systems decommissioning should be reduced.

Category of System	Typical Systems	Impact of Failure or Compromise
Non-critical	Nice-to-know news systems	Minimal impact to using organization May be damaging to supplier of system
Business critical	Customer-support systems Supplier-interface systems Business information processing systems Required to be operational by law or regulation	Loss of customers Disruption of supply chain Loss of business, customer dissatisfaction Fines, removal of licenses, cessation of business
Security critical	Systems processing sensitive information, such as company secrets, non-public personal information, other sensitive information	Loss of future business due to competitors having obtained proprietary information Subject to fines by regulators Threat to national security for classified government information
Safety critical	Process control for systems upon which human safety depends	Injury and/or loss of life
Security and safety critical	Process control systems that might be subject to attack by unauthorized parties intent on doing damage	Injury and/or loss of life Reduced ability to defend the nation Delays in creation of critical infrastructure systems

Figure 52: Categorization of systems by impact of failure or compromise (Axelrod, 2011)

(Zhenhai, et al., 2010) proposes a service-oriented framework of information integration of safety and security for high-speed railway. It consists of four layers: basic platform layer, data organization layer, key service layer and application layer. According to the authors, the framework breaks the hard situation of various information systems at present, which are always independent and have difficult data sharing. The framework makes a system more dynamic and expandable, as it is easy to establish different service modes for users with different information requirements.

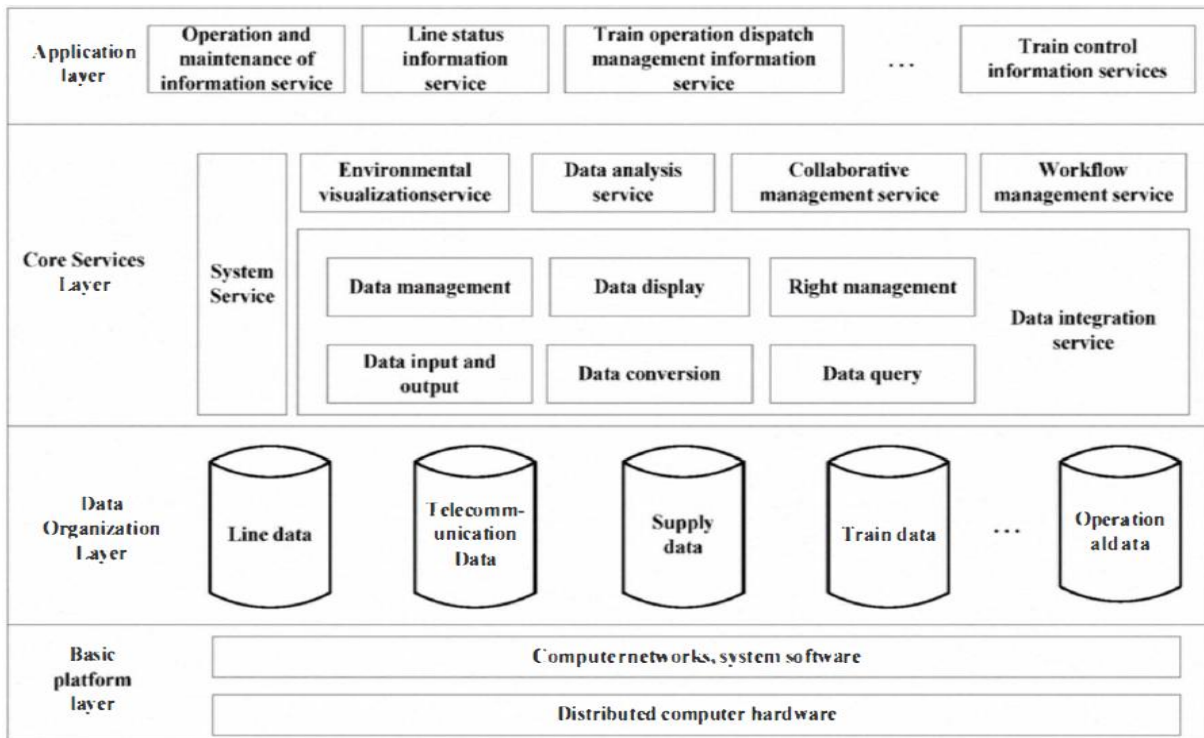


Figure 53: Framework of Information integration of safety and security for high-speed railway (Zhenhai, et al., 2010)

(Åkerberg, 2011) starts by recalling that in the process industry, network and system security have become important since the introduction of Ethernet-based fieldbus protocols. Wired fieldbus protocols are mature with respect to safety and there are existing standards for safe communication (cf. Figure 54). However, the wired fieldbuses lack adequate security measures to be deployed in industrial automation. In wireless sensor networks, security is addressed thoroughly in the standards, but is not mature with respect to safety. Future automation systems need ideally to seamlessly support safety and security in heterogeneous networks while hiding the complexity for the end-users in order to successfully manage large-scale industrial production. This short thesis (57 pages) presents one feasible solution towards safe and secure communication in heterogeneous industrial networks for process control (cf. Figure 55). A security layer is added between the communication layer and the application layer, using the communication layer as the black channel³². The security layer is not added within the scope of the Open Systems Interconnection model (OSI model), but rather between the OSI model and the application to avoid conflicts with standards and to allow end-to-end security. In the same manner the safety layer is used between the communication layer, or security layer depending of the usage of the security layer. For safety certification reasons, the security layer is part of the safety layer's black channel. Within the proposed framework, safety and security layers can be utilized independent of each other and are deployed based on the current requirements. The presented solution addresses several other important aspects such that engineering efficiency, transparency, possibilities for retrofitting, coexistence with international standards in order to protect the return-of-investment of products, systems, and installed base within the area of process automation. Field trials show that several improvements of wireless sensor networks with respect to determinism in both the uplink and the downlink are needed. This is not only true when it comes to the research problems addressed within the scope of this thesis, but rather a necessity for market acceptance and deployment in process automation in general. The major contribution of this thesis is a method that enables end-to-end safe and secure communication in heterogeneous automation networks without major changes in existing standards, while preserving engineering and integration efficiency.

³² The principle of the black channel simplifies the overall safety certification process, as the standard transmission system does not have to be part of the safety certification.

IEC 61784-1	IEC 61784-3
Foundation Fieldbus	FF-SIS
CIP	CIP-Safety
PROFIBUS & PROFINET	PROFIsafe
INTERBUS	INTERBUS Safety

Figure 54: Standardized safety profiles (Åkerberg, 2011)

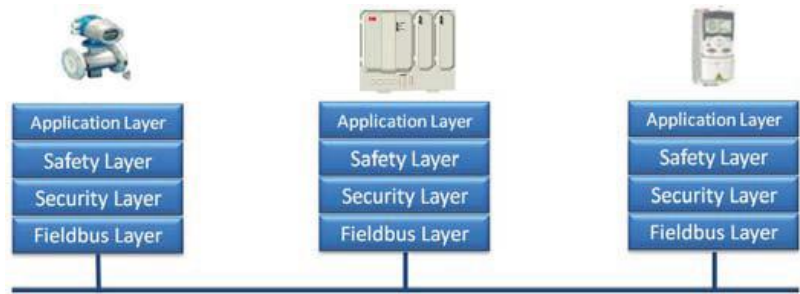


Figure 55: Proposed framework for safe and secure communication (Åkerberg, 2011)

(De Saqui-Sannes, et al., 2011) presents an overview of the Automated Verification of reAl Time softwARE (AVATAR) language, and the open-source TURTLE Tool (TTool). AVATAR is derived from SysML and enriched with the TEmporal Property Expression (TEPE) language. AVATAR allows for the expression of safety and security properties. Its formal semantics are translated to timed automata (for safety properties) and pi-calculus (for security properties) to allow for formal proofs. The TTool provides a user-friendly interface to edit the system models and interface with UPPAAL, ProVerif and the C Posix code generator. The features are illustrated on a simple case study. See also (Knorreck, et al., 2010), (Pedroza, et al., 2011) and (Aprville, et al., 2014).

(Gerhold, 2011) presents the results of a qualitative Delphi study performed in the scope of a Research Forum on Public Safety and Security (Freie Universität Berlin, Institut für Informatik, 2009). The achieved results supply an image of German research on safety and security from the perspective of all relevant disciplines, i.e. the scope of the publication is much larger than the topic of safety and security-critical software-intensive systems co-engineering addressed herein. Based on developments relevant for safety and security and exemplary research topics, challenges are defined for the future of research on safety and security (cf. Figure 56). In this context, this contribution deals with the question of using different definitions of the term, alignment of research for different recipients and use of different research strategies and methods. One important conclusion that is relevant for our current study is that, according to the author, research on safety and security needs to open up to a terminology discourse that will be able to productively link and expand the difference between the perspectives of research on safety and security in the sense of absence of danger and in the sense of coping with uncertainty.

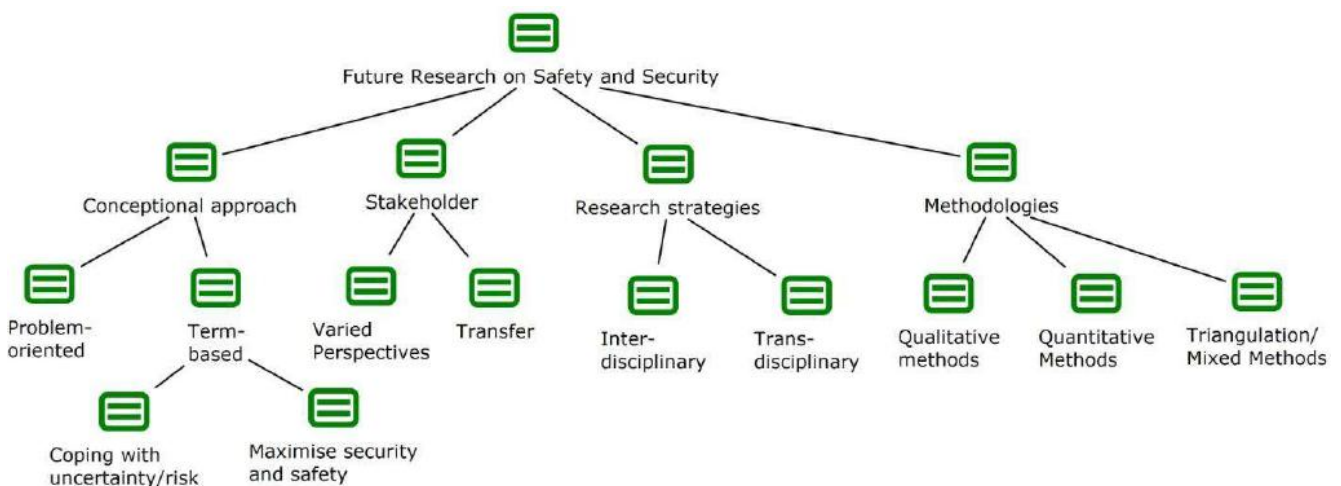


Figure 56: Challenges of Future Research on Safety and Security in Germany (Gerhold, 2011)

(Goertzel, et al., 2011) discusses the safety hazards that can arise in safety-critical component-based software-intensive systems (also known as “software-reliant systems”) such as weapons systems, as well as the security risks that can result in safety mishaps (i.e., “safety-impacting security”). The report also discusses assessment and analysis techniques that can be used to pinpoint and assess such hazards and risks, and architectural engineering countermeasures that can be used mitigate those that cannot be avoided or eliminated. Specifically, the paper discusses: (i) the types of anomalous, unsafe, and non-secure behaviours that can emerge when components interact in component-based systems; (ii) analysis and assessment techniques that can be used to predict where and how such anomalous behaviours are likely to occur; (iii) architectural engineering counter-

measures that can be used by the system's developer to either prevent such behaviours or to contain and minimize their impact, thereby mitigating the risk they pose to the safe and secure operation of the system.

(Johnson, 2011) recalls that the latest generation of augmented Global Navigation Satellite Systems (GNSS) has been approved for use in safety-related applications, but a range of organisations, including the UK Ministry of Defence, have raised concerns about its increasing vulnerability to attacks. As a response, the author proposes the integration of security concerns into safety cases to sketch the potential consequences of a malicious attack on an underlying Satellite Based Augmentation Systems (SBAS). A key benefit of the approach is that the safety case provides a means of collating the diverse sources of evidence from design, testing and analysis. However, this evidence must be derived using other tools and techniques. It is for this reason that the paper also presents a means of analysing the more detailed interactions between the security and safety of GNSS. In particular, the author shows how Boolean Driven Markov Processes (BDMP) help to avoid some of the state explosion limitations of conventional Markov techniques using extensions to the well-known Fault Tree notation.

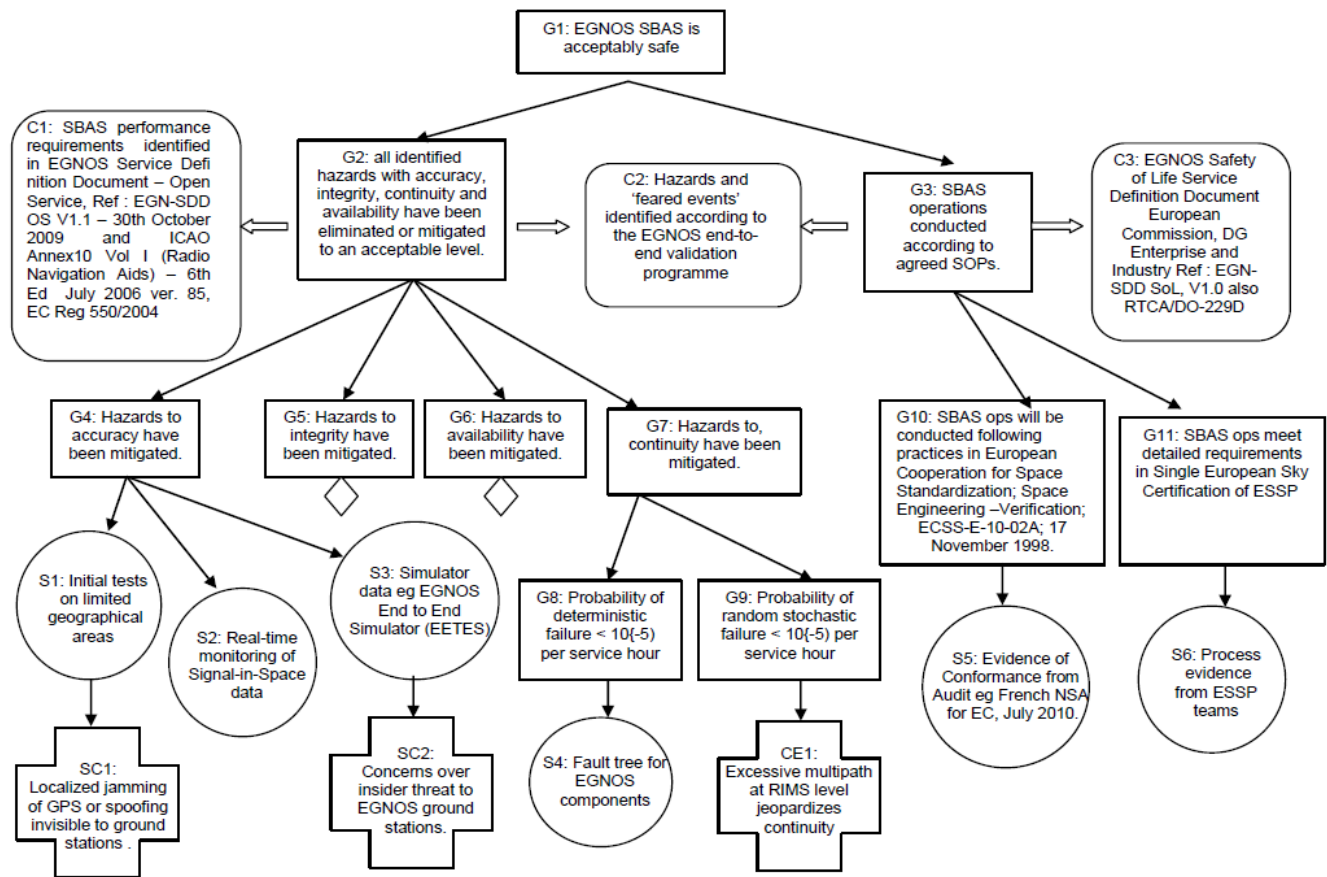


Figure 57: Integrating Security Threats to GNSS Architectures within GSN Safety Arguments (Johnson, 2011)

(Mc Guire, 2011) starts by recalling that security has traditionally been excluded from functional safety³³ considerations, but *safety by secrecy* is now recognised as one of the most critical systematic faults of the safety community. The author shows that things as starting to change, illustrating the point on the controversial introduction of security considerations in (S + IEC 61508, 2010). The paper then lists and discusses some mature security methods, used in open-source operating system software, and that can help with respect to safety issues, because still poorly used by the safety community: address space randomization, stack/heap randomization, Instruction Set Randomiza-

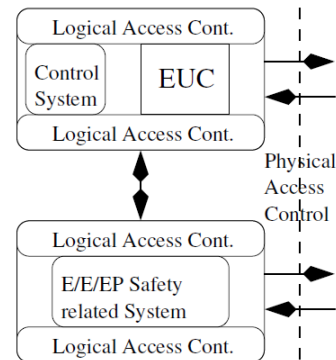


Figure 58: S + IEC 61508 security model for segregation

³³ Functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs, incl. the safe management of likely operator errors, hardware failures and environmental changes.

tion (ISR), isolation enhancements, etc.

(Mc Guire, 2011)

(Pedroza, et al., 2011) recalls that critical embedded systems are now commonly distributed, thus exposing their communication links to attackers. The design of those systems therefore needs to handle new security threats whilst maintaining a high level of safety. To address that issue, the paper introduces a SysML-based environment named AVATAR. AVATAR can capture both safety and security related elements in the same SysML model, and provides means for their verification, at the push of a button. Safety and security requirements are expressed in terms of SysML requirement diagrams, whereas the static and the behavioural aspects of the system are represented with block and state machine diagrams respectively. Safety properties are further refined within parametric diagrams, and security properties are described within specific pragmas of block diagrams. With respect to standard SysML, AVATAR offers a number of new features to cope with security modelling specificities such as: (i) modelling initial shared knowledge, through the use of pragmas; (ii) independence of the attacker model from the system model, through the use of public broadcast channels between blocks that can be listened up by an attacker and an implicit Dolev-Yao³⁴ attacker model (Dolev, et al., 1983); (iii) modelling of security properties, again through the use of pragmas. AVATAR also offers a library of typical security functions, such as cryptographic functions, for fast modelling. Finally, safety and security proofs are accomplished by first transforming the SysML model to domain specific languages: UPPAAL for safety proofs, and ProVerif for security proofs. Modelling features and translators are implemented in TTool, an open-source UML toolkit. The applicability of the approach is highlighted with a realistic embedded automotive system taken from the EVITA project (EVITA, 2011). This paper covers security issues only. The modelling and verification of safety properties in AVATAR is introduced in (Knorreck, et al., 2010).

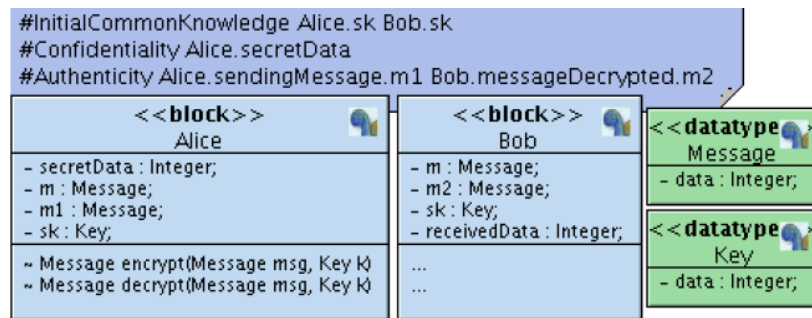


Figure 59: SysML block diagram showing initial shared knowledge, confidentiality and authenticity properties, and classical cryptographic functions (Pedroza, et al., 2011)

(Axelrod, 2012) offers a broad and detailed understanding of software systems engineering from both security and safety perspectives. Addressing the overarching issues related to safeguarding public data and intellectual property, the book defines such terms as systems engineering, software engineering, security, and safety as precisely as possible, making clear the many distinctions, commonalities, and interdependencies among various disciplines. It explores the various approaches to risk and the generation and analysis of appropriate metrics. The book explains how processes relevant to the creation and operation of software systems should be determined and improved, how projects should be managed, and how products can be assured. The author explains the importance of integrating safety and security into the development life-cycle. Additionally, this practical volume helps identify what motivators and deterrents can be put in place in order to implement the methods that have been recommended.

(Banerjee, et al., 2012) recalls that cyber-physical systems (CPSs) couple their cyber and physical parts to provide mission-critical services. Their operation needs to ensure three key properties, collectively referred to as S3: (i) safety: avoidance of hazards; (ii) security: assurance of integrity, authenticity, and confidentiality of information; and (iii) sustainability: maintenance of long-term operation of CPSs using green sources of energy. Ensuring S3 properties in a CPS is a challenging task given the spatiotemporal dynamics of the underlying physical environment. In this paper, the formal underpinnings of recent CPS S3 solutions are aligned together in a theoretical framework for cyber-physical interactions, empowering CPS researchers to systematically design solutions for ensuring safety, security, or sustainability (cf. Figure 60). The general applicability of this framework is demonstrated with various exemplar solutions for S3 in diverse CPS domains. Further, insights are provided on some of the open research problems for ensuring S3 in CPSs.

³⁴ The Dolev-Yao model is a formal model used to prove properties of interactive cryptographic protocols [Wikipedia].

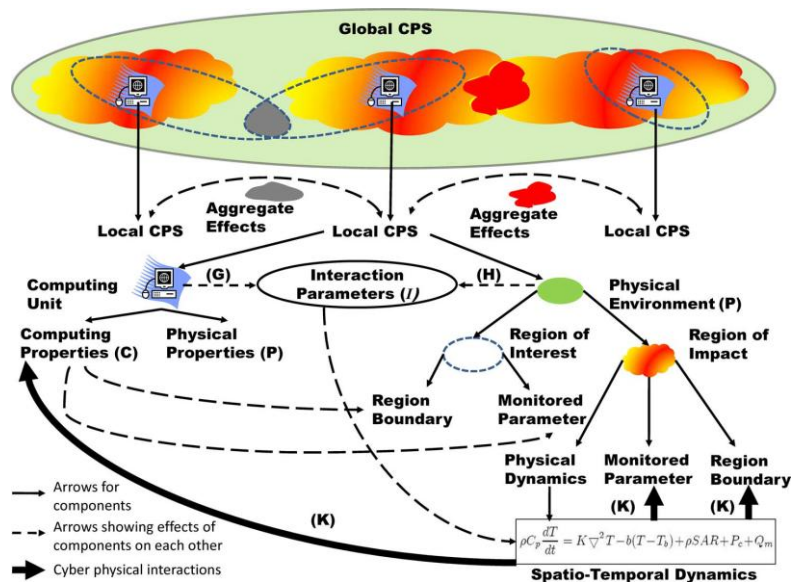


Figure 60: Abstract modelling framework for CPS, global CPS (Banerjee, et al., 2012)

(Bieber, et al., 2012) builds upon (EUROCAE ED-202, 2010) and (Altran Praxis, 2006), focusing exclusively on security for safety in the aviation domain. The authors start by referencing relevant standards and organise them according to their applicability to different engineering activities at system or item level (cf. Figure 61). Then a development assurance process framework is proposed, in which processes are organised in 3 groups: risk assessment, assurance-effectiveness and assurance correctness. The activities of each process are implemented using assurance activities already existing in the aforementioned standards. The authors recognise that some concepts / terms slightly differ between the two engineering specialties, but the authors believe that the chances are high that a natural convergence will occur in time if the processes are correctly synchronised.

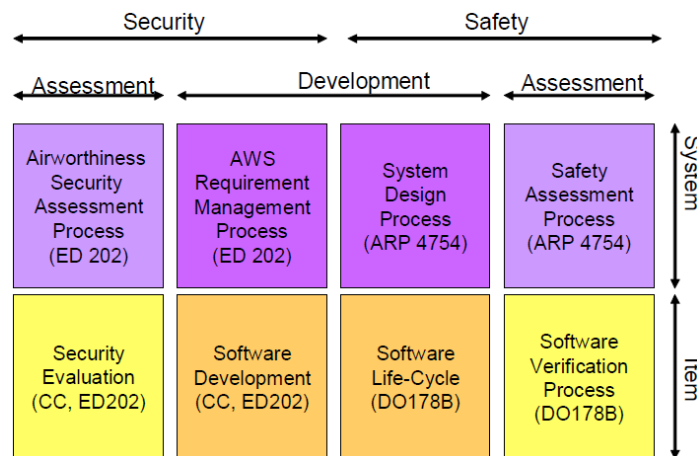


Figure 61: Relevant existing processes for the SEISES programme (Bieber, et al., 2012)

In the context of the French collaborative SEISES project (SEISES, 2008), (Blanquart, et al., 2012) proposes, as prerequisite to the definition of a security for safety engineering process, a comparative analysis of the notions of safety levels and security levels as defined, under various names, by the relevant standards, in particular (ISO/IEC 27005, 2011), (SAE ARP 4754A, 2010) / (EUROCAE ED-79A, 2010), (EUROCAE ED-202, 2010), (ECSS-Q-ST-30C, 2009), (ECSS-Q-ST-40C, 2009), (ECSS-Q-ST-80C, 2009), (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992), and Common Criteria (ISO/IEC 15408-1, 2009). After recalling some standard definitions, the authors propose a mapping between the ED-202 security levels (cf. Figure 62) and the Common Criteria Evaluation Assurance Levels (EAL), cf. Figure 63. The authors conclude on a discussion of what could be a security for safety level.

Security Level	Effectiveness (reduction in likelihood classification)
E	No Reduction
D	Reduction by One level
C	Reduction by Two levels
B	Reduction by Three levels
A*	Reduction by Four levels

* = A single vulnerability in the architecture must not compromise all the security countermeasures

Figure 62: Security level classification (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010)

SL	E	D	C	B	A
AVA	1	2	3	4	4
EAL	1	2,3	4	5	5

Figure 63: A possible SL / EAL mapping (Blanquart, et al., 2012)

In the scope of the (SeSaMo, 2012) project, (Bloomfield, et al., 2012) reports on the results of a security analysis of the European Railway Traffic Management System (ERTMS) specifications. ERTMS is designed to be fail-safe and the general philosophy of 'if in doubt, stop the train' makes it difficult to engineer a train accident. However, it is possible to exploit the fail-safe behaviour of ERTMS and create a situation that causes a train to halt. Thus, denial of service attacks are possible, and could be launched at a time and place of the attacker's choosing, perhaps designed to cause maximum disruption or passenger discomfort. According to the authors, causing an accident is more difficult, but not impossible.

(Bock, et al., 2012) recalls that some recent incidents have shown that the vulnerability of IT systems in railway automation has been possibly underestimated so far, and that due to several trends, such as the use of commercial IT and communication systems or privatization, the threat potential could increase in the near future. However, up to now, no harmonized IT security requirements for railway automation exist. This paper defines a reference communication architecture which aims at separating IT security and safety requirements as well as certification processes as far as possible, and discusses the threats and IT security objectives including typical assumptions in the railway domain. Finally examples of IT security requirements are stated and discussed based on the approach advocated in the Common Criteria (ISO/IEC 15408-1, 2009), in the form of a protection profile. See also (Braband, 2014a).

(Casals, et al., 2012) gives a set of characteristics for a security risk assessment methodology to be used in the early design of safety-critical airborne systems. This paper is particularly relevant with regard to (EUROCAE ED-202, 2010) standard and the upcoming (EUROCAE ED-203, 2012)³⁵ draft standard. The discussion is illustrated on a Weight and Balance (WBA) function that ensures 3D stability control of aircraft gravity centre.

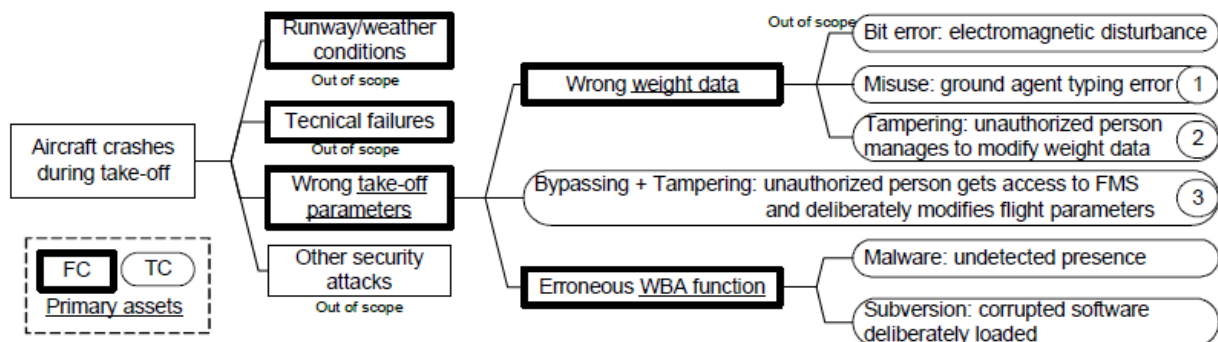


Figure 64: Top-down approach threat scenario identification: from feared event to potential causes (Casals, et al., 2012)

(Chapon, et al., 2012) recognises the need to orchestrate safety and security engineering for complex systems. The authors propose a common ontology for a small number of safety and security concepts, and discuss some co-engineering techniques, with a focus on Boolean logic Driven Markov Process (BDMP) and SysML extensions. For the approaches, a partition is proposed between formal methods to address known and controlled risks (e.g. internal system faults, script kiddies), and in-depth defence, to address unknown or uncontrolled risks (e.g. causes external to the system, 0-day threats).

³⁵ The Radio Technical Commission for Aeronautics draft counterpart was known as DO-YY3. It is now published as (RTCA DO-356, 2014).

The mission of the EURO-MILS project (EURO-MILS EC FP7 Project, 2012) is to develop a solution for virtualisation of heterogeneous resources and provide strong guarantees for isolation of resources by means of Common Criteria certification with usage of formal methods. The project aims at providing trustworthiness by design and high assurance based on the Multiple Independent Levels of Security (MILS) approach. MILS is a high-assurance security architecture based on the concepts of separation and controlled information flow.

(Johnson, 2012) starts by recalling that common software components are gradually being integrated across many safety-critical infrastructures, creating significant security concerns across many industries, and in particular Air Traffic Management (ATM). The paper presents a roadmap for increasing resilience to future Cyber-Safety attacks (cf. Figure 65). The author states that we must raise awareness about the potential threats to safety-related systems amongst regulators and senior management, pointing out that without greater strategic leadership there is a danger that Air Navigation Service Providers (ANSPs) will continue to respond to security breaches in a piecemeal way that leaves major vulnerabilities in underlying infrastructures. Because ANSPs continue to ignore the “insider threat” and lack the expertise either to diagnose or resolve potential attacks, second element of the roadmap focuses on improved screening, competency assessment and training for engineering staff. Other areas for action include the use of drills and exercises to support team resource management in the aftermath of an attack. The final element of the roadmap proposes a new generation of tools that use lessons learnt from previous attacks together with the insights from drills and exercises to assess the risks of future cyber-attacks.

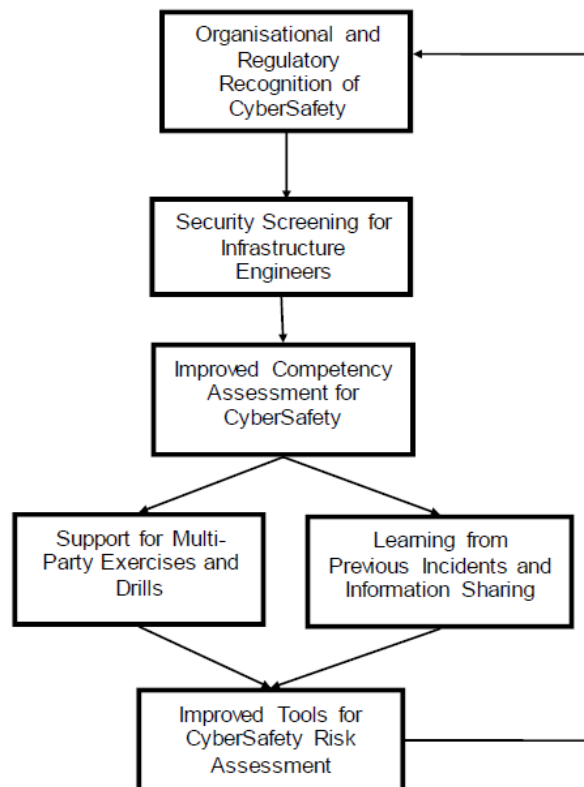


Figure 65: A roadmap for cyber-safety engineering (Johnson, 2012)

(Kleidermacher, et al., 2012) provides: (i) a broad understanding of security principles, concerns, and technologies, (ii) proven techniques for the efficient development of safe and secure embedded software, (iii) a study of the system architectures, operating systems and hypervisors, networking, storage, and cryptographic issues that must be considered when designing secure embedded systems, and (iv) nuggets of practical advice and numerous case studies throughout. It is difficult to summarize this extensive book (418 pages) in just a few lines herein. We just wish to highlight the detailed descriptions given of the MILS virtualisation technique (cf. Figure 66), which supports a layered approach to security, by offering a small OS microkernel that implements a limited set of critical functional security policies, including: data isolation, information flow control, damage limitation and periods processing. The author also propose a Trustworthy Embedded Transaction Architecture (cf. Figure 66), based on the MILS technology, in which virtualization is used to host two critical security subsystems that run in a separate virtual machines or within a native microkernel process (if applicable). The first subsystem, i.e. the communications server, provides a trustworthy communications connection between the embedded system and

the remote device / server. The second subsystem, i.e. the transaction verifier, provides a trusted verification interface for the client.

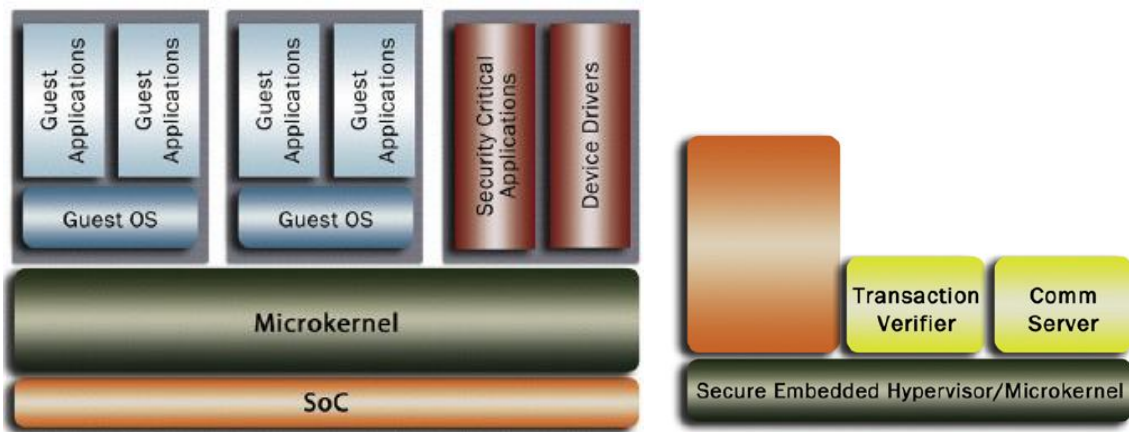


Figure 66: MILS virtualisation technique [left] and trustworthy embedded transaction architecture [right] (Kleidermacher, et al., 2012)

(Monakova, et al., 2012) presents a tool-supported framework that extends modelling and execution of business processes with specification, execution and monitoring of the security and safety constraints that are used to protect business assets. Overall, this transfers the well-known model-driven software development paradigm to workflow management systems that can execute the abstract process models directly. The approach is illustrated by a supply chain for perishable goods case study. The prototype is based on the Windows Workflow Foundations, and has been showcased at various trade fairs and received positive feedback from the different parties involved in such supply chains. The authors found that even a non IT audience easily understands the visualization of security constraints (e.g., a signature symbol on a purchase order) as well as safety constraints (e.g., a temperature symbol on the purchased good). Future work includes specification of the reactive actions that must be taken when a violation occurs.

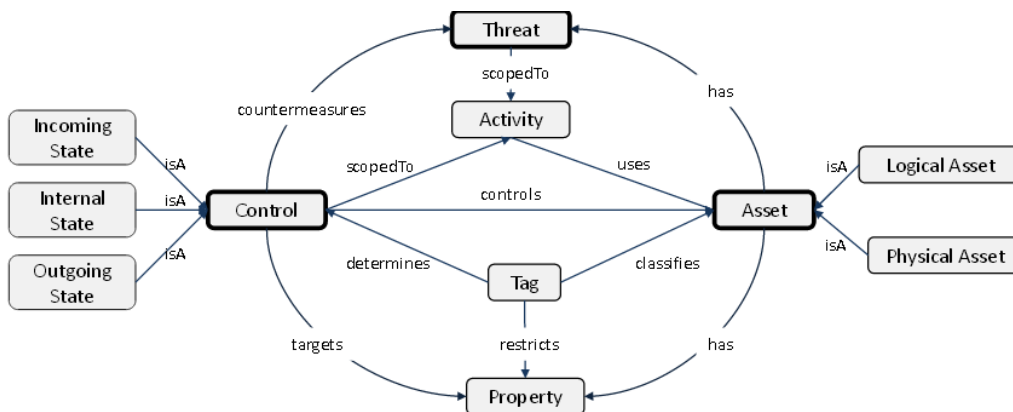


Figure 67: Conceptual model (Monakova, et al., 2012)

(Müller, et al., 2012a) recalls that software architectures in the aerospace domain are becoming more and more integrated and interconnected for functional and architectural reasons (Integrated Modular Avionics, IMA), which exacerbates potential security problems of avionic software. As a consequence, security considerations are gaining importance for the general airworthiness of modern aircraft, and proper security assurance requires increasing effort. In this paper, the authors report on-going work in the SeSaM research project. They propose to leverage modularity as a key to obtain more secure software and higher assurance of this claimed security with reasonable effort. Using Multiple Independent Levels of Security (MILS), the authors present a case study on how an application can be systematically designed, secured, and proven secure by adopting a composite evaluation approach reflecting the modular system architecture. More specifically, the authors employ a separation kernel as the foundation for a security-critical application (cf. Figure 68), and investigate how a security evaluation can be achieved systematically and with reduced effort if the underlying kernel and dependent application independently is evaluated before joining these partial results to obtain an overall evaluation verdict.

Thus, the authors illustrate how a compositional approach may ease security design and security assurance of IMA architectures.

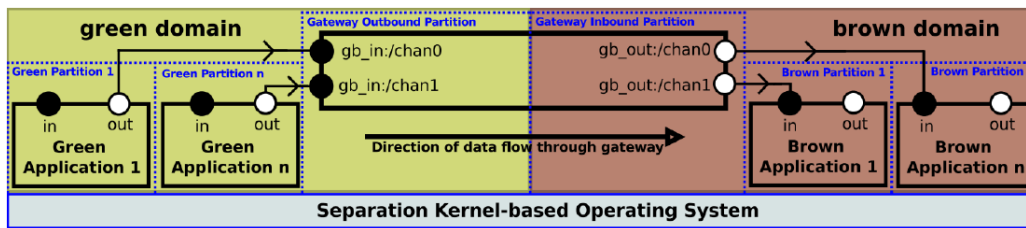


Figure 68: Gateway Software Architecture (Müller, et al., 2012a) (Müller, et al., 2012b)

(Müller, et al., 2012b) presents and discusses their third specification and implementation of a security gateway integrated into an avionics architecture. The gateway specifications include six major requirements: (i) content-based flow control; (ii) separation of duty; (iii) strict unidirectional data flow between two domains; (iv) generic interface for filter implementations; (v) real-time capability; and (vi) audit support. The gateway design is split into two partitions: outbound and inbound (cf. Figure 69); these partitions belong to different security domains and are connected via a unidirectional OS-provided communication channel. The outbound partition of the gateway is used to prevent leaking of data from the given security domain. The inbound partition is used to protect the system from possibly malicious input from the outside. Each partition comprises 3 to 4 modules. The paper describes the role and architecture of each module in detail. For example, the outbound viewer module implements the filtering functionality, i.e. it checks the packet regarding the defined egress security policy of the associated domain. This module iterates a packet over all available protocol filters. Each filter starts by checking the packet validity. If the packet is valid, the filter runs its security checks based on predefined rules and responds whether the packet is allowed or denied to leave the security domain. If a packet passes all filters, then it is allowed to leave the security domain and be transferred to the border-crossing module. Otherwise, the packet is dropped. The gateway implementation is responsible for documenting the final decision. The filter can provide additional information for audit entry. The authors point out that one covert channel remains, but it was decided that this was acceptable with respect to Worst Case Execution Time (WCET) safety requirements. More technical details related to the performance of input/outputs can be found in (Müller, et al., 2014).

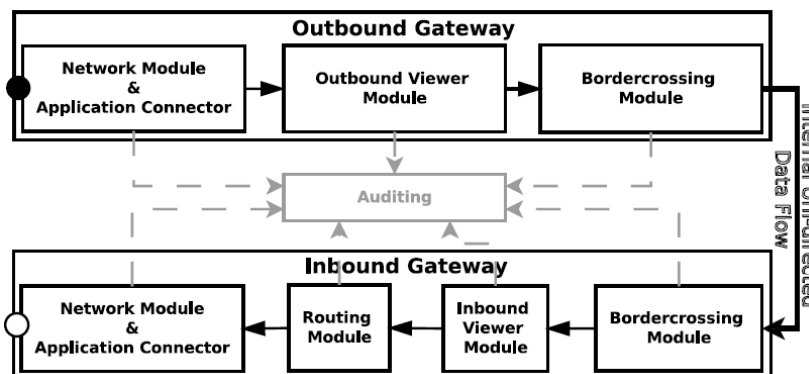


Figure 69: Gateway modules (Müller, et al., 2012b)

(Paulitsch, et al., 2012) starts by recalling that, in the aerospace domain, security concerns of safety-critical systems increase due to interconnections of systems. The paper outlines future security requirements in avionics and issues in assessing the reliability of software from the safety and security perspective. The authors claim that quantitative work on software reliability has focused on requirements-to-code translation (cf. Figure 70), whilst software security has focused more on requirements correctness, and thus that future work must take advantage of results from both the security and safety areas.

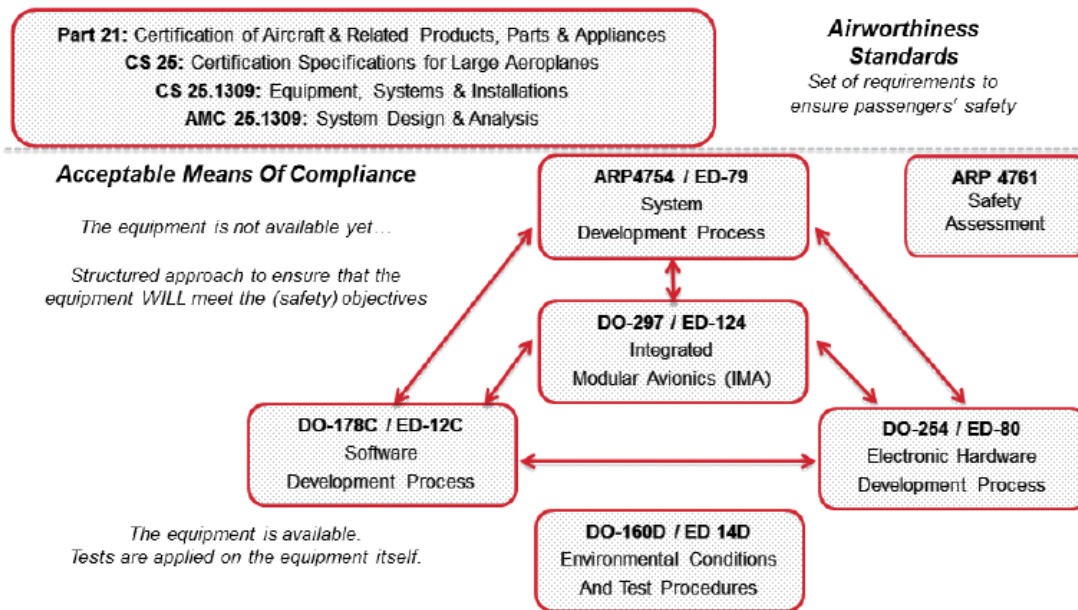


Figure 70: Overview of safety-related development assurance in aerospace (Paulitsch, et al., 2012)

Building on (Sindre, 2007) and (Stålhane, et al., 2008), (Raspotnig, et al., 2012a) proposes to adapt the security-related Misuse Sequence Diagrams to support failure analysis. The resulting technique, called Failure Sequence Diagrams (FSD) is used to support Failure Mode and Effect Analysis (FMEA), for the mutual benefit of both specialties (cf. Figure 71).

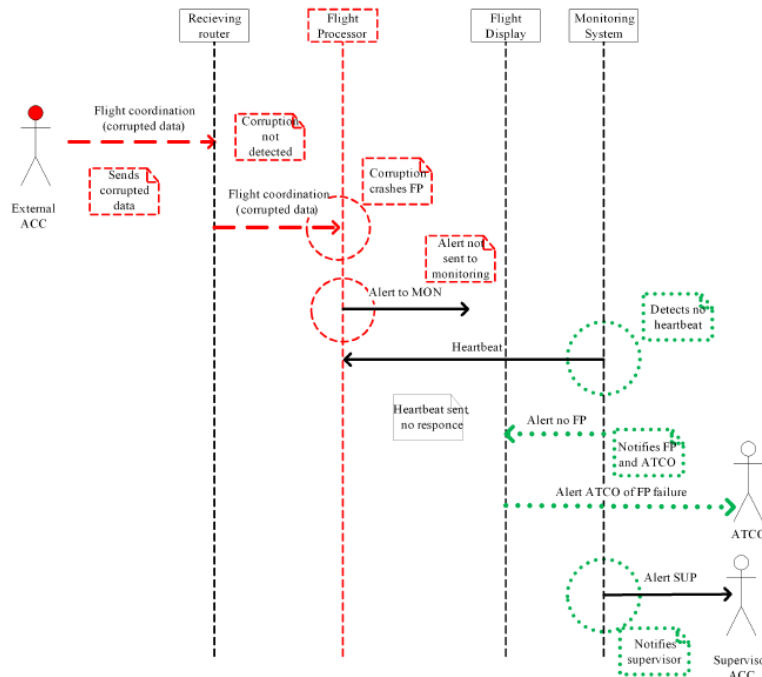


Figure 71: Example of FSD usage (Raspotnig, et al., 2012a)

(Raspotnig, et al., 2012b) proposes a unified process for the elicitation and analysis of safety and security requirements, called the Combined Harm Assessment for Safety and Security of Information Systems (CHASSIS) method. It combines safety and security modelling techniques with the aim of transferring their best characteristics and aligning them in a beneficial way. The method is thoroughly illustrated on an Air Traffic Management Remote Tower example. After further validation exercises, the process was enhanced in (Raspotnig, et al., 2013b), (Raspotnig, 2014) – cf. Figure 100. In (Raspotnig, et al., 2013b), a conceptual model for safety and security is proposed (cf. Figure 72).

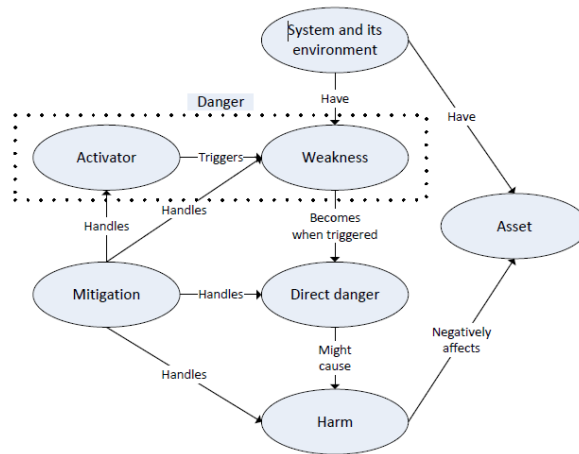


Figure 72: The conceptual model for safety and security (Raspotnig, et al., 2013b)

(Reichenbach, et al., 2012) proposes an approach for combining safety analysis with security analysis by considering the Safety Integrity Levels (SIL) of (S + IEC 61508, 2010) as an extension of the Threat Vulnerability and Risk Assessment (TVRA) method. In this method, risk likelihood is calculated based on the attack potential value, which is calculated using the factors Time, Expertise, Knowledge, Opportunity, and Equipment, whilst the risk impact is calculated from the asset impact value and the attack intensity value. The paper proposes to extend the impact calculation by including the SIL (cf. Figure 73). The spirit of the approach is similar to the one proposed in (Gutgarts, et al., 2010).

Threat Group	Attack		
	Factor	Range	Value
DoS attack of the synchronization interface between the two processors for diagnosing a Safety Module for Drives	Time	<= 1 week	1
	Expertise	Proficient	2
	Knowledge	Restricted	1
	Opportunity	Difficult	12
	Equipment	Standard	0
	Asset Impact	High	3
	Intensity	Moderate inten	1
Unauthorized access to a Safety Module for Drives and disabling the safety	SIL	SIL 2	1
	Time	SIL 1	1
	Expertise	SIL 2	2
	Knowledge	SIL 3	1
	Opportunity	SIL 4	12
	Equipment	Standard	0
	Asset Impact	High	3

Figure 73: Adding SIL in TRVA, for impact calculation (Reichenbach, et al., 2012)

(Sadvandi, et al., 2012) recalls the existence, nature and impacts of safety-security interdependencies in complex systems, promoting the idea that System Engineering (SE) tools and methodologies may help to master them. Echoing (Chapon, et al., 2012), the authors propose a safety and security integrated paradigm in which: (a) formal risk assessment frameworks may be used to cover both safety and security known threats; and (b) defence in-depth may help to mitigate both safety and security hardly-predictable risks (cf. Figure 74). The paper lists some issues with respect to this proposed harmonizing of safety and security engineering processes in terms of their respective ontologies, processes, standards, tools, industrial organisation, etc.

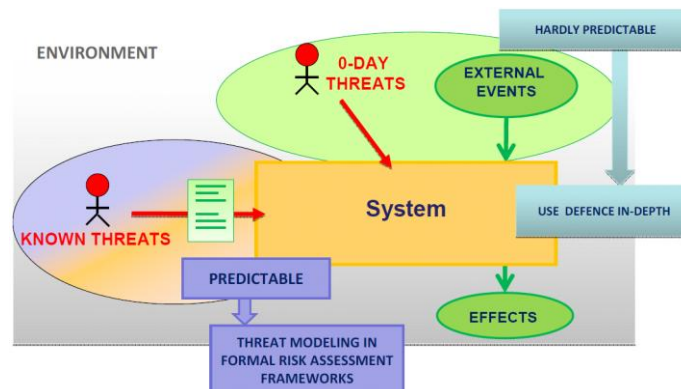


Figure 74: Safety and security integrated paradigm (Sadvandi, et al., 2012)

The SeSaMo project (SeSaMo, 2012) addresses the root causes of problems arising with convergence of safety and security in embedded systems at architectural level, where subtle and poorly understood interactions between functional safety and security mechanisms impede system definition, development, certification, and accreditation procedures and standards. The project proposes to develop a component-oriented design methodology based upon model-driven technology, jointly addressing safety and security aspects and their interrelation for networked embedded systems in multiple domains (e.g., avionics, transportation, industrial control). Key elements of the SeSaMo approach are: (i) a methodology to reduce interdependencies between safety and security mechanisms and to jointly ensure their properties; (ii) constructive elements for the implementation of safe and secure systems, cf. Figure 75; (iii) procedures for integrated analysis of safety and security; (iv) an overall design methodology and tool-chain utilizing the constructive elements and integrated analysis procedures to ensure that safety and security are intrinsic characteristics of the system.

No.	Name	Safety	Security	Cross-influence
1	Encryption and decryption	+	+++	++/--
2	Signature generation and verification	+	+++	o/--
3	Node authentication	++	+++	++/--
4	Access control and traffic filtering	+	+++	+/-
5	Integrity protection	+	+++	++/--
6	Checksums	++	+++	++/-
7	Bootchecks	+++	+++	++/-
8	Software configuration checks	+++	+++	++/-
9	Run-Time Monitoring	+	++	++/--
10	Plausibility checks	+++	+	++/--
11	Logging	+	+++	++/--
12	Security Audit	++	+++	++/-
13	Levels of Operation	++	++	++/-
14	Information Flow Control	-	+++	+/-
15	Partitioning	+++	+++	+++/-
16	Virtualisation	+++	+++	+++/-
17	Protocols for secure real-time communications	+	++	+/-
18	Redundancy and diversity	+++	depends on architecture and threats	depends on architecture and threats

Figure 75: Overview of building blocks (SeSaMo, 2012)

Based on the lessons learnt from the Stuxnet malware, (Aoyama, et al., 2013) proposes a novel framework tackling plant safety and security from a more comprehensive point of view, i.e. including obviously computer security, but also plant availability and robustness. The presented methodology allows one to understand how unsafe activities and cyber-attacks may propagate throughout a plant system and affect the physical side of the plant.

(Axelrod, 2013b) and (Axelrod, 2013c) start by recalling that cyber-attacks on safety-critical systems are big news nowadays, but little action is yet visible, possibly because the backgrounds, training and experience of InfoSec professionals and software engineers have resulted in very different cultures and approaches to system design, development, testing and implementation (see also §5). The author proposes examples to raise attention, and models to help understand what actually happens when something bad occurs to security-critical and safety-critical systems (cf. Figure 76). He concludes by a roadmap which includes: (i) the need to develop individuals who have deep expertise in both security-critical and safety-critical software systems; the need to set up mechanisms so that security and safety information can be shared among those tasked with protecting and supporting critical systems; (iii) the need to include security and safety professionals at each step in the System Development Lifecycle (SDLC), particularly in the requirements phase, and give them the authority to include

their needs and be able to ensure that their requirements are met effectively, with a particular focus on verification and validation of security-critical systems, functional security testing and built-in creation of security data (iv) the need to assign some responsibility and to enforce requirements through law and / or regulation.

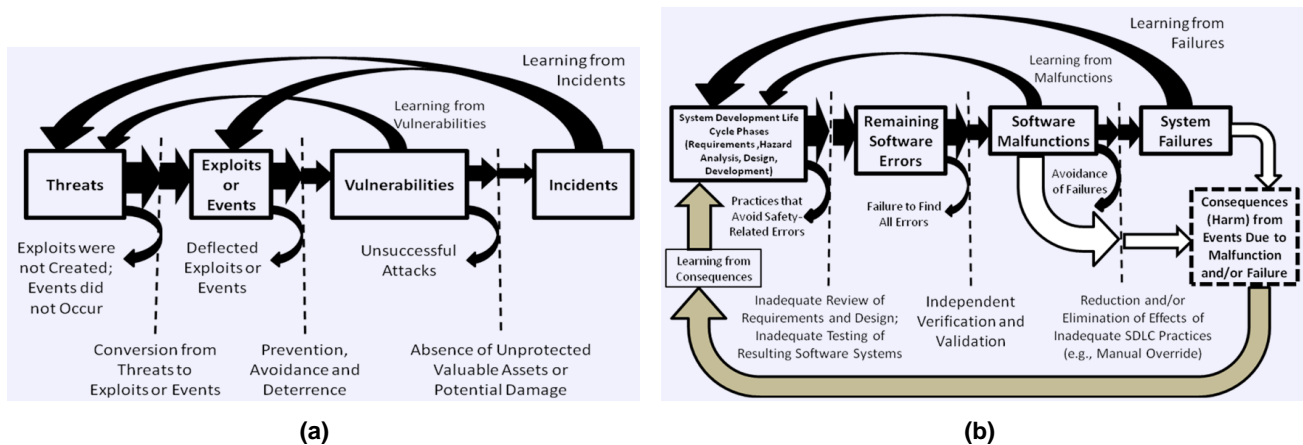


Figure 76: Securing information systems and making software systems safe (Axelrod, 2013b)

(Bezzateev, et al., 2013) starts by recalling that there is no concerted method to develop safe and secure systems by using actual safety and security standards. The paper analyses the safety standards of the European Train Control System (ETCS), showing that there is no consideration of security hazards. The authors suggest taking into account security hazards during the standard fault tree analyses. The security hazards for the Eurobalise³⁶ part of ETCS are defined, and the corresponding safety-security fault tree example is built. Results of numerical calculations of safety with security show that the total level of system safety is increased.

(Czerny, 2013) starts by recalling that today's vehicles contain a number of safety-critical systems designed to help improve overall vehicle safety. Such systems may control vital vehicle functions such as steering, braking and/or propulsion independently of the driver. In today's vehicles, much emphasis has been placed on helping ensure that these safety-critical vehicle systems operate as intended. Applying rigorous system safety engineering principles in developing these safety-critical automotive systems helps ensure that they operate as desired and expected. Less emphasis has been placed to-date on helping ensure cyber-security of cyber-physical automotive systems. However, this is changing as both the world and the automotive industry become more aware of the potential ramifications of cyber-attacks on vehicles. As with system safety, applying a rigorous system security engineering process to the development of cyber-physical automotive systems is beneficial and will help reduce the likelihood of successful attacks on vehicles. System security and system safety interact with one another and cannot be considered in isolation. However, there are also differences between system security and system safety that require unique engineering activities to be performed to address these unique aspects. This paper describes some of the differences and similarities between system security and system safety, between safety-critical systems and security-critical systems, and between system safety and system security engineering, and presents a system security engineering process for applying to cyber-physical automotive systems that is based on the ISO 26262³⁷ process framework.

³⁶ An electronic beacon or transponder placed between the rails of a railway as part of an Automatic Train Protection system.

³⁷ See (ISO 26262-1, 2011) (ISO 26262-2, 2011) (ISO 26262-3, 2011) (ISO 26262-4, 2011) (ISO 26262-5, 2011) (ISO 26262-6, 2011) (ISO 26262-7, 2011) (ISO 26262-8, 2011) (ISO 26262-9, 2011), and (ISO 26262-10, 2012).

(Fisher, 2013) presents some highlights of the Defense Advanced Research Project Agency (DARPA³⁸) Information Innovation Office (I2O³⁹) High-Assurance Cyber Military Systems (HACMS) programme. The goal of the HACMS programme is to create technology for the construction of high-assurance cyber-physical systems, where high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties. For the programme manager, achieving this goal requires a fundamentally different approach from what the software community has taken to date. Consequently, HACMS has adopted a clean-slate based on: (i) model-based design; (ii) program synthesis; (iii) security- and safety-aware composition; and (iv) simplex-based architectures (cf. Figure 106 on page 81). In addition to generating code, the HACMS synthesizer is capable of producing a machine-checkable proof that the generated code satisfies functional specifications as well as security and safety policies (cf. Figure 77). A key technical challenge is the development of techniques to ensure that such proofs are composable, allowing the construction of high-assurance systems out of high-assurance components. The work is illustrated on a quadcopter test case.

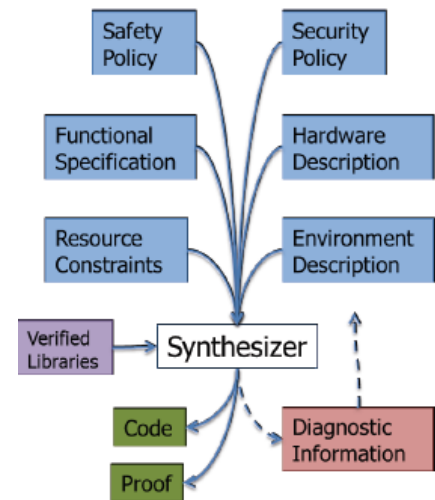


Figure 77: Program synthesis (Fisher, 2013)

Key HACMS technologies include interactive software synthesis systems, verification tools such as theorem provers and model checkers, and specification languages. For the project participants, recent fundamental advances in the formal methods community, including advances in satisfiability (SAT) and satisfiability modulo theories (SMT) solvers, separation logic, theorem provers, model checkers, domain-specific languages and code synthesis engines suggest that this approach is feasible. If successful, HACMS will produce a set of publicly available tools (DARPA I2O HACMS, 2014) integrated into a high-assurance software workbench, which will be widely distributed for use in both the commercial and defence software sectors. HACMS intends to use these tools to: (1) generate open-source, high-assurance, and operating system and control system components; and (2) use these components to construct high-assurance military vehicles. HACMS will likely transition its technology to both the defence and commercial communities. For the defence sector, HACMS will enable high-assurance military systems ranging from unmanned vehicles, to weapons systems, satellites, and command and control devices.

(Garavel, et al., 2013) is the result of a study initiated at the BSI (Bundesamt für Sicherheit in der Informationstechnik), the German Federal Office for Information Security. The main motivation behind the study was to obtain a state-of-the-art account on formal methods used in academia, industry, and governmental institutions in charge of certifying information technology products, and to infer where and how formal methods can be deployed to improve over current development practices. The report presents a comprehensive (with over 100 pages of references) but yet non-exhaustiveness picture of the situation, in which the different approaches to formal methods are organized into a systematic framework and compared with each other. The authors recall that there are different approaches to guaranteeing the quality of software-intensive systems:

- organizational approaches, i.e. processes, methods & standards, essentially focusing on the design processes, and
- technical approaches, essentially focusing on the assessment of the final product, e.g. testing.

The first class of approaches provides quality assurance, the second class, quality control. The combination of both usually allows for high quality software / systems. For safety- or mission-critical systems, the authors demonstrate that it is necessary and even cost-effective to track down as many of the remaining issues as possible before operation. To this end, formal methods can be used as a punctual complement to address known and controlled risks⁴⁰. A specific effort was made to position formal methods with respect to conventional methodologies used in industry.

(Katta, et al., 2013a) extends the Combined Harm Assessment for Safety and Security of Information Systems (CHASSIS) framework, cf. (Rasputnig, et al., 2012b), with a requirements traceability capability. The approach builds upon the Safety Traceability Approach (SaTrAp) (Katta, et al., 2013b), extending it to security-related artefacts (cf. Figure 78). The approach constitutes a process model defining what type of artefacts are generated during development and assessment activities, what type of relations between the artefacts should be cap-

³⁸ DARPA is an agency of the U.S. Department of Defense responsible for the development of new technologies for use by the military.

³⁹ I2O aims to ensure U.S. technological superiority in all areas where information can provide a decisive military advantage. It is one of the seven DARPA programme offices.

⁴⁰ Thus excluding unknown or uncontrolled risks (e.g. 0-day threats), for which in-depth defence remains the only viable approach.

tured, and how to extract traces. It is illustrated on a small part of on an Air Traffic Management Remote Tower example.

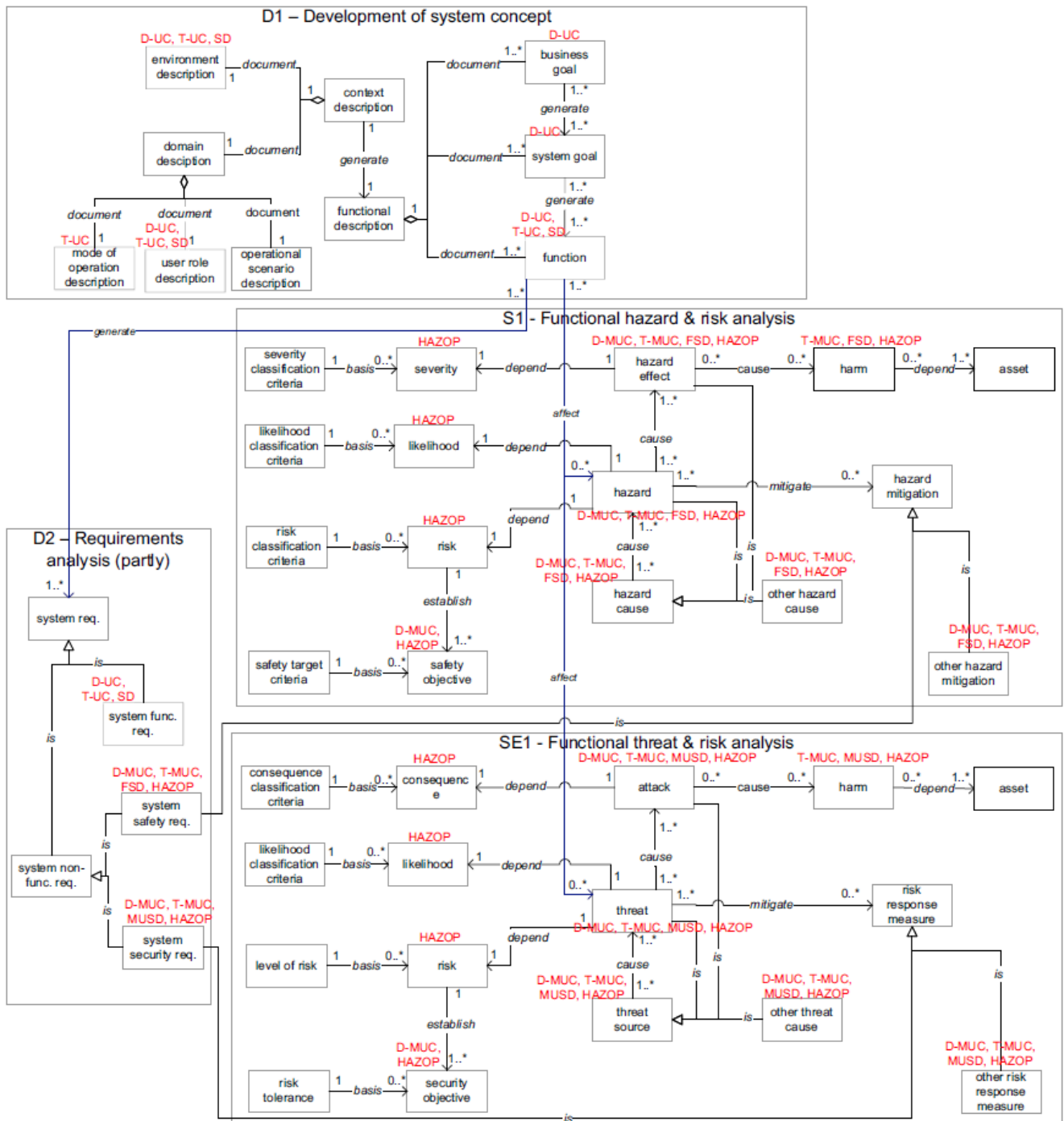


Figure 78: Traceability-process model with CHASSIS artefacts, relations & coverage (Katta, et al., 2013a)

(Kornecki, et al., 2013a) presents a practical case of Fault Tree Analysis (FTA) application for safety and security requirements engineering in the aviation domain, and more precisely on a gateway software ensuring two-way communications and data storage between simulation systems used in the scope of the American Next Generation Air Traffic Management system (NextGen). A safety and security requirements engineering process (cf. Figure 79) is proposed and results are exposed.

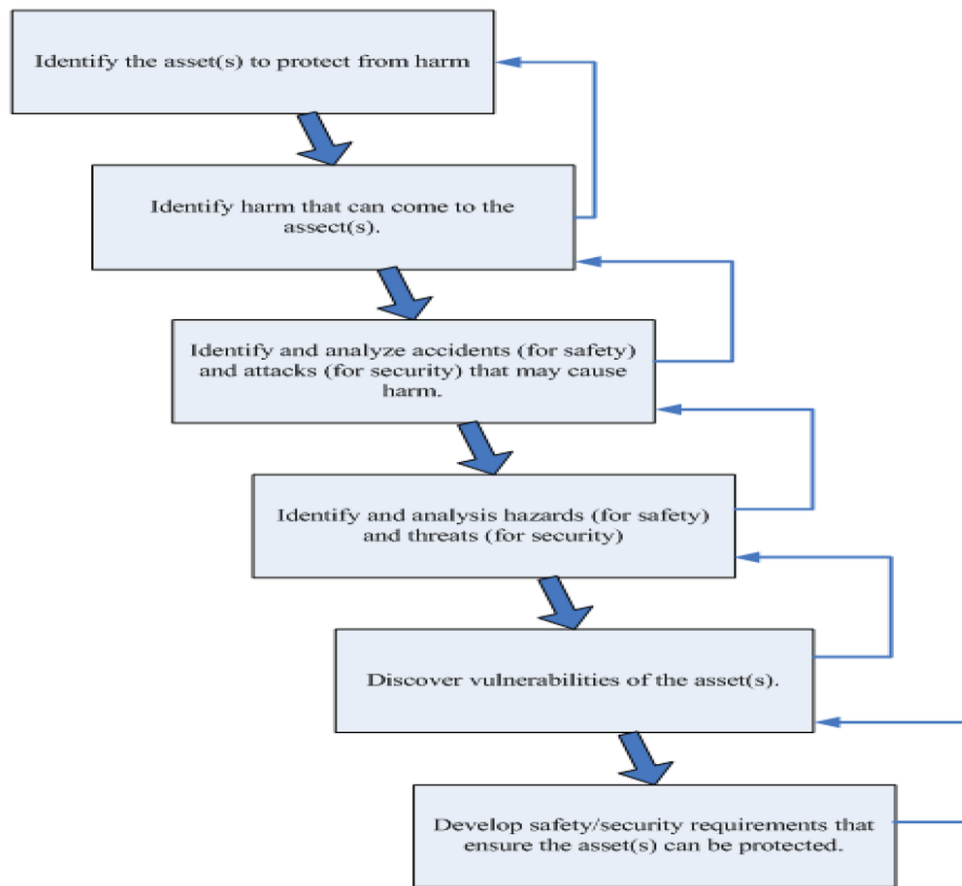


Figure 79: Safety/security requirements engineering process (Kornecki, et al., 2013a)

(Kornecki, et al., 2013b) discusses mutual relationships of safety and security properties in cyber-physical systems (CPS). The authors compare the traditional non-functional requirement (NFR) approach with a new Bayesian Belief Network (BBN) approach, which can be used when the factors related to the safety and security of the CPS are assumed to be randomly distributed. It is recalled that the NFR approach is a goal-oriented technique that can be applied to determine the extent to which specific objectives are achieved by a design. It uses a well-defined ontology that includes soft goals, contributions, and propagation rules. The approach relies on a qualitative assessment based on the concept of the contribution “satisficing” positively or negatively the soft goals. In contrast, the BBN approach uses likelihood estimates of a system’s configuration to evaluate quantitatively the achievement or denial of safety and security of CPS; likelihood estimates can include failure rates of system components and connections or could be likelihood of incidents impacting safety and security. An obvious challenge is to identify not only the likelihoods of events at specific nodes representing the system components but also the initial likelihoods of dependency relations between them (cf. Figure 80). The authors conclude that both these techniques can be used in a complementary manner to iteratively reassess safety and security of cyber-physical systems.

Parent Node(s)			SECURITY_CPS_		
ACCESS_CONTROL	AUDIT_LOG	ENCRYPTION	Yes	No	bar charts
Yes	Yes	Yes	1.0	0.0	
		No	0.5	0.5	
	No	Yes	0.5	0.5	
		No	0.25	0.75	
No	Yes	Yes	0.5	0.5	
		No	0.25	0.75	
	No	Yes	0.25	0.75	
		No	0.0	1.0	

Figure 80: Dependency relations for the Security node of the BBN (Kornecki, et al., 2013b)

(Kriaa, et al., 2013) marks a turning point in this state of the art. This paper does not advocate safety and security co-engineering by bringing together techniques from the two communities, but compares two already established approaches to safety and security co-engineering, namely the Combined Harm Assessment for Safety

and Security of Information Systems (CHASSIS) method (Raspotnig, et al., 2013b), and the Boolean logic Driven Markov Process (BDMP) technique (Piètre-Cambacédès, et al., 2010). Results of the comparison tend to show that the ultimate approach to co-engineering has not yet been found, since both approaches were found to complement each other.

(Mattila, 2013) addresses the different views on defining safety, security and social responsibility, and thus contributes to clarifying the relations between these terms.

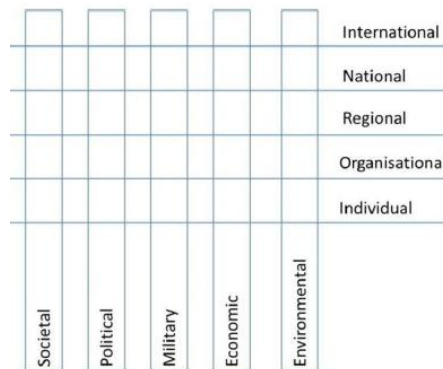


Figure 81: Conceptual layers (Mattila, 2013)

Safety and security are both needed for ensuring that cyber-physical systems live up to expectations, but often an intelligent trade-off is called for, because sometimes it is impossible to obtain optimal safety at the same time as optimal security. In the context of the Quality Calculus, (Nielson, et al., 2013) develops a *type system* for checking the extent to which safety and security goals have been met. Safety goals include showing that certain error configurations are in fact not reachable and hence do not require intelligent error handling. Security goals include showing that highly trusted communications can only be performed in highly trusted contexts. According to the authors, this is potentially too demanding and the Quality Calculus is therefore extended with a primitive for endorsing data to a higher trust level (accepting violations of the explicit flow) and for temporarily asserting a higher trust in the context (accepting violations of the implicit flow).

(Piètre-Cambacédes, et al., 2013) gives a comprehensive view of methods, models, tools and techniques that have been created in safety engineering and transposed to security engineering, or vice versa. Since the concepts of safety and security can somewhat vary according to the context, the first section of the paper deals with the scope and definitions that will be used in the sequel. The similarities and differences between the two domains are analysed. A careful screening of the literature (this paper contains 201 references) made it possible to identify cross-fertilizations in various fields such as architectural concepts (e.g. defence in depth, security or safety kernels), graphical formalisms (e.g. attack trees), structured risk analyses or fault tolerance and prevention techniques.

Type	Safety-oriented approach	Adaptation to security	Main ref.	Category
From safety to security				
Architectural concepts	Fault-tolerant architectures	Intrusion-tolerant architectures FRS technique; survivable networks Diversity-based intrusion detection	[8,75,77,79] [8,74] [84]	Tolerance
	Defense in depth	Defense in depth/security in depth	[86,34]	Tolerance
Graphical modeling	Fault trees	Threat trees, attack trees	[91,6]	Forecasting
	Dynamic fault trees	Dynamic attack trees	[111]	Forecasting
	BDMP	BDMP for security	[117,116]	Forecasting
Structured risk assessment	HAZOP	HAZOP for security Vulnerability Identification & Analysis HAZOPs	[120] [121,96] [122]	Forecasting
	Sneak circuit analysis	Sneak path security analysis	[124,125]	Forecasting
	Zonal analysis	Security zonal analysis	[122]	Forecasting
	Safety cases	Security Assurance case	[136–138]	Other
	FMEA	IMEA	[129,130]	Forecasting
	GEMS	GEMS for security	[142]	Prevention/ removal
	SIL (safety integrity levels)	SAL (security assurance levels)	[145,147]	Prevention/ removal
Testing	Fault injection	Fault injection, Fuzzing	[151]	Removal/ forecasting
	Software reliability growth	Software security growth modeling	[153]	Forecasting
From security to safety				
Architecture	Security kernel	Safety kernel	[158,159]	Prevention/ tolerance
Graphical modeling	Misuse case	Misuse case for safety	[174,175] [176,177]	Forecasting
	Misuse sequence diagram	Failure sequence diagram	[179]	Forecasting
Formal modeling	Non-interference property	Safe behaviors formalization	[163]	Prevention
	...Non-deducibility, causality	(fail-safe, fail-stop, etc.)	[166]	
	Integrity-oriented access control models (e.g. Biba model)	Model with multiple levels of integrity (Totel's model)	[167]	Prevention

Figure 82: An overall vision of existing cross-fertilizations between safety and security engineering tools and methodologies (Piètre-Cambacedes, et al., 2013)

(Piètre-Cambacedes, et al., 2013b) provides an overview of the work of the International Electrotechnical Committee (IEC) on the development of a series of standards dealing with the cyber security of nuclear power plant instrumentation and control systems. In particular, the status and content of the first, top level future document of the series, (IEC 62645, 2014), is described. The draft version of (IEC 62859, 2015), dealing with the coordination between safety and cyber security aspects, is also presented. Future work and perspectives associated with this new series of standards are finally discussed.

(Raspotnig, et al., 2013a) provides an extensive (50 pages) review of risk identification techniques for safety and security requirements. The added-value of the article is that it proposes an assessment framework. All techniques are assessed against the selected criteria to obtain knowledge on strengths and weaknesses of the different techniques in both the safety and security fields, and suggestions are provided to mutually enhance their efficiency.

(Roth, et al., 2013) proposes State/Event Fault Trees (SEFTs) for modelling and analysing the safety and the security aspects of cyber-physical systems (CPSs) in a common model. SEFTs make it possible to model deterministic state spaces and probabilistic failure behaviour with the visualization power of original Fault Trees (FTs). SEFTs provide a component concept where components (I) can communicate with each other and failure propagation is facilitated with in-ports (II) and out-ports (III). In SEFTs, the temporal dependencies are modelled within the components by the use of state charts, where the state changes can be triggered by exponentially distributed probabilistic events (IV), deterministic events (V) and triggered events (VI). These triggered events can be seen as externally controlled transitions. All events can be guarded by states (VII). This means that a guarded event is only able to fire if the connected state is active. States and events have to be connected by using so called temporal connections (VIII). In contrast, causal dependencies of the component's states and events are modelled, as typical in fault trees, with gates (IX) using causal connections(X), cf. Figure 83. The authors introduce SEFT models for basic vulnerabilities including denial of service (of message exchanges and of a component), spoofing, bypassing and reprogramming, and then propose an attack component, representing the cyber-physical attacker, nested in the system's environment and connected via ports to the system's

vulnerabilities. Such an attacker can execute various attack steps to reach his goal. The model allows for attack steps as subcomponents of the attack component which can be connected to each other through event ports to build logical attack queues, thus reducing the risk of getting lost in an over-detailed attack model. An important advantage of the above introduced method is that SEFTs can analyse stochastically dependent events.

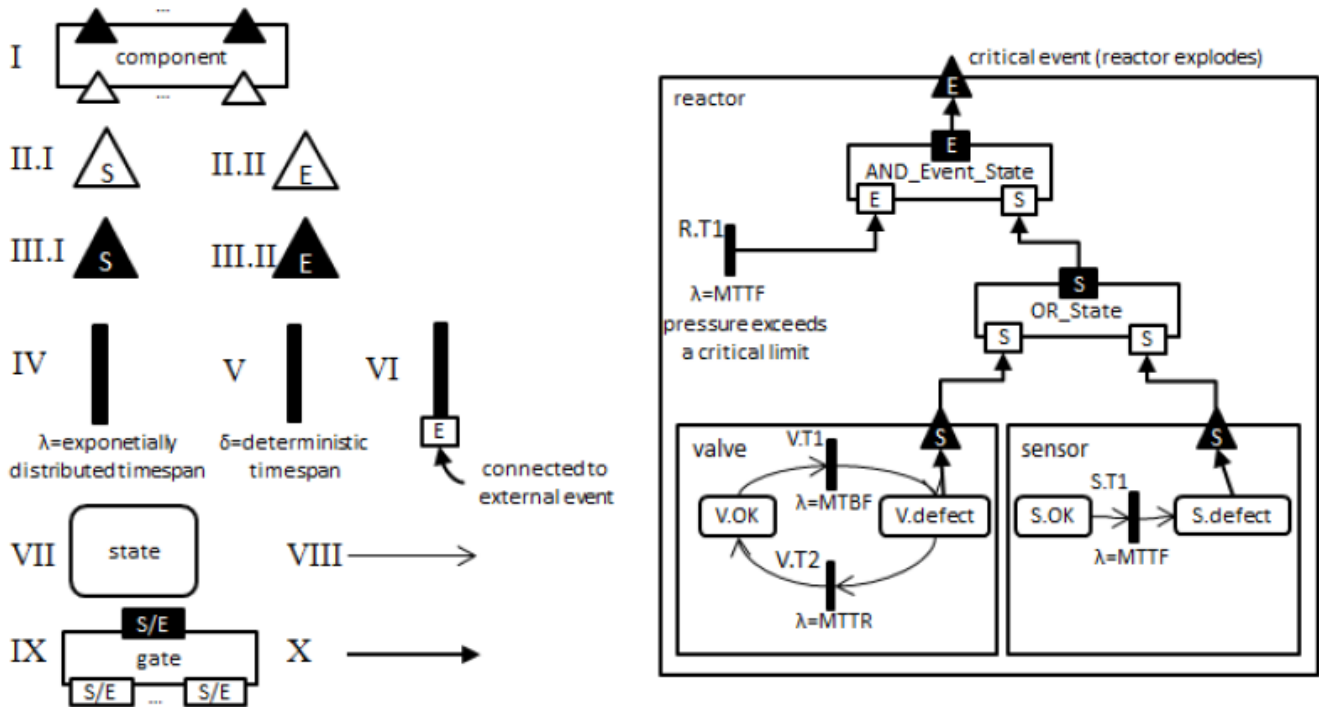


Figure 83: (a) SEFT modelling elements, and (b) Reactor modelled as a SEFT (Roth, et al., 2013)

(Rowe, 2013) starts by recalling that the increase of loadable software parts in Boeing aircraft (cf. Figure 84) brought the FAA to publish Special Conditions for aircraft network security (25-356-SC, 2008), (25-357-SC, 2007). To meet these special conditions, Boeing published the 787 Airplane Network Security Operator Guidance (ANSOG), which the FAA approved. The ANSOG contains requirements, e.g. keeping of security logs, and security recommendations, e.g. controlling access to wireless networks. Likewise, for the A380, Airbus includes “Aircraft Information System Security” guidance in Part 6 of Aircraft Limitations Section (ALS) of the aircraft maintenance manual, which EASA approved. The author proceeds with a presentation of (CASA CAAP 232A, 2013) of the Australian Civil Aviation Safety Authority, which provides generic guidance on aircraft network security covering detail in ANSOG. Then, an overview of the progress on the RTCA and EUROCAE airworthiness security standards is given, i.e. (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014), (RTCA DO-356, 2014) and (EUROCAE ED-204, 2014) / (RTCA DO-355, 2014). The presentation proceeds with an interesting discussion on the definition, the use and the history of loadable software, which brings (RTCA DO-178C, 2011) into play, together with its supplements. The author concludes that standards will overlap and future integration will be needed beyond 2014.

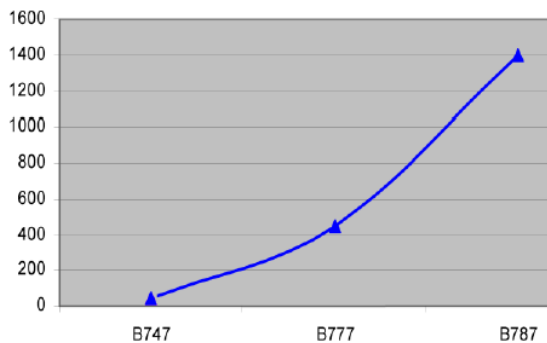


Figure 84: Quantity of loadable software parts in Boeing aircraft (Rowe, 2013)

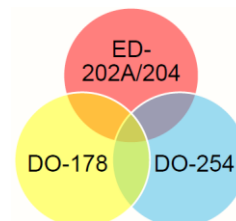


Figure 85: Standards overlap (Rowe, 2013)

(SeSaMo D2.1, 2013) provides the definition of 18 building blocks (BBs) for safety and security modelling, examples of which are (cf. Figure 75): encryption and decryption, signature generation and verification, node authentication, access control and traffic filtering, etc. A building block definition consists of the description of the BB, BB main interfaces, BB contribution to safety and/or security, as well as cross-influence between safety and security within the BB. The deliverable also provides a first attempt to quantify safety, security and their cross-influence (cf. Figure 86). Some of the BBs are further analysed within particular modelling environments and / or tool-chains. The last major part of the deliverable is an analysis of BBs within SeSaMo use-cases. This analysis provides a first feedback on modelling approaches.

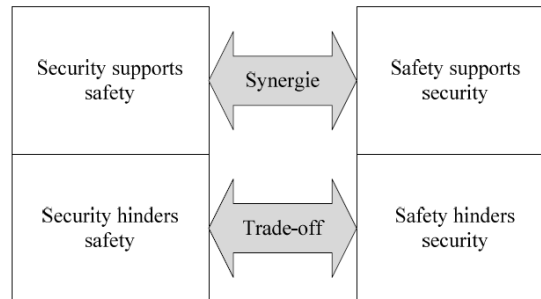


Figure 86: Attributes of Building Blocks (SeSaMo D2.1, 2013)

(SeSaMo D3.1, 2013) provides a specification of safety and security analysis and assessment techniques. It focuses on the definition of the safety and security metrics, and on the definition of the methodologies and techniques for the assessment of the safety and security properties. The document presents a number of core methodologies and techniques, but does not claim to be a comprehensive survey of all methods and techniques that exist in the field. The presented methodologies and techniques are: (1) stochastic models of interdependent infrastructures; (2) security-informed safety cases, cf. Figure 87; (3) message authentication and schedulability analysis on CAN bus; (4) Pareto frontier between safety and security constraints; (5) safety and security in the presence of denial of service attacks; (6) the KB3 workbench; (7) safety & security analysis of resilient services in communication networks; (8) formal metrics; (9) FMEA techniques; (10) safety and security analysis for railway application; and (11) safety analysis.

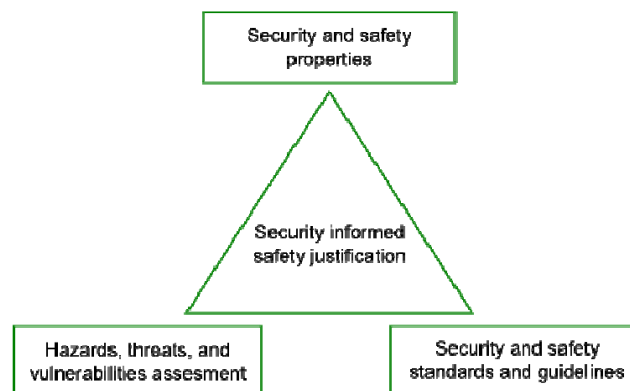


Figure 87: The security-informed safety case triangle of assessment (SeSaMo D3.1, 2013)

(Steiner, et al., 2013) builds upon (Fovino, et al., 2009) and (Förster, et al., 2010) by extending Component Fault Trees (CFTs) with Attack Trees (ATs) and with adapted qualitative and quantitative analyses. This leads to three classes of Minimal Cut Sets (MCSs): pure safety, pure security and mixed MCSs. The problem of the missing or hard to obtain probabilities for security events is avoided by the use of a hybrid rating scheme: probabilities for safety events and a simple rating for security events. Safety MCSs have a probability P, security MCSs have a rating R, and mixed MCSs have a tuple of probability and rating (P;R). P is calculated from the individual probabilities of the included safety events and R is calculated from the individual ratings of the included security events. Each class of MCSs can be ordered by itself. The tuples of the mixed MCSs can be ordered first by probability or by rating. A complete order is not possible for all cases.

	$P_1 < P_2$	$P_1 = P_2$	$P_1 > P_2$
$R_1 < R_2$	$MCS_1 < MCS_2$	$MCS_1 < MCS_2$	undefined
$R_1 = R_2$	$MCS_1 < MCS_2$	$MCS_1 = MCS_2$	$MCS_1 > MCS_2$
$R_1 > R_2$	undefined	$MCS_1 > MCS_2$	$MCS_1 > MCS_2$

Figure 88: Conditions for an order of mixed MCSs according to two tuples (Steiner, et al., 2013)

(Subramanian, et al., 2013) proposes the Non-Functional Requirements (NFR) technique that allows simultaneous evaluation of both safety and security at the architectural level, using qualitative reasoning to evaluate whether the properties have been achieved (cf. Figure 89). The approach is illustrated on an oil-pipeline control system.

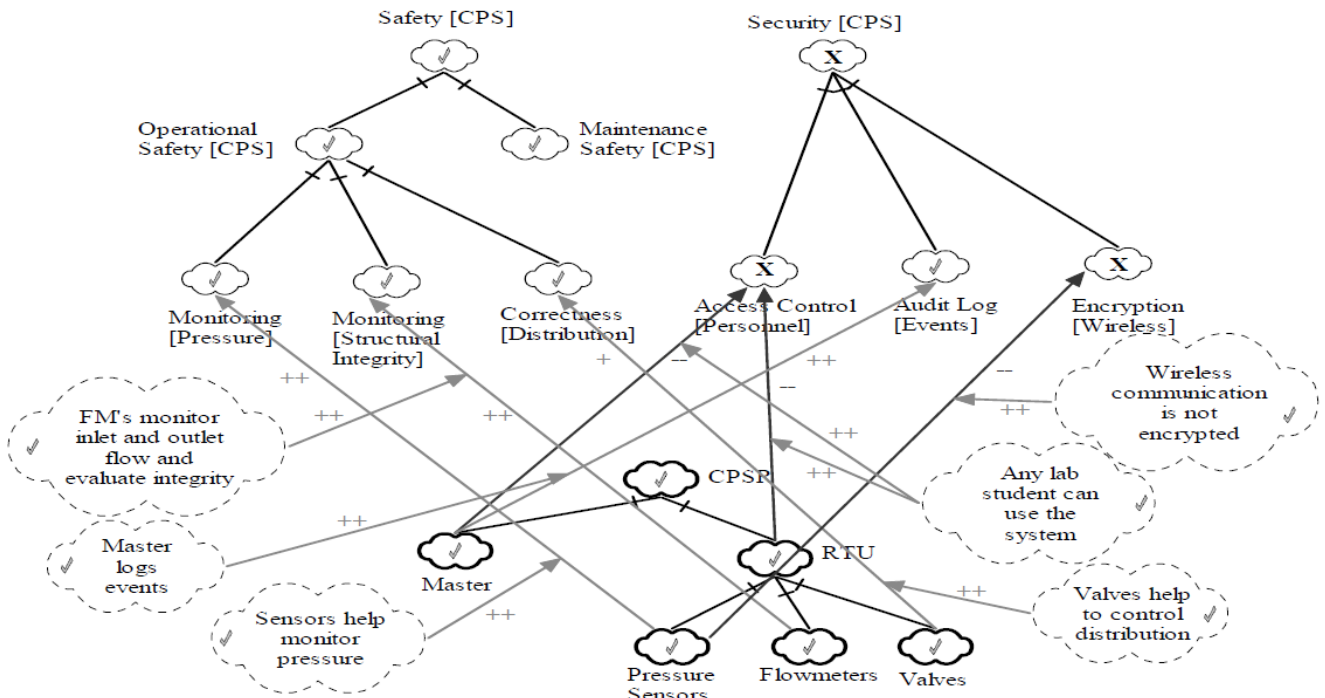


Figure 89: Phase 2 of assessment using the NFR approach (Subramanian, et al., 2013)

In (Vouk, 2013), software reliability (resp. security) engineering is defined as applied science of risk-based measuring, modelling, predicting, preserving and managing reliability (resp. security) of software-based systems to maximize customer satisfaction. The talk proceeds with the definition of fault vs. vulnerability, and asserts that engineers appear to avoid and eliminate vulnerabilities more by luck (aleatoric process) than through knowledge driven (epistemic) methods. The main reasons are fault rarity, complexity, process and human lacks, limitations, noise, and policies. The number of security faults represents approximately 1% of the total number of faults (cf. Figure 90). The talk continues with a discussion on operational profiles, and the state of science, in particular with respect to epistemic and aleatory uncertainty.

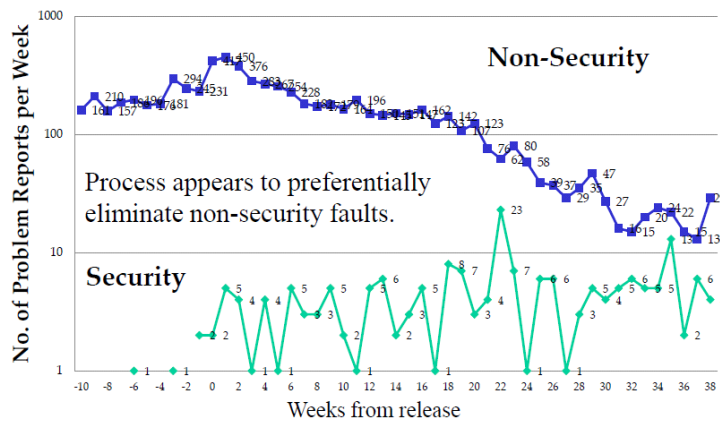


Figure 90: Security vs. non-security fault elimination during operational use (Vouk, 2013)

(Ward, et al., 2013) recognises that while functional safety hazard analysis and risk assessment processes could be used for threat analysis, these methods need extension and adaptation to the cyber security domain. This paper describes how such a method has been developed based on the approach described in (ISO 26262-1, 2011)- (ISO 26262-10, 2012) and the related MISRA Safety Analysis Guidelines. In particular key differences are described in the understanding of the severity of a security attack, and the factors that contribute to the probability of a successful attack. The paper also explores some potential future directions, such as how the threat analysis and risk assessment can be used to support an assurance case for cyber-security.

(Aprville, et al., 2014) introduces SysML-Sec, a SysML-based model-driven engineering environment aimed at fostering the collaboration between system designers and security experts, at all methodological stages of the development of an embedded system. The requirements are captured in a component-centric manner through existing SysML diagrams with only minimal extensions; they are then derived into security and cryptographic mechanisms, security properties, which can be formally verified. The authors are not directly concerned by safety and security co-engineering, but they pay particular attention to validating the innocuousness of security mechanisms, both computationally and in terms of bandwidth usage, with respect to safety requirements, whose specifications are outside the scope of the paper (cf. Figure 91).

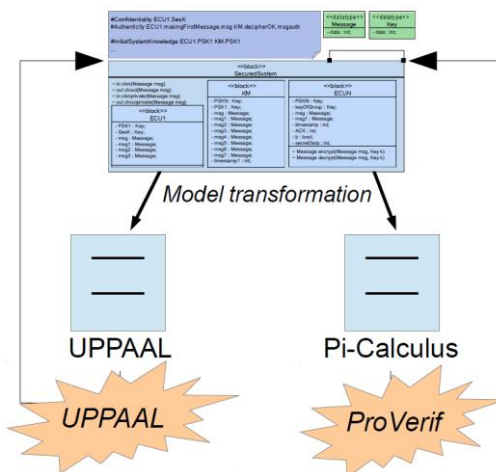


Figure 91: Model transformations for proving safety & security properties (Aprville, et al., 2014)

(Bieber, et al., 2014) reports on the development of common models and tools to assess both safety and security of avionics platforms. The authors studied the adaptation of models devised for safety assessment in order to analyse security; they describe a security modelling and analysis approach based on the AltaRica language and associated tools. The preliminary lessons learnt are: (i) the layered model for the safety analysis of avionics platform can be reused efficiently for the security model; only the Agent layer needs to be added to model threat activation; (ii) the AltaRica code can be easily extended to deal with security threats; the main addition is related with the modelling of confidentiality; (iii) it is required to model the propagation of threats due to the use of shared resources; (iv) the OCAS sequence generator can be used successfully to generate threat scenarios; (v) using DAL to model the security level of nodes in the architecture is possible (cf. Figure 92); extra work is needed in order to check the consistency of DAL allocation rules with security level allocation rules.

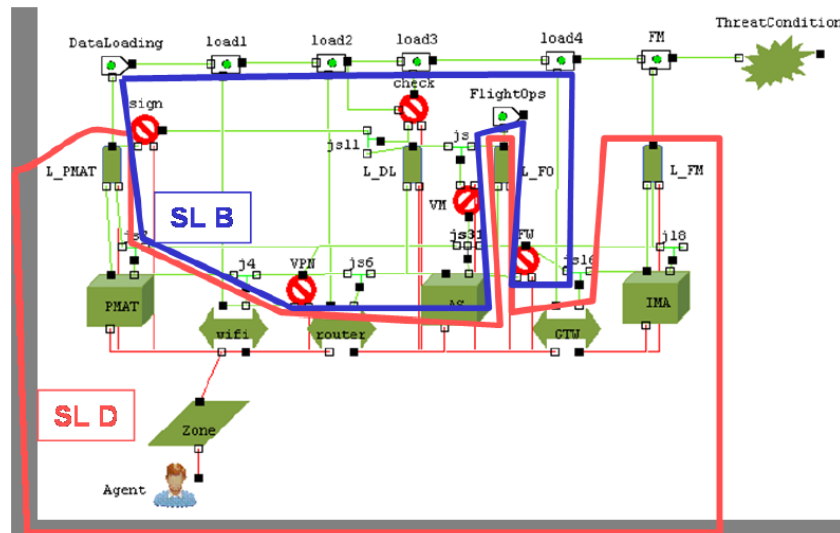


Figure 92: Security Level Allocation (Bieber, et al., 2014)

(Braband, 2014a) builds upon (Bock, et al., 2012). This paper defines an IT security framework, built on the well-known safety and certification processes from (CENELEC EN 50129, 2003), which aims at separating IT security and safety requirements as well as certification processes as far as possible, in order to match the approach for IT security requirements based of the ISA 99 / IEC 62443 standard series⁴¹. This is achieved by integrating safety-related security requirements into the safety process and the safety case. The paper starts with a discussion of the normative background, and then defines a reference architecture (cf. Figure 93). A short overview of the basic concepts of ISA 99 / IEC 62443 is given and it is finally discussed how these concepts could be adapted to the railway automation domain. The highlights of the paper were also presented at the Safety and Security workshop in Kaiserslautern (Braband, 2014b).

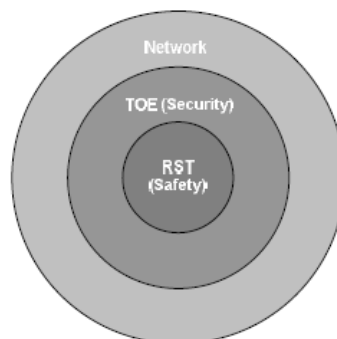


Figure 93: The onion skin model (Braband, 2014a)

(Brunel, et al., 2014a) proposes an approach based on Alloy (Jackson, 2012) to formally model and assess a system architecture with respect to safety and security requirements. The authors illustrate this approach by considering as a case study an avionic system, which provides guidance to aircraft. The paper shows how to define in Alloy a meta-model of avionic architectures with a focus on failure propagations. It then expresses the specific architecture of the case study in Alloy. Finally, the authors express and check properties that refer to the robustness of the architecture to failures and attacks.

Building upon (Brunel, et al., 2014a) and (Bieber, et al., 2014), (Brunel, et al., 2014b) proposes an integrated process (cf. Figure 94) in which system engineers design the system architecture, safety and security engineers define the failure modes and specify the propagation of failures and attacks inside each component. The analyses with respect to safety and security properties are then performed using Alloy. The approach is illustrated on a landing aircraft test case using Melody, the system engineering workbench from Thales, and Safety Architect, the Failure Mode, Effects and Analysis (FMEA) tool from All4Tec.

⁴¹ See (IEC/TS 62443-1-1, 2009), (IEC 62443-2-1, 2010), (IEC/TR 62443-3-1, 2009), and (IEC 62443-3-3, 2013).

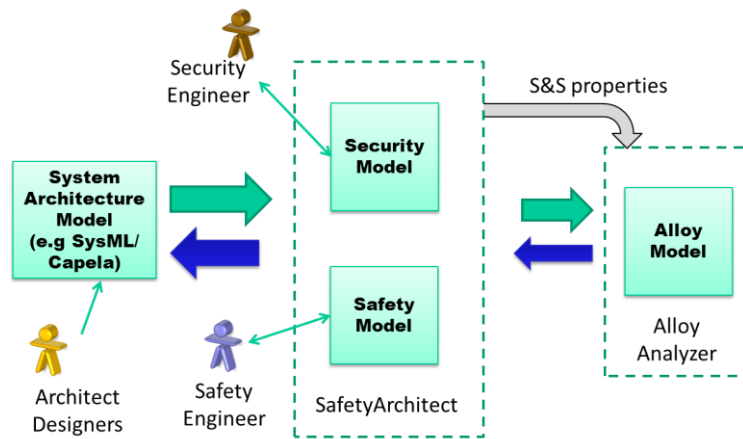


Figure 94: Integrated safety and security verification process (Brunel, et al., 2014b)

(Favaro, et al., 2014) is an overview of the SeSaMo project’s highlights – see (SeSaMo, 2012), (SeSaMo D2.1, 2013), (SeSaMo D3.1, 2013) and (SeSaMo D4.1, 2014) for details. One of the presented highlights is the security-informed safety cases. According to the authors, addressing these safety cases implies: (i) reviewing how the claims might be impacted by security; (ii) reviewing security controls to see if these can be used to provide an argument and evidence for satisfying the claim – cf. Figure 95; (iii) reviewing the impact of deploying controls on architecture and implementation; and (iv) applying an iterative layered approach considering three abstraction layers. In the 1st layer, the system requirements, safety and security policies are analysed; in the 2nd layer, the abstract system components combined according to the abstract architecture are analysed; in the 3rd layer, the implementation of specific components and their integration within the specific architecture are analysed. As in (Schwarz, et al., 2014), the presentation concludes on engineering integration pros and cons: the arguments in favour of integrated process include the jeopardizing effects of security on safety, the similar but possibly contradictory countermeasures, the need to consider both from the beginning; the arguments against an integrated process include the incompatible lifecycles, the disjoint communities, and the integration overheads.

Claim	Control
C22 Training OK.	Awareness and Training (AT) AT-2 Security Awareness AT-3 Security Training
C42 Supply chain integrity	System and Services Acquisition (SA) SA-12 Supply Chain Protection SA-12-3 Trusted Shipping SA-12-7 Independent Analysis and Penetration Testing
C52 Vulnerabilities and hazards addressed	System and Services Acquisition (SA) SA-10 Developer Configuration Management SA-11 Developer Security Testing SA-13 Trustworthiness

Figure 95: Mapping safety claims onto NIST security controls (Favaro, et al., 2014)

(Fruth, et al., 2014) is a borderline paper in this survey of safety and security engineering practices, as it focuses on a unified framework for safety and security alarm communication in human-machine interaction scenarios. In the paper, the topic is termed *risk communication*. In this paper a selection of current safety and security risk communication standards and recommendations are compared using selected evaluation criteria (cf. Figure 96). The authors focus on alarm system standards in the industrial process automation domain and intrusion detection systems known from conventional desktop IT domain. A series of DIN standards and recommendations, which are available free of charge from approved industrial and computer security organisations, are reviewed. According to the authors, current risk communication standards and recommendations offer domain-specific solutions, but are not sufficient to fulfil safety and security requirements of distributed IT environments with safety and security properties. Therefore a new model based approach is introduced.

Standard	Content	Advantages	Properties not covered
<i>Industrial process control (Safety)</i>			
DIN EN 62541-9 / IEC 62541 (2012) [4]	Model	1) Formal description of alarms via a holistic information model (OPC unified architecture) 2) Exemplary models	1) No providing of information acquisition 2) Only focus on system failures (safety) 3) No user specific model/design examples
NA 102 (Worksheet, 2008) [3]	Procedure	1) Providing of all four stages 2) Holistic and interdisciplinary approach of alarm management design 3) Optical and acoustical design pattern 4) Examples of practical experiences	Only focus on system failures (safety)
VDI/VDE 3699, Blatt 5 (German Draft, 2013) [6]	Model	Strategies to minimise the cognitive overload of operators (e.g. minimising, automated selection, and prioritisation of alarms)	1) No providing of information acquisition and analysis 2) Only focus on system failures (safety) 3) Only optical alarm design
<i>Desktop IT (Security)</i>			
ISO/IEC DIS 27039 (Draft, 2013) [5]	Procedure	1) Providing of all four stages 2) Holistic procedure of selection, deployment and operation of IDS in an organisation	1) Only focus on cyber attacks (security) 2) Only general description of handling of IDS alerts (information and severity of attacks) - no user specific design approaches
BSI - Guideline for introduction of IDS (2002) [1]	Procedure	1) Providing of all four stages 2) Holistic procedure of selection, deployment and operation of IDS in an organisation	1) Only focus on cyber attacks (security) 2) Only general description of alert and incident handling - no user specific design approaches

Figure 96: Comparison of selected standards / recommendations (Fruth, et al., 2014)

(Gebauer, 2014) discusses the evolution of the Automotive Functional Safety standard (ISO 26262-1, 2011) - (ISO 26262-10, 2012) in particular with respect to its impacts on the automotive industry, and asserts the need for a dedicated security standard. The author points out that following an analysis of attacks and attacker motivations, four protection layers are currently being deployed (cf. Figure 97). However, an OEM typically addresses only one level. This is one of the major reasons why a security standard would be helpful, so as to bring the community together, and ensure the overall consistency of the countermeasures.

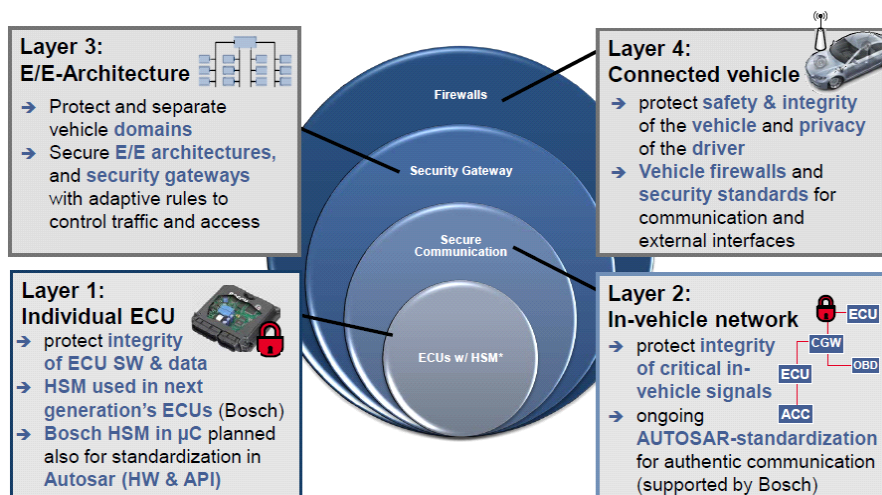


Figure 97: Protection layers (Gebauer, 2014)

(Joyce, et al., 2014) recalls that aircraft type certification currently acts in the absence of comprehensive rules and guidance for how cyber-security affects safety (cf. §3.2.4 for more details) and explains how the aerospace community has addressed the challenges of integrating safety and security through guidance in recently pub-

lished standards (RTCA DO-326A, 2014) / (EUROCAE ED-202A, 2014), (RTCA DO-356, 2014)⁴² and (RTCA DO-355, 2014) / (EUROCAE ED-204, 2014), which are anticipated to become reference documents for the certification of aircraft and aircraft systems in the context of information security. The paper highlights the fact that the elaboration of the 2014 version of the Airworthiness Security Process Specification standard was highly disputed in the community, on at least three topics: (i) the safety and security co-engineering process; (ii) the influence of security on the safety Design Assurance Levels (DALs), and (iii) the list of security activities to be performed and the level to which they have to be performed to ensure the required security assurance.

Indeed, in (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010), the security activities were depicted as embedded within the safety activity (cf. Figure 98): the safety functional hazard analysis was seen as including threat conditions along with failure conditions. Jeff Joyce explains that during 2013, in the draft versions of the A standard, security activities were extracted from the safety activities and positioned parallel to the safety activities. In the 2014 release, security activities are no longer positioned next to the safety activities⁴³; instead mainstream system engineering activities have been inserted between them (cf. Figure 139 on page 154). This does not prevent security information to flow directly to safety, but it is not mandated.

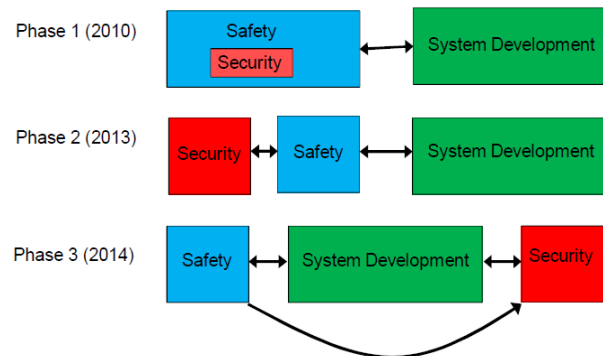


Figure 98: Evolution of the DO-326 standard in time (Joyce, et al., 2014)

(Kriaa, et al., 2014) recalls that the digitalization of industrial control systems (ICS) raises several security threats that can endanger the safety of the critical infrastructures supervised by such systems. This paper presents an analysis method that enables the identification and ranking of risks leading to a safety issue, regardless of the origin of those risks: accidental or due to malevolence. This method relies on a modelling formalism called BDMP (Boolean logic Driven Markov Processes) that was initially created for safety studies, and then adapted to security. The use of the method is first illustrated on a simple case to show how it can be used to make decisions in a situation where security requirements are in conflict with safety requirements. Then it is applied to a realistic industrial system: a pipeline and its instrumentation and control system in order to highlight possible interactions between safety and security.

(Mazzini, et al., 2014) provides an overview of the SeSaMo project (SeSaMo, 2012) two years after its kick off. The paper starts by recalling the safety and security convergence problem, the related work and what appeared in 2012 as the remaining needs, i.e. progress on quantitative security analysis techniques, methods to cope with safety and security from requirement elicitation to system design and analysis, enriched languages to deal both with security and probabilistic/stochastic aspects, and an integrated validation framework. These needs have led SeSaMo to focus on a model-driven process for the compositional development of safety and security critical systems. One axis is the definition of building blocks, cf. (SeSaMo D2.1, 2013). Another axis relates to analysis methods: quality calculus (Nielson, et al., 2013), security-informed safety cases (Paulitsch, et al., 2012). A third axis relates to trade-off decision support through the exploration of Pareto frontiers. The authors then discuss how different safety standards have, or have not, integrated security requirements, e.g. see above discussion on (S + IEC 61508, 2010), concluding that the path to convergence lies in the definition of *interaction points* between separate safety and security processes (cf. Figure 99), rather than on a unified process. It is pointed out that, even if the processes remain separate, their work-products are shared and unique. The paper closes on the description of the toolset, mainly composed of *medini analyze*⁴⁴ and CHES⁴⁵.

⁴² Known as DO-YY3 when still a draft. The European Organization for Civil Aviation Equipment counterpart, ED-203, is not scheduled to be published at the same time.

⁴³ Despite the expressed preference of some regulation authorities.

⁴⁴ <http://www.ikv.de/index.php/en/products/functional-safety>.

⁴⁵ <http://www.chess-project.org>.

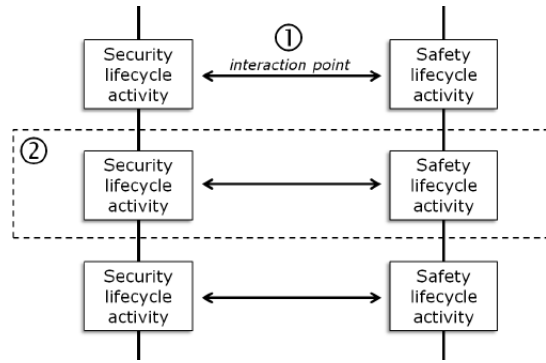


Figure 99: Safety and security lifecycle activities (Mazzini, et al., 2014)

(79 FR 60574, 2014) is a Federal Register notice calling for public comments on the National Highway Traffic Safety Administration's research program on vehicle electronics, in particular the need for safety standards with regard to electronic systems in passenger motor vehicles. The notice presents background information on safety in the motor vehicles and motor vehicle equipment domain and summarizes the examination results. From our safety and security co-engineering point of view, it is interesting to notice that *Security Needs to Prevent Unauthorized Access to Electronic Components* is one of the three topics addressed in the NHTSA research. As part of this topic, NHTSA has identified two general process-oriented approaches to address cyber-security concerns: the first is design and quality control processes, e.g. (NIST Cybersecurity Framework, 2014); the second is through establishing robust information sharing forums. Interesting also, is the list of questions explicitly asked by the NHTSA, e.g.: (i) could security assurance be handled within a modified framework of existing safety process standards (such as FMEAs, FTAs, ISO 26262) or does “design for security” require its own process? (ii) what types of metrics are available to test a vehicle’s ability to withstand a cyber-attack? (iii) are there any common design characteristics that help ensure a minimum level of security from unauthorized access to a vehicle’s electronic control systems? (iv) what performance-based tests, methods, and processes are available for security assurance of automotive electronic control systems? (v) are there hardware, software, watchdog algorithm, etc. requirements or criteria that would help differentiate algorithm designs that are more secure against cyber-attack?

(Ramirez, et al., 2014) formally compares two industrially relevant and popular models of non-interference, namely, the model defined in (Rushby, 1992) and the GWV one (Greve, et al., 2003). The authors create a mapping between the objects and relations of the two models. They prove a number of theorems showing under which assumptions a system identified as “secure” in one model is also identified as “secure” in the other model. Using two examples, they illustrate and discuss some of these assumptions. Their main conclusion is that the GWV model is more discriminating than the Rushby model. All systems satisfying GWV’s separation also satisfy Rushby’s non-interference. The other direction only holds if we additionally assume that GWV systems are such that every partition is assigned at most one memory segment. All of the proofs have been checked using the Isabelle/HOL proof assistant.

GWV	Rushby
$S_g : \mathcal{S} \times \mathcal{A}$, with $s_g.s \in \mathcal{S}$ and $s_g.a \in \mathcal{A}$	states in \mathcal{S} , actions in \mathcal{A}
Partition, \mathcal{D}	Domain, \mathcal{D}
Memory segment, \mathcal{M}	Object, \mathcal{N}
output _g	output
current(s_g)	dom($s_g.a$)
segs(p)	alter(p)
select(s_g, n)	contents($s_g.a, n$)
next(s_g).s	step($s_g.s, s_g.a$)
$\{s \mid \exists s' \in \text{segs}(u).s \in \text{dia}(s')\}$	observe(u)
$s \sim_g t$	$s \sim t$
$u \rightsquigarrow_g v$	$u \rightsquigarrow v$

Table 1: Mapping between the elements of the GWV and Rushby models (Ramirez, et al., 2014)

In (Raspotnig, 2014), the author combines safety and security requirements elicitation supported by the Combined Harm Assessment for Safety and Security of Information Systems (CHASSIS) method and a Security Conceptual Model (SeCM). For this PhD, it has been important to compare the safety and security fields, but more importantly to investigate the concrete foundations, i.e., techniques that exist in each field for requirements elicitation; this has been done by identifying common characteristics for certain techniques through a set of cri-

teria – see also (Raspotnig, et al., 2013a). As a result, the CHASSIS method includes three modelling techniques: the Diagrammatical Misuse Cases (D-MUC), Misuse Sequence Diagrams (MUSD) and the new Failure Sequence Diagrams (FSD) – see also (Raspotnig, et al., 2012a). CHASSIS also includes templates for documenting important harm information, namely Textual Misuse Cases (T-MUC) and HAZard and OPerability (HAZOP) tables. These techniques and associated templates are organised into a Harm Assessment Process that consists of specific activities for safety and security assessment activities. One of the combined safety and security activities is the trade-off analysis, where four interdependencies are used for investigating mitigations. A roadmap is given for further enhancements.

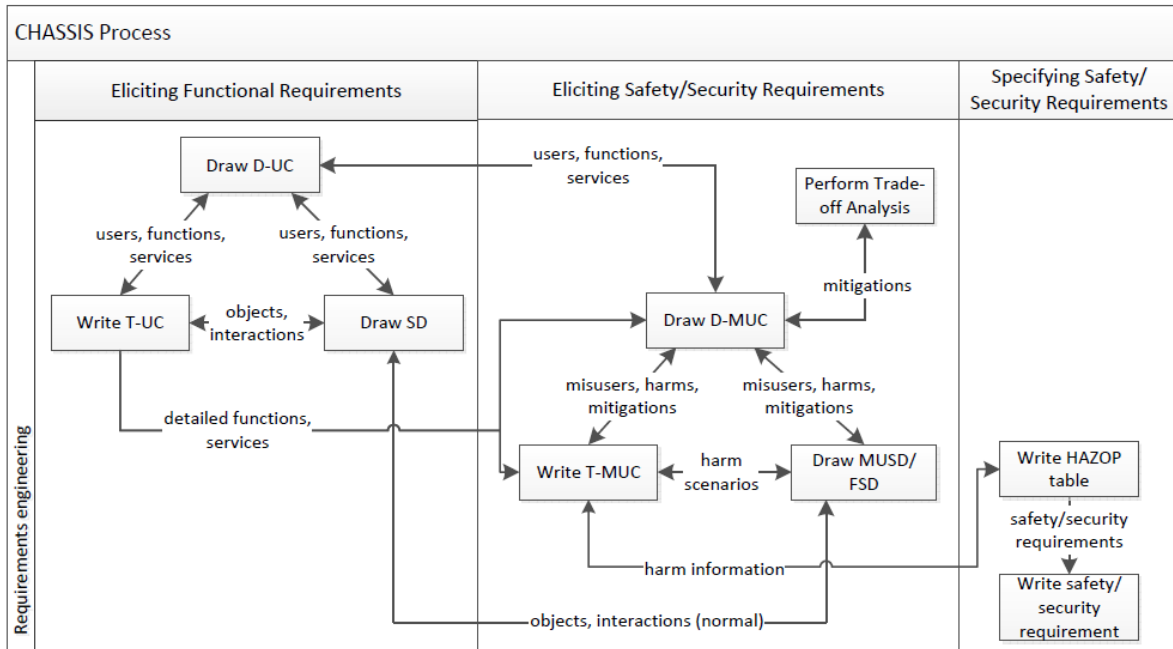


Figure 100: The CHASSIS process diagram (Raspotnig, 2014)

(Schmittner, et al., 2014b) and its shorter counterpart published in a satellite workshop (Schmittner, et al., 2014a) present a new technique for security engineering called Failure Mode, Vulnerabilities and Effect Analysis (FMVEA) that extends the classical Failure Mode and Effect Analysis (FMEA) technique used in safety engineering, cf. Figure 116. The approach is illustrated on a system of intelligent and cooperative vehicles case, cf. Figure 101. The authors report that whilst the approach provided a good overview of vulnerable functions, the risk rating remained a relatively complex process, essentially because attacks consisted of multiple steps. The authors recall that FMVEA (like FMEA) is best used for an early design time assessment of systems, allowing for the anticipation of the effects of potential failures and threats during design time.

ID	component	Vulnerability / Failure Cause	Threat Mode / Failure Mode	Threat Effect / Failure Effect	System Status	System Effect	Severity	System Susceptibility	Threat Properties	Attack / Failure Probability	Risk
1	OTA	insufficient authentication of TNOS	Attacker masquerades itself as TNOS and sends own firmware update	Attacker deploys own firmware	same susceptibility in all system states	safety-critical, Attacker has control over the vehicle	6	4	4	8	48
2	OTA	wireless connection, susceptibility to jamming	Attacker interrupts OTA	Update is interrupted	Updating	none	1	6	4	10	10
3	OTA	disturbance while transmitting update	Update data is incorrect	incorrect firmware is applied	Updating	safety-critical, firmware could include critical faults	6	6	36
4	OTA	connection is lost	Data missing from update	Update is interrupted	Updating	none	1	6	6
5	bluetooth connection	attacker exploit buffer overflow in bluetooth implementation	The attacker could use a already connected device and extend it's privileges	Attacker is able to execute code on TCU	connected to compromised device	safety-critical, Attacker has control over the vehicle	6	3	4	7	42
6	external media	no congestion control at TCU	data overflow at TCU from streaming data	TCU malfunctions	streaming connection	TCU services not longer available	3	6	18
7	transmit diagnostic data	man in the middle attack on GSM base station	Attacker is manipulating diagnostic data	wrong data is transmitted	system receives "limp home command" from TNOS	reduced functionality	2	3	4	7	14

Figure 101: Failure Mode, Vulnerabilities and Effect Analysis (Schmittner, et al., 2014a)

(Schmittner, et al., 2014c) is a very short paper (2 pages) partially funded by the CARONTE (Creating an Agenda for Research ON Transportation sEcurity) project. The authors briefly describe three challenges: (i) since connected vehicles form a connected system of systems, safety and security must be ensured at the sub-system level as well as the systems combined; (ii) with an open system we cannot regard a vehicle system to be safe unless the security of the system is assessed and assured; (iii) connected, automated and intelligent vehicles will have more conflicts between privacy and safety and security requirements, which calls for an integrated approach for solving these conflicts. The authors then analyse the state of the art of safety and security co-engineering standards for connected, automated and intelligent vehicles, identify some gaps and conclude by some directions for improvements.

(Schneider, 2014) proposes a contract-based approach called ConSerts to address the challenges of openness and runtime adaptation which are common the safety and security critical systems. The work is performed as part of the (ARTEMIS EMC2, 2014) project and applied on a Tractor Implement Management system.

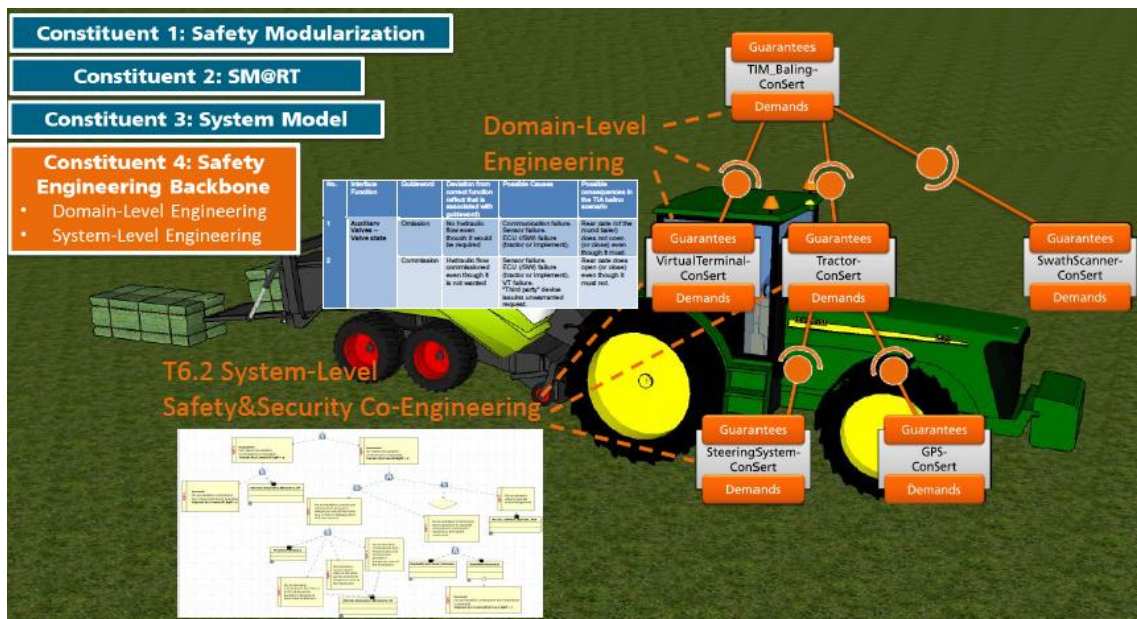


Figure 102: ConSerts Overview – Engineering Backbone (Schneider, 2014)

(Schoitsch, 2014) traces the evolution of three different safety standards that have integrated security concerns: the Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems from (IEC 61508-1, 1998) - (IEC 61508-7, 2000) to (S + IEC 61508, 2010), the Functional Safety - Safety Instrumented Systems for the Process Industry Sector (IEC 61511-SER, 2004), and the Airworthiness Security Process Specification, from (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010) to (RTCA DO-326A, 2014). Since Erwin was involved in the elaboration of (S + IEC 61508, 2010), it is interesting to read his record of what happened behind the scene, between the two editions of the standard.

(Schwarz, 2014) compares the merits of safety and security metrics by leveraging previous work on a survey of security metrics (Rudolph, et al., 2012). The author asserts that security metrics display significant deficiencies compared to safety metrics (cf. Figure 103).

Safety	Security
Probabilistic nature of safety incidents, stochastic independence of faults	no stochastic independence of security incidents, probabilities not applicable
Basic safety metrics (e.g., reliability)	Lack of true metrics or <u>direct</u> indicators
Basic reliability arithmetic	Security as a discontinuous property that poorly fits into a continuous calculus
Reliability composes (to some degree)	Security is not invariant under composition or stepwise refinement
Test coverage as approximation for software reliability	Lack of adequate software metrics (fuzz testing as an [im]proper substitute for test coverage?)

Figure 103: Safety vs. security metrics (Schwarz, 2014)

(SeSaMo D4.1, 2014) presents the SeSaMo integrated design and evaluation methodology, which aims at combining best practices in safety and security engineering as a unified process. The SeSaMo approach is based on the idea of establishing points of contact between parallel safety and security lifecycle activities. According to the authors, this approach of parallel processes with “weak” trade-off interactions and “strong” interactions for joint activities has the advantage of providing a smooth migration path for the standards communities. This extensive document (121 pages) starts by addressing the foundation stones on which the methodology is based, i.e.: (i) terminology, by which security concepts (i.e. attack, vulnerability and intrusion) are defined in terms of dependability concepts, and a mapping is proposed between safety and security terms, e.g. *hazardous substance* \approx *internal threat*; (ii) levels, may they be safety or security levels; (iii) ways of reducing risk, may they be techniques, measures and / or controls; (iv) the ALARP principle; and (v) security-informed safety cases (cf. Figure 95). Then, a generic process is proposed (cf. Figure 104), based on the risk assessment approach of (ISO/IEC 27005, 2011) and the safety lifecycle of (IEC 61508-1, 1998) - (IEC 61508-7, 2000).

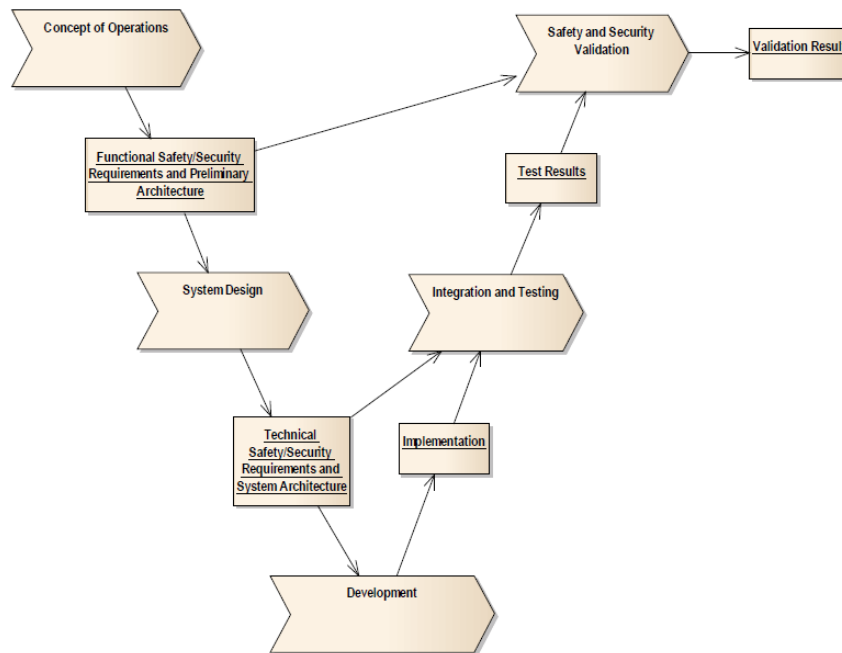


Figure 104: Generic Process Definition (SeSaMo D4.1, 2014)

Each activity of the process is detailed graphically (e.g. cf. Figure 105) and textually in terms of overall description, inputs and outputs. Following the formalized description of the generic process, two perspectives on its intended use are provided: (i) a model-based perspective discusses the intended use of tool support for the process; (ii) an assurance perspective, with a particular focus on security-informed safety cases, cf. (SeSaMo D3.1, 2013). The report closes on an analysis of the compatibility of the generic process with existing approaches in the automotive, avionics, railway, and industrial process control domains. The authors conclude in five points:

- concepts: there is a need to establish a lingua franca or even a common ontology;
- methodology: the unification of well-accepted approaches, typically related to risk management, allow for ad hoc hooks for specific techniques and measures;
- model-based development: heterogeneous but pervasive tool support, with positive side-effects on re-assurance through keeping the assurance in models;
- security-informed safety case: express safety case about system behaviour in terms of claims-arguments-evidence; review how the claims might be impacted by security; review security controls to see if these can be used to provide an argument and evidence for satisfying the claim; review architecture and implementation impact of deploying controls and iterate the process;
- standards: security standards are often based on security controls, a concept that embraces a wide range of different interventions covering process, product and organisation; in contrast, safety standards are typically based on an engineering life cycle model; the communities need to find a way of combining both approaches within a common framework.

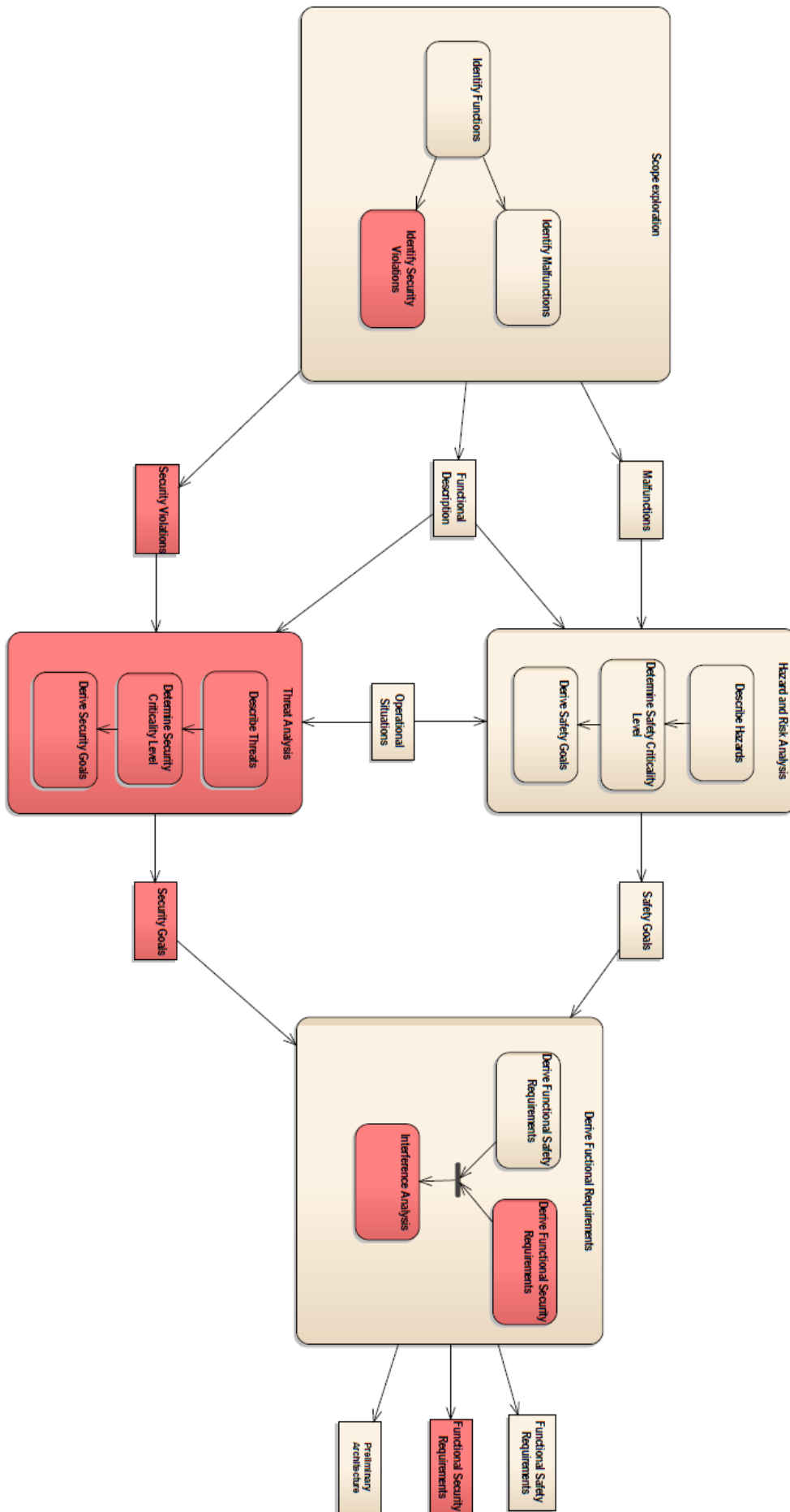


Figure 105: The concept of operations (SeSaMo D4.1, 2014)

(Subramanian, et al., 2014) is an extension of the Non-Functional Requirements (NFR) technique published in (Subramanian, et al., 2013), in which the original qualitative reasoning is extended with a quantitative assessment.

(Tiwari, et al., 2014) presents an approach for detecting sensor spoofing attacks on a cyber-physical system. The approach consists of two steps. In the first step, the authors construct a safety envelope of the system. Under nominal conditions, i.e. when there are no attacks, the system always stays inside its safety envelope. In the second step, an attack detector is built, i.e. a monitor that executes synchronously with the system and raises an alarm whenever the system state falls outside the safety envelope (cf. Figure 106). The authors synthesize safety envelopes using a modified machine learning procedure applied on data collected from the system when it is not under attack. They present experimental results that show the effectiveness of their approach, and also validate the novel features that are introduced in the learning procedure.

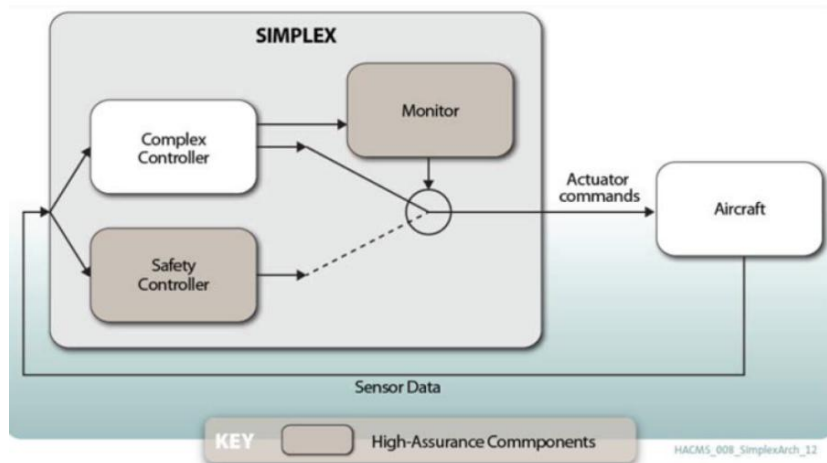


Figure 106: Runtime Assurance Architecture (Fisher, 2013)

(Tverdyshev, 2014) reports that, if MILS⁴⁶ was initially designed to address security issues, this approach actually shows excellent safety properties architecture. The MILS acronym is thus more and more used as noun, to alleviate the focus on security. The authors assert that architecture, and in particular the MILS approach (cf. Figure 107), is a good starting point to look for synergies & divergences between safety and security.

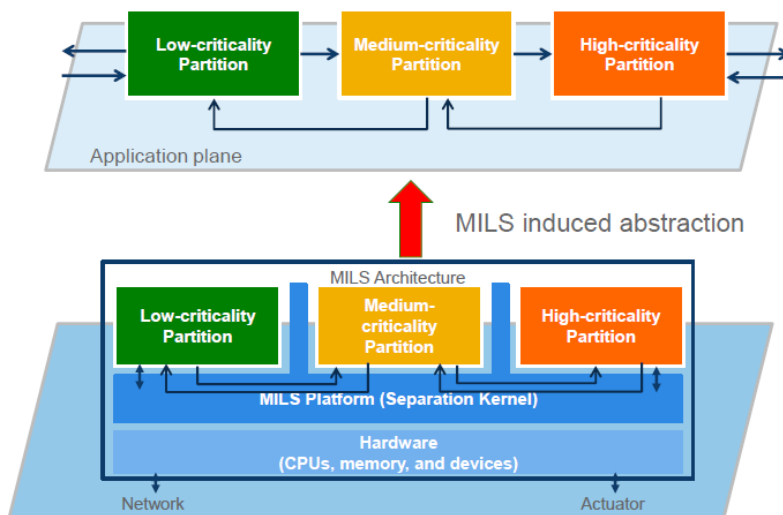


Figure 107: The MILS architectural approach (Tverdyshev, 2014)

⁴⁶ Cf. (EURO-MILS EC FP7 Project, 2012).

(Vogt, 2014) provides examples of real-life conflicts between safety and security requirements illustrated on a Smart Grid case. The presentation shows that the reality is far from simple, with possibly major negative consequences in case of revocation of security certificate.

(Woskowski, 2014) recalls that the problem of integration and interaction of medical devices has up to now been handled less seriously than in other safety-critical domains. The author discusses a pragmatic risk-based approach to handle these problems and the related standards, in particular (IEC 60601-1-SER, 2014), (ISO 14971, 2007) and (IEC 80001-1, 2010). The risk management required by (ISO 14971, 2007) is extended beyond device boundaries, covering interface safety, interface usage and network security aspects, and defining appropriate risk mitigation techniques.

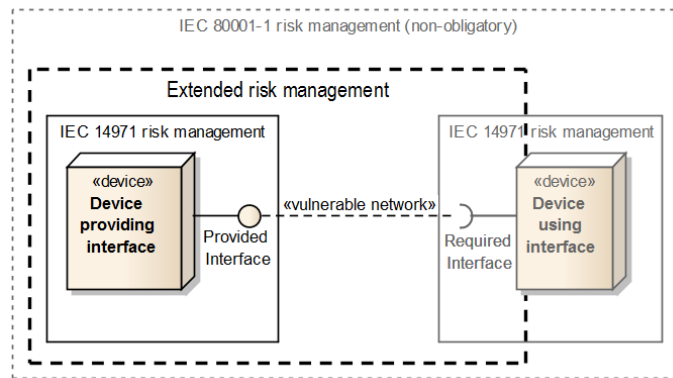


Figure 108: Proposed extended risk management (Woskowski, 2014)

(Young, et al., 2014) argues that by using a causality model based on systems theory, an integrated and more powerful approach to safety and security is possible. Indeed, hazards lead to safety incidents in the same way that vulnerabilities lead to security incidents. Use of a systems-theoretic approach to security, however, requires a reframing of the usual security problem. Just as the System-Theoretic Accident Model and Processes (STAMP) model reframes the safety problem as a control rather than a failure problem, applying STAMP to security involves reframing the security problem into one of strategy rather than tactics. In practice, this reframing involves shifting the majority of security analysis away from guarding against attacks (tactics) and more toward design of the broader socio-technical system (strategy). Because contemporary security and safety both attempt to prevent losses in complex software-controlled systems, the authors believe that applying the same system-theoretic causality model may benefit security the same way it is benefitting safety. Research is currently under way to test this notion. The key underlying idea is that from a strategy perspective, the physical (or proximate) cause of a disruption does not really matter. What matters is the efficacy of the strategy in dealing with (controlling) the effects of that disruption on overall system function or assuring the mission. This is a significant paradigm shift for security experts (as it was for safety experts). While likely to force a re-examination of many of the accepted truths of security, the authors believe such a refocus will help address three of the major problems with contemporary approaches to security—quantity, threat variety, and threat prioritization—can all be addressed more effectively through this new approach than through existing approaches. The new approach does not discard traditional security thinking, but does suggest it is tactically focused and must be augmented by an effective strategy in order to succeed.

(Blasum, 2015) recalls that while safety and security, at a high-level, are white-board concepts, once it comes to implementation in a MILS core (i.e. separation kernel + minimal set of additional hardware and software needed for the separation of partitions), sometimes the concrete realization depends on what is doable. In this paper, several use cases of partitioning are mapped to partitioning mechanisms implementing the partitioning (cf. Table 2). The main result is that different use cases of safety and security can be compared.

Safety/security use cases	Partitioning mechanisms implementing space separation	Partitioning mechanisms implementing time separation
Operating system protection	Access Control to Management data (ACM) + Access Control to User space memory (ACU)	CPU Reuse (CR)
Real-time safety	ACM + ACU + Quotas for Memory	CR + Worst Case Execution Time

	(QM)	(WCET)
Safety + confidentiality by MMU	ACM + ACU + QM	CR + WCET
Control of information flow between colluders	Access Control to Kernel resources (ACK) + ACU	Temporal normalization (TN)
Multi-core	Same as single-core	Same as single-core + Drift Avoidance (DA)

Table 2: Safety/security use cases and how they are implemented by partitioning mechanisms (Blasum, 2015)

(Brunel, et al., 2015) extends previous work by the same authors (Brunel, et al., 2014a), (Brunel, et al., 2014b), (Bieber, et al., 2014) on formal system modelling using Alloy and Failure Mode, Effects and Analysis (FMEA). The modelling environment has been package as a new framework called Coy. The approach is detailed at code level and richly illustrated on a fire alarm case study.

(Cimatti, et al., 2015) provides an overview of the approach to safety and security undertaken in the D-MILS project (D-MILS, 2007). The MILS architecture is well known to ensure properties that are relevant to both safety and security. The project develops a distributed version of the MILS architecture: the D-MILS concept extends the capacity of MILS to implement a single unified policy architecture to a network of separation kernels. To accomplish this, each separation kernel is combined with a new MILS foundational component, the MILS Networking System (MNS), producing the effect of a distributed separation kernel. Robustness and determinism of the network is ensured through the use of Time-Triggered Ethernet (TTE). The project offers a rich tool set. This paper focuses on the contract-based method extension, to prove that the composition of components that satisfy their contracts will meet the system requirements, provided that their integrity is protected (cf. Figure 109 in which contracts are represented by green scrolls). The approach is illustrated on a simple multi-level security case, whereby e.g. message authenticity and data confidentiality are shown to be preserved.

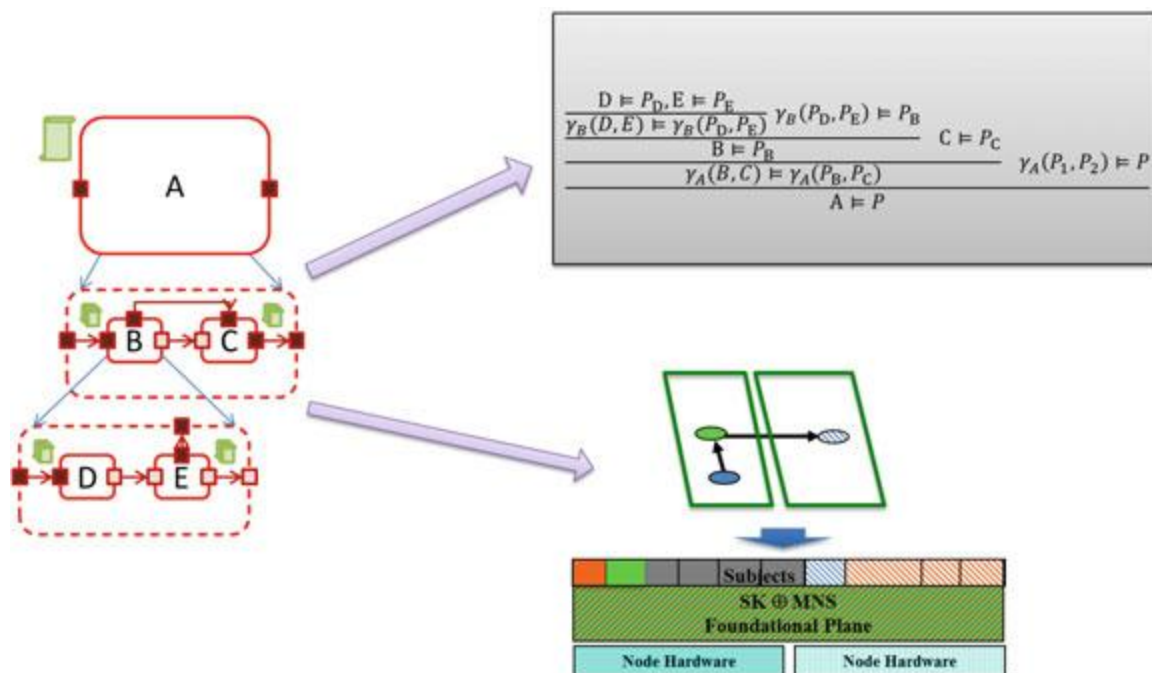


Figure 109: Formal reasoning and platform configuration based on the system architecture (Cimatti, et al., 2015)

(Chen, et al., 2015) presents a case of safety and security co-engineering in the urban railway domain. First, the authors use state-of-the-art Failure Mode, Vulnerabilities and Effect Analysis (FMVEA) and Attack Trees for respectively safety analyses and security analyses. Then, the limitations of the approaches are explained, and a new framework is proposed to address cross-domain events, i.e. cyber & physical events, and enhance the analysis of the consequences on the physical world (cf. Figure 110). The paper also addresses the question of standards (CENELEC EN 50129, 2010).

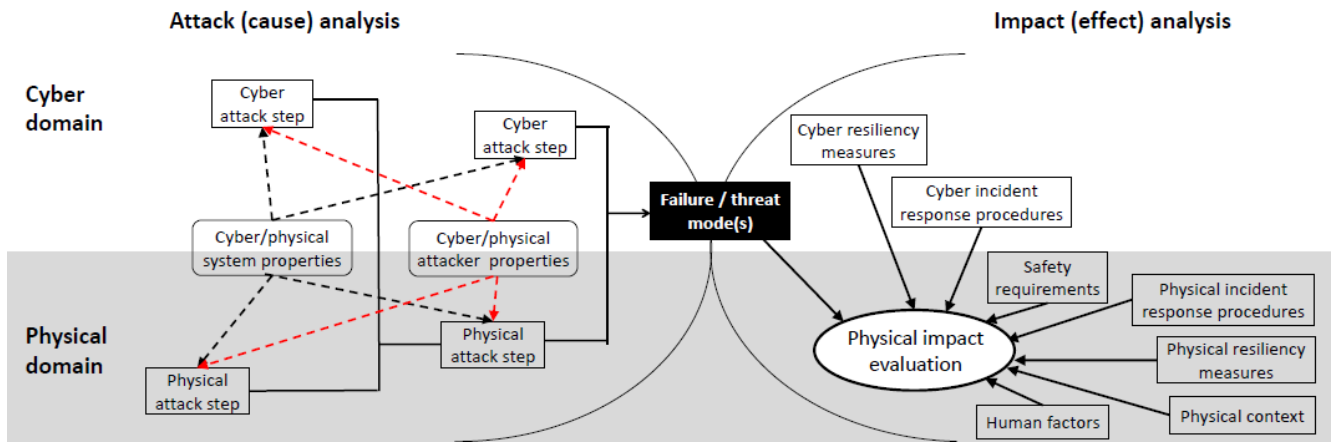


Figure 110: Analysing railway systems security with an integrative cyber-physical approach (Chen, et al., 2015)

Categorization criteria	Unification vs. integration		Lifecycle phase		Qualitative vs. quantitative	
	Unification	Integration	Development: requirements or design	Operational	Qualitative	Quantitative
Approaches						
Generic						
Stoneburner [44]	x			x	x	x
Aven [3]	x		x	x	x	x
Derock [38]	x		x	x	x	
Woskowski [45]	x		x		x	
Eames [24]		x		x	x	
Johnson [1]		x		x	x	
Kornecki [2]		x	x		x	
Novak [19,32,36]		x	x		x	
Hunter [30]		x	x	x	x	
Sørby [26]		x	x		x	
Ostby [48]		x	x		x	x
Bieber [5]		x	x		x	
Schmittner [49]		x	x	x	x	
Model-based						
Graphical methods						
GSN [6,30,52,53]		x	x	x	x	
NFR [54]		x	x	x	x	
Extended fault trees						
Fovino [56]		x		x	x	x
Bezzateev [58]		x	x		x	x
Kornecki [25]		x	x	x	x	x
Steiner [59]		x		x	x	x
BDMP [63]	x	x	x	x	x	x
BBN [77]		x		x	x	x
Misuse cases [80]		x	x	x	x	
CHASSIS [43]		x	x	x	x	
UMLsec/UMLsafe [86]		x	x		x	
SysML-Sec [88]		x	x	x	x	x
Stochastic Petri nets [67,68,70]	x	x	x	x	x	x
MBSE [90]		x	x	x	x	
Formal methods						
Zafar [91]		x	x		x	
GSE method						
Approaches for electrical networks [92,93,95]		x		x	x	x
Non-graphical methods						
Informal						
Reichenbach [33]		x		x	x	x
Holstein [97]		x		x	x	x
Depoy [98]	x			x	x	x
Pieters [99]		x	x	x	x	x
Formal						
Sun [37]		x	x	x	x	
Maude language						
Simpson [101]		x	x		x	
CSP/non-interference						
AADL [103]		x	x	x	x	
STPA-sec [107]		x	x	x	x	

Figure 111: Classification of the identified approaches (Kriaa, et al., 2015a)

(Kriaa, et al., 2015a) provides a comprehensive survey of existing approaches to industrial facility design and risk assessment that consider both safety and security (cf. Figure 111), with some 112 references. The set of

identified approaches is classified: (i) as generic versus model-based; (ii) as unification versus integration; (iii) by applicability in the development versus operational system lifecycle phase; and (iv) as qualitative versus quantitative. The authors argue that safety and security should no longer be treated separately and that dependencies should be identified and taken into consideration to ensure efficient risk management. To that end, a safety security integrated risk analysis process is proposed (cf. Figure 112).

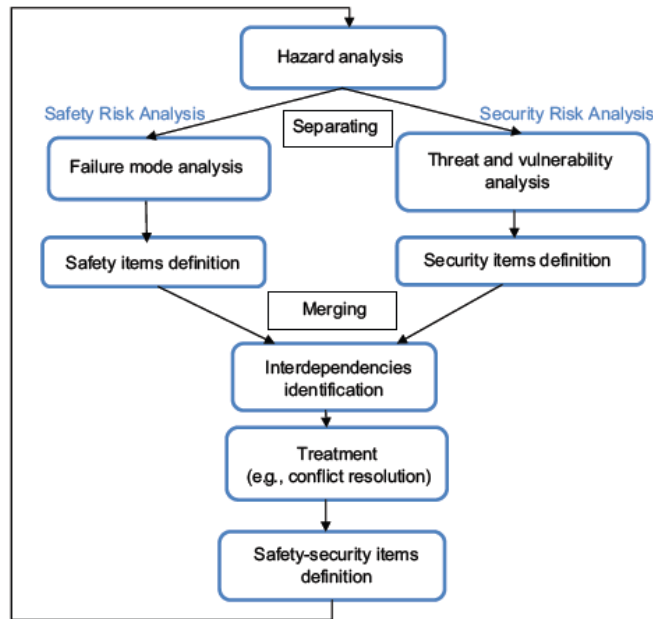


Figure 112: Safety security integrated risk analysis process (Kriaa, et al., 2015a)

(Kriaa, et al., 2015b) starts by recalling that modern control systems are becoming complex and interconnected as they are increasingly integrating new information and communication technologies. Many industries like automobile, aeronautics and energy are facing great challenges as their systems are becoming less isolated and vulnerable to external malevolence. Indeed, cyber-attacks targeting industrial infrastructures can engender heavy impacts on the safety of humans and environment. In this topical context, the authors propose a new model based approach: S-cube for SCADA Safety and Security joint modelling (cf. Figure 113). This approach provides a risk analysis framework that enables to evaluate industrial information and control architectures. Starting from the system description, S-cube generates automatically the different attack and failure scenarios it is exposed to. The S-cube approach relies on a knowledge base (the S-cube KB) that gathers expertise on ICS and particularly SCADA systems and the related safety and security risks. The S-cube KB is a Domain Specific Language that enables to describe the typical components of digital industrial infrastructures with safety and security aspects (authentication, access control, redundancy). Each component is associated with the attacks and failure modes likely to happen on it. The S-cube KB generic models are instantiated on the input system architecture and processed by calculation engines that generate automatically attack and failure scenarios. This approach is illustrated on a use case for which qualitative and quantitative results are given.

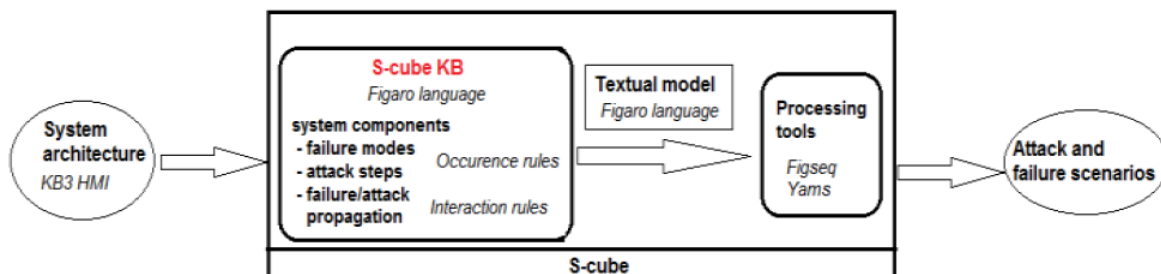


Figure 113: The S-cube approach (Kriaa, et al., 2015b)

(Macher, et al., 2015b), and its shorter counterpart (Macher, et al., 2015a), present a combined approach of the automotive HARA (hazard analysis and risk assessment) approach with the security domain Microsoft STRIDE approach, and outlines the impacts of security issues on safety concepts at system level. The method is called SAHARA, for Security-Aware Hazard Analysis and Risk Assessment. The focus of the method is placed on the

early development phase - the so-called concept phase - of safety-critical embedded automotive systems, which is also addressed by (ISO 26262-3, 2011). The first step of the SAHARA approach, combining security and safety analyses, is to quantify the STRIDE security threads of the system under development in an analogue manner as is performed for safety hazards as part of the Hazard Analysis and Risk Assessment (HARA) approach. Threats are quantified with reference to the Automotive Safety Integrity Level (ASIL) analysis, according to the resources (R) and know-how (K) that are required to pose the threat and the threats criticality (T), cf. Figure 114. The approach is applied on an automotive Battery Management System (BMS); for this specific example, the SAHARA approach allowed for the identification of 34% more hazardous situations than the traditional HARA approach.

Level	Required Know-How	Example
0	no prior knowledge (black-box approach)	average driver, unknown internals
1	technical knowledge (gray-box approach)	electrician, mechanic, basic understanding of internals
2	domain knowledge (white-box approach)	person with technical training and focused interests, internals disclosed

Level	Threat Criticality	Example
0	no security impact	no security relevant impact
1	moderate security relevance	annoying manipulation, partial reduced availability of service
2	high security relevance	damage of goods, invoice manipulation, non-availability of service, privacy intrusion
3	high security and possible safety relevance	maximum security impact and life-threatening abuse possible

Level	Required Resource	Example
0	no additional tool or everyday commodity	randomly using the user interface, strip fuse, key, coin,
1	standard tool	screwdriver, multi-meter, multi-tool
2	simple tool	corrugated-head screwdriver, CAN sniffer, oscilloscope
3	advanced tools	debugger, flashing tools, bus communication simulators

		Threat Level 'T'			
Required Resources 'R'	Required Know-How 'K'	Threat Level 'T'			
		0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

Figure 114: Required resource, required know-how and threat criticality classifications (left), and SecL Determination Matrix (right) (Macher, et al., 2015a)

(Netkachova, et al., 2015) recalls that safety cases are the development foundation for safety-critical systems and are often quite complex to understand depending on the size of the system and operational conditions. This paper describes an approach to analysing safety and security in a structured way and creating security-informed safety cases. It includes an overview of the structured assurance case concept, a security-informed safety methodology and a layered approach to constructing cases. The following main layers of assurance are proposed: L0 Policy and requirements – the highest level of abstraction where the system represents its requirements, and defines safety and security policies and their interaction (cf. Figure 115); L1 Architectural layer – the intermediate level where the abstract system components and architecture are analysed; L2 Implementation layer – the detailed level where the implementation of specific components and their integration within the specific system architecture are scrutinised. These layers of assurance fit well the layered system design approach of aerospace described in (SAE ARP 4754A, 2010) combined with the compositional approach of MILS and Integrated Modular Avionics (IMA). The approach is applied to a Security Gateway that is used to control data flow between security domains in a separation kernel based operating system (i.e. PikeOS) in avionics environment. The authors show that a clear and structured way of presenting a safety case combining safety and security alleviates understanding important interactions and, hence, increases safety.

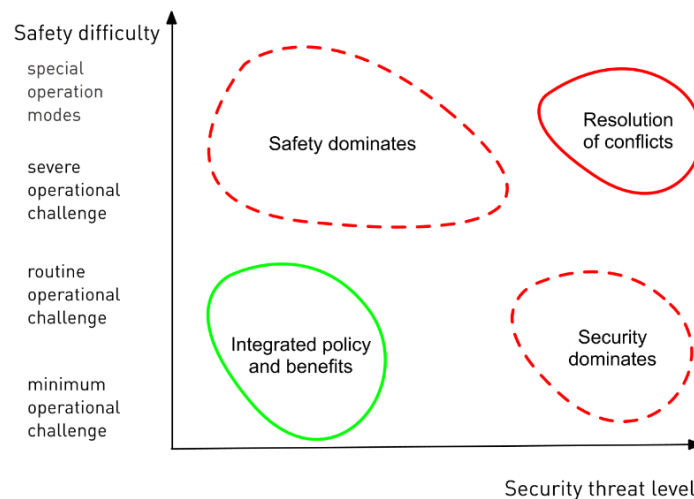


Figure 115: Defining an integrated policy (Netkachova, et al., 2015)

(Paul, et al., 2015) provides a bibliography of research papers on safety and cyber-security co-engineering since the early 90's. It only covers papers that address both safety and security architecting and / or engineering specialties explicitly and simultaneously. It is an extract of the state of the art synthesis given in part B, §5 of this deliverable.

(Paul, 2015) recalls that 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 cyber-security 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 cyber-security 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, the author analyses this would-be seamless integration of security engineering activities into the safety engineering world, and discusses the areas in which a lot of fuzziness still remains.

(Schmittner, et al., 2015a) presents the application of two methods, namely the Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) and Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) methods, to a case study of safety and security co-analysis of cyber-physical systems in the automotive domain. The authors show that one weakness of CHASSIS is that, while safety and security are analysed with the same methodology, the two assessments are done separately; ; there is a need for exchange and discussion between both the safety and the security domains in all phases of system engineering lifecycle; from an engineering point of view, commonalities and conflicts from both domains need to be identified in the beginning, documented and resolved; a unified risk rating for threats and failures which influences security would be a necessary improvement for both methods. Moreover both methods do not explicitly address how to conduct safety and security analysis in a continuous manner; this becomes an issue when a new vulnerability or attack vector is identified, which will change the risk assumptions and the risk postures based on the previous analyses and assumptions. Directions are given for further improvements of the methods.

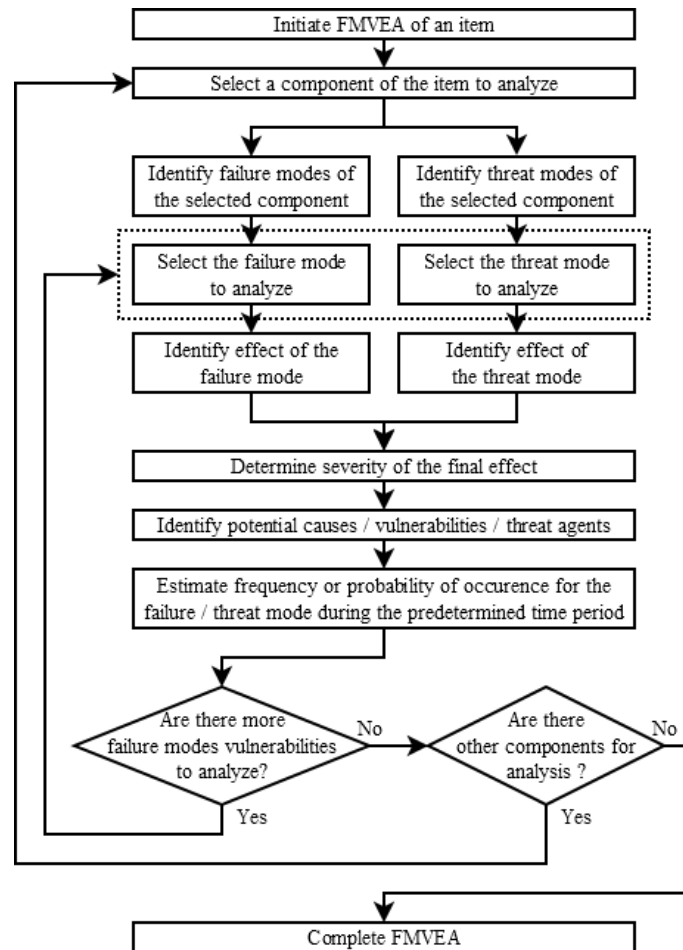


Figure 116: Overview of FMVEA method (Schmittner, et al., 2015a)

(Schmittner, et al., 2015b) investigates how to extend existing safety standards to address security concerns in the automotive domain. To complement the (ISO 26262-1, 2011)- (ISO 26262-10, 2012) safety standard and to promote a combined approach to safety and security, the authors identified three requirements for the evaluation of candidate security standards: (i) there should be an overlap in required work products for safety and security argumentation; (ii) assurance levels between safety and security should be translatable; (iii) approaches and concepts from the safety standard should be mirrored by the security standard. Based on these requirements, they investigate the feasibility of using the Common Criteria (ISO/IEC 15408-1, 2009)- (ISO/IEC 15408-3, 2008) to complement the safety standard. They provide a comparison of work products from the two standards, propose a translation between Evaluation Assurance Levels (EALs) and Automotive Safety Integrity Levels (ASILs), based on their strictness and degree of formalism (cf. Figure 117), and redefine exposure as the probability that a driving scenario takes place in which a cyber-attack is possible.

ASIL		EAL
ASIL A	~	EAL3
ASIL B	~	EAL4
ASIL C	~	EAL5
ASIL D	~	EAL6

Figure 117: Comparison of integrity and assurance levels (Schmittner, et al., 2015b)

(Taguchi, et al., 2015) presents several case patterns, called Safe & Sec case patterns, derived from process patterns, which integrate safety and security activities at the early stage of the system life-cycle. The Independent Case Pattern treats safety and security independently. The Subordinate Case Pattern (cf. Figure 118) reflects the safety point of view, i.e. security as a part of safety. The Uni-Directional Reference Case Pattern relates to the (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014) standard, in which some outcomes in the safety assessment process flows to security risk assessment but not vice versa. The other two proposed patterns are the Interrelated (Independent) Case Pattern and the Interrelated (SafSec) Case Pattern.

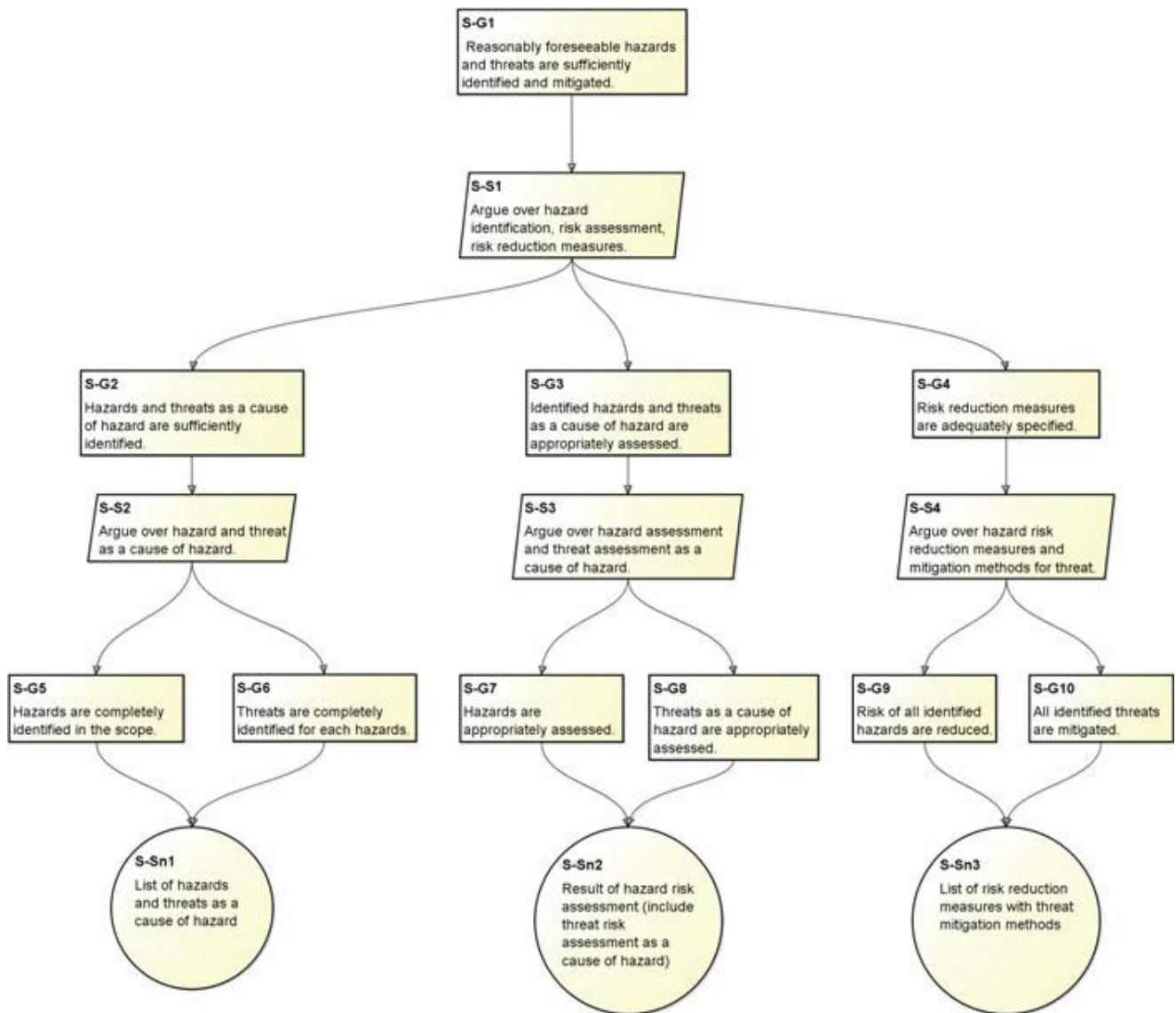


Figure 118: Subordinate case pattern (Taguchi, et al., 2015)

(Braband, 2016) recalls that some recent incidents and analyses have indicated that possibly the vulnerability of IT systems in railway automation has been underestimated so far. Due to several trends, such as the use of commercial IT and communication systems or privatization, the threat potential has increased. This paper discusses the relation between Security Levels (SLs) from the ISA 99 / IEC 62443 standard series (cf. §3.2.3.4) and Safety Integrity Levels (SILs) from (CENELEC EN 50129, 2003) for safety systems. The four major new results are: (i) SL and SIL are completely different concepts, e. g. SL is a seven dimensional vector in contrast to the scalar SIL; (ii) There is no simple relationship between SL and SIL; (iii) SL 0 for safety-related systems is not acceptable; for safety systems, it is recommended to always take the requirements of SL 1 into account; (iv) A preliminary proposal for SL profiles has been made in order to master the complexity of potentially 16384 SL vectors. Table 3 gives a summary of which requirements for SL 1 are already covered or not relevant from a safety perspective. The annex gives a more detailed discussion including a comparison with SL2 requirements. The results should also hold for other related safety standards such as the IEC 61508 series, i.e. (IEC 61508-1, 1998)- (IEC 61508-7, 2000).

Reference	Title	Assessment
SR 1.6	Management of wireless access processes	This requirement is not relevant for SL1.
SR 1.13	Access through untrustworthy networks	This requirement is not relevant for SL1.
SR 2.2	Use control in the case of radio connections	This requirement is not relevant for SL1.
SR 3.1	Communication integrity	This requirement is fulfilled by application of EN 50159.
SR 3.3	Verification of IT security functionality	This requirement is fulfilled by application of EN 50128.
SR 3.4	Software and information integrity	This requirement is fulfilled by application of EN 50128.
SR 3.5	Input validation	This requirement is fulfilled by application of EN 50129 and EN 50128.
SR 3.6	Deterministic output	This requirement is fulfilled by application of EN 50129 and EN 50128.
SR 4.1	Confidentiality of information	This requirement is not relevant for railway applications with SL1.
SR 4.3	Use encryption	This requirement is not relevant for railway applications with SL1.
SR 5.1	Network segmentation	This requirement is fulfilled by application of EN 50159.
SR 5.2	Protection of the zone boundary	This requirement is not relevant for SL1.
SR 5.3	Restriction of general communication between persons	Generally, voice communication is not part of the safety system. However, this requirement shall be exported to the operator.
SR 7.1	Protection against DoS attacks	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported to the operator.
SR 7.2	Resource management	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported to the operator.
SR 7.3	Backups of the automation system	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported.
SR 7.4	Restart and recovery of the automation system	This requirement is fulfilled by application of EN 50129.
SR 7.5	Emergency power supply	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported to the operator.
SR 7.6	Network and security settings	This requirement is fulfilled by application of EN 50128 and EN 50129.

Table 3: IT security requirements that are already covered or are irrelevant (Braband, 2016)

3 Overview of safety and security standards

This section provides an overview of safety and security standards, which revises⁴⁷, summarizes⁴⁸ and complements⁴⁹ the state of the art already provided in chapter §3 of D3.4.1 (Faucogney, et al., 2014).

According to the International Council on System Engineering (INCOSE, 2004), a standard is a document that establishes engineering and technical requirements (for products, processes, procedures, practices, and methods) that have been decreed by authority or adopted by consensus. Standards can be of two categories: *de jure*, or *de facto*. A *de jure* standard is an official standard with legal status; it is usually produced by a national or international organization which has no specific (biased to any one company) commercial interests. A *de facto* standard is a standard (formal or informal) that has achieved a dominant position, by tradition, enforcement, or market dominance.

Most of this state of the art relates to *de facto* standards because many domains are not subject to regulation. However, some parts of this safety and security overview are structured according to *Regulatory* documents versus their *Acceptable Means of Compliance* (AMC) and *Guidance Material* (GM). A regulation is a document providing binding legislative rules, which is adopted by an authority. Regulations are difficult to comply with “as is”, so AMC/GM are usually provided.

⁴⁷ The most recent editions of the standards have been added, and some errors have been corrected.

⁴⁸ Fewer details are given for each standard.

⁴⁹ The number of addressed standards is increased.



Figure 119: Significant safety standards per application domains

This overview starts with safety standards (cf. §3.1) and proceeds with security standards (cf. §3.2). Standards that are relevant for both safety and security are described separately (cf. §3.3). With respect to our focus on safety and security co-engineering, our overview of safety standards is more extensive than the overview of security standards because the safety community is questioning itself with respect to security concerns, whilst the security community seems globally unconcerned by safety issues. This section closes on an analysis of the safety and security standards from the point of their evolution towards co-engineering safety and security (cf. §3.4).

3.1 Overview of safety standards

This section is organised per application domain, with a first section about transverse standards. The description of each standard is deliberately kept short⁵⁰, but full references are given for the reader to access more details.

3.1.1 Transverse safety standards

The functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems (S + IEC 61508, 2010) is a single-file 1000 pages compilation of the 7-part official IEC standard: parts 1 to 3 contain the requirements of the standard (normative), whilst parts 4 to 7 are guidelines and examples. It sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of product and application sector international standards based on the IEC 61508 series.

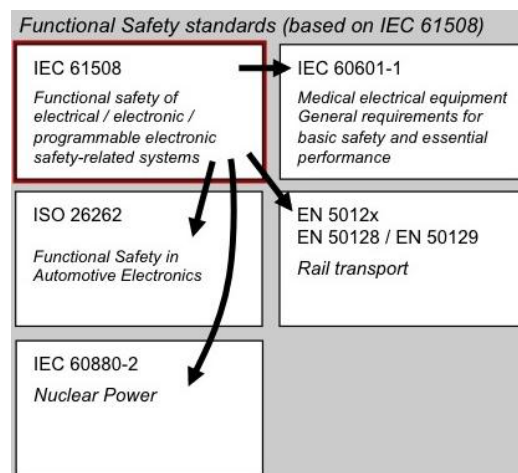


Figure 120: Functional safety standards based on the IEC 61508 series

This international standard:

- adopts a risk-based approach by which the safety integrity level requirements can be determined;
- introduces Safety Integrity Levels (SILs) for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;
- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in:
 - a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5} per hour;
 - a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} per hour;
- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry; even though the probability of occurrence of sys-

⁵⁰ A complementary review of safety standards is available in (CESAR D_SP1_R5.2_M1, 2009). For interested readers, (Lee, et al., 2014) provides a history of the families of DO-178 (commercial avionics), MIL-STD-882 (US Department of Defence), and DEF STAN 00-56 (UK Ministry of Defence) standards.

tematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;

- introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail-safe; however, the concepts of fail-safe and inherently safe principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

(TÜV Rheinland, 2015) is the internationally recognized certification authority for the IEC 61508 and related safety standards. (exida, 2015) is another firm that performs IEC 61508 and related certifications.

(MIL-STD-882E, 2012) is the US Department of Defence standard practice for system safety. It is a key element of systems engineering, for both the programme manager and contractor, which provides a standard generic method for the identification and classification of hazards, and the mitigation of associated risks encountered in the development, test, production, use, and disposal of defence systems. It is in existence since 1969.

The Safety Management Requirements for Defence Systems (DEF STAN 00-56, 2014) captures the requirements and guidance of the United Kingdom Ministry of Defence regarding the procurement, analysis, development and operation of safety-critical systems. This standard is also widely credited as popularising the use of the safety case as a means of showing that a level of acceptable safety has been reached.

3.1.2 Automotive safety standards

3.1.2.1 Regulation

The World Forum for Harmonization of Vehicle Regulations is a working party (WP.29) of the Inland Transport Division of the United Nations Economic Commission for Europe (UNECE). It is tasked with creating a uniform system of regulations, called UN Regulations, for vehicle design to facilitate international trade. The forum works on regulations covering vehicle safety, environmental protection, energy efficiency and theft-resistance. The work is recognized to varying degree by most countries except the United States.

The Federal Motor Vehicle Safety Standards (FMVSS) are U.S. federal regulations specifying design, construction, performance, and durability requirements for motor vehicles and regulated safety-related components, systems, and design features. They are the U.S. counterpart to the UN Regulations developed by the World Forum for Harmonization of Vehicle Regulations.

3.1.2.2 Acceptable means of compliance

Road vehicles -- Functional safety

The 10 parts Road vehicles -- Functional safety standard (ISO 26262-1, 2011) - (ISO 26262-10, 2012) is the adaptation of (S + IEC 61508, 2010) to comply with the automotive specific application related to Electric / Electronic systems.

This international standard:

- provides an automotive safety lifecycle including management, development, production, operation, service, and decommissioning, and supports tailoring the necessary activities during these lifecycle phases;
- provides an automotive specific risk-based approach for determining risk classes: the Automotive Safety Integrity Levels (ASILs);
- uses ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk;
- provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved.

Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems

The 4 parts Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems (ISO 25119-1, 2010), (ISO 25119-2, 2010), (ISO 25119-3, 2010), (ISO 25119-4, 2010) is applicable to safety related parts of control systems used in tractors for agriculture and forestry, self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture and municipal equipment (e.g. street sweeping machine).

Earth-moving machinery -- Machine-control systems using electronic components -- Performance criteria and tests for functional safety

The Earth-moving machinery -- Machine-Control Systems (MCS) using electronic components -- Performance criteria and tests for functional safety (ISO 15998, 2008) specifies performance criteria and tests for functional safety of safety-related MCS using electronic components in earth-moving machinery and its equipment.

This standard does not present a safety process or list of methods, it refers directly to the withdrawn (IEC 61508-1, 1998) - (IEC 61508-7, 2000) standard series for it, but it provides specific requirements for the specification of MCS regarding physical environment (temperature, humidity...) and operating conditions (electromagnetic, mech. vibration...). It also recommends specific tests (to meet the previous requirements): test of basic functions, entering in safe state test, functional test at operating temperature and humidity, Electromagnetic Compatibility test, and shock and vibration tests.

Electrically propelled road vehicles -- Safety specifications

The Electrically propelled road vehicles -- Safety specifications -- Part 1 (ISO 6469-1, 2009) specifies requirements for the on-board rechargeable energy storage systems (RESS) of electrically propelled road vehicles, including battery-electric vehicles (BEVs), fuel-cell vehicles (FCVs) and hybrid electric vehicles (HEVs), for the protection of persons inside and outside the vehicle and the vehicle environment. Flywheels are not included in the scope. The standard applies only to RESS in on-board voltage class B electric circuits for vehicle propulsion.

Part 2 (ISO 6469-2, 2009) specifies requirements for operational safety means and protection against failures related to hazards specific to electrically propelled road vehicles, including BEVs, FCVs and HEVs, for the protection of persons inside and outside the vehicle and the vehicle environment. Requirements related to internal combustion engine systems of HEVs are not covered. The standard applies only if the maximum working voltage of the on-board electrical propulsion system is lower than the upper voltage class B limit.

Part 3 (ISO 6469-3, 2011) specifies requirements for the electric propulsion systems and conductively connected auxiliary electric systems, if any, of electrically propelled road vehicles for the protection of persons inside and outside the vehicle against electric shock. It applies only to on-board electric circuits with maximum working voltages according to voltage class B.

The three parts neither apply to motorcycles and vehicles not primarily intended as road vehicles, such as material handling trucks or forklifts, not provide comprehensive safety information for manufacturing, maintenance and repair personnel.

Fuel cell road vehicles -- Safety specifications

The Fuel cell road vehicles -- Safety specifications -- Protection against hydrogen hazards for vehicles fuelled with compressed hydrogen standard (ISO 23273, 2013) specifies the essential requirements for fuel cell vehicles (FCV) with respect to the protection of persons and the environment inside and outside the vehicle against hydrogen-related hazards. It applies only to such FCV where compressed hydrogen is used as fuel for the fuel cell system. It does not apply to manufacturing, maintenance and repair. The requirements address both normal operating (fault-free) and single-fault conditions of the vehicles.

3.1.3 Aviation safety standards

This section first provides a quick overview of the main regulations. Then, the acceptable means of compliance and guidance material are briefly described.

Following a real need for international standards for air transport, the 1944 Chicago Conference developed the Convention on International Civil Aviation, which led to the foundation of the International Civil Aviation Organisation (ICAO), in April 1947. The objectives of the convention are: (i) a safe and orderly development of international civil aviation; (ii) international Air transport services established on the basis of equality of opportunity and operated soundly and economically. Originally signed by 52 States, the principles and arrangements laid down in the Convention and its annexes are now ratified by 191 States.

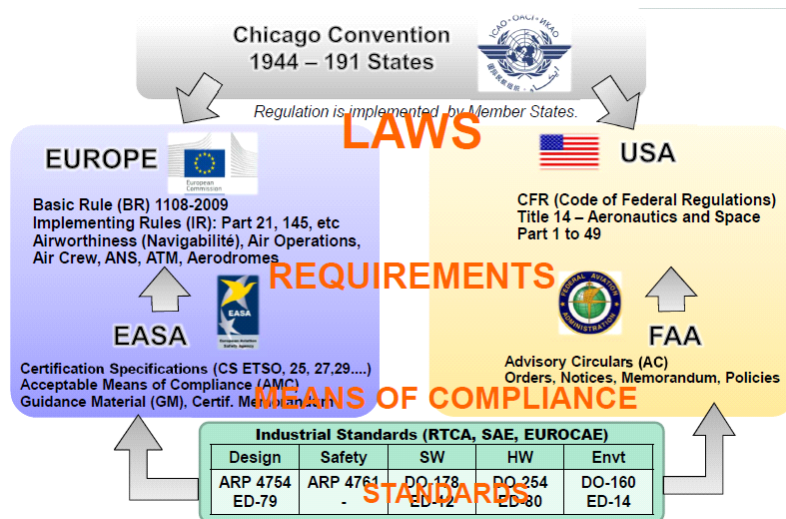


Figure 121: EU and US Regulation Structures, an avionics point of view (Chevrel, 2014)

ICAO regulation is implemented by its member States. The two main airworthiness authorities are (cf. Figure 121):

- the European Aviation Safety Agency (EASA);
- the US Federal Aviation Authority (FAA).

But there are many more national authorities that publish national regulations, e.g. the UK's Civil Aviation Authority (CAA) and the Canadian Aviation Authority.

The list of specific EASA and non-EASA aircraft types is contained in CAP 747 - "Mandatory Requirements for Airworthiness". CAP 747 also provides a statement of the general categories of aircraft that are excluded from European Regulations and so remain subject to National rules.

3.1.3.1 European Aviation Safety Agency (EASA) Regulations

On September 27th, 2002, entered into force Regulation (EC) N° 1592/2002 "Basic Regulation" of 15 July 2002 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency (EASA) with regulatory and executive tasks in the field of civilian aviation safety. EASA reached full functionality in 2008, taking over functions of the Joint Aviation Authorities (JAA). The Basic Regulation of 2002 was repealed by Regulation (EC) No 216/2008, which was itself amended by (Regulation (EC) No 1108, 2009).

As part of its regulatory framework, the Agency issues Certification Specifications (CS), including Airworthiness Codes and Acceptable Means of Compliance (AMC), as well as Guidance Material (GM) for the application of the Basic Regulation and its implementing rules. CSs are used to demonstrate compliance with the Basic Regulation and its implementing rules; these include, in particular: (i) airworthiness codes, which are standard technical interpretations of the airworthiness essential requirements contained in Annex I to the Basic Regulation; and (ii) acceptable means of compliance, which are non-exclusive means of demonstrating compliance with airworthiness codes or implementing rules. AMCs illustrate a means, but not the only means, by which a specification contained in an airworthiness code or a requirement of an implementing rule can be met; satisfactory demonstration of compliance using a published AMC shall provide for presumption of compliance with the related specification or requirement; it is a way to facilitate certification tasks for the applicant and the competent authority. GM is issued by the Agency to assist in the understanding of the Basic Regulation, its implementing rules and CSs.

The responsibilities of EASA include conducting analysis and research of safety, authorising foreign operators, giving advice for the drafting of EU legislation, implementing and monitoring safety rules (including inspections in the member states), giving Type Certification of aircraft and components as well as the approval of organisations involved in the design, manufacture and maintenance of aeronautical products.

An overview of the regulations produced by EASA is given in Figure 122. Full details are available online (EASA, 2014). When available the corresponding AMC & GM are offered on this same view.

It is impossible to cover all the regulations with their amendments and list of AMC & GM. For example, the sole list of Mandatory Continuing Airworthiness Information contains, at the date of writing this report, 9885 publications, applicable to all types of aircraft, the oldest applicable publication dating back to November 1957.

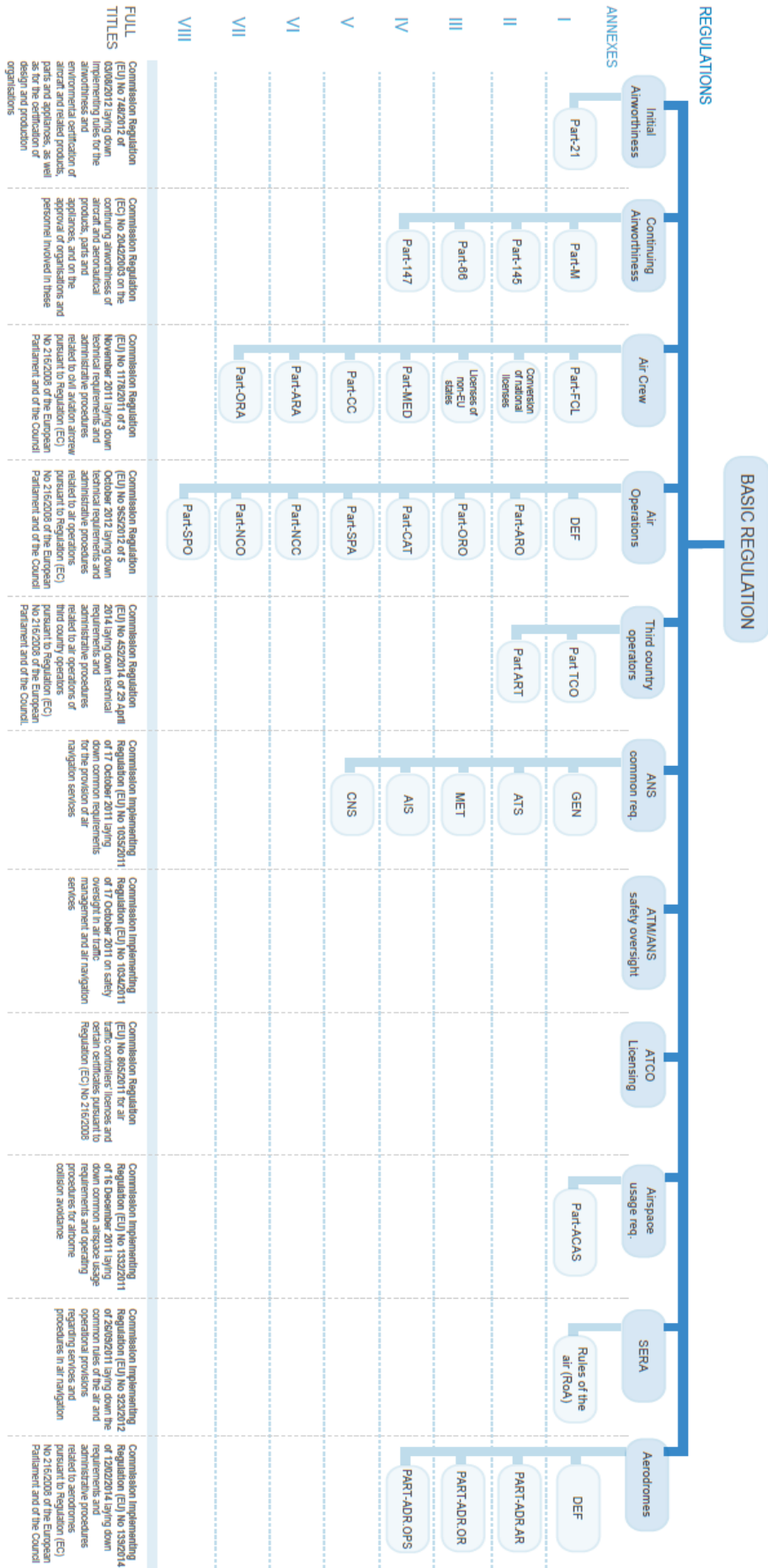


Figure 122: EASA regulation structure (EASA, 2014)

Of particular interest for this state of the art, from the avionics point of view, are the Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (EASA CS-25, 2014). Within this extensive document (921 pages), parts CS 25.1309 *Equipment, systems and installations*, and AMC 25.1309 *System Design and Analysis*, broadly require that there must be an inverse relationship between the probability of a failure and its consequences (cf. Figure 70 on page 58). It is in this document that the 4-categories severity scale (i.e. minor, major, hazardous, catastrophic) was defined. CS 25.1309 recognises (EUROCAE ED-14G, 2011) / (RTCA DO-160G, 2010), (SAE ARP 4754A, 2010) / (EUROCAE ED-79A, 2010), and (SAE ARP 4754A, 2010) as acceptable means of compliance.

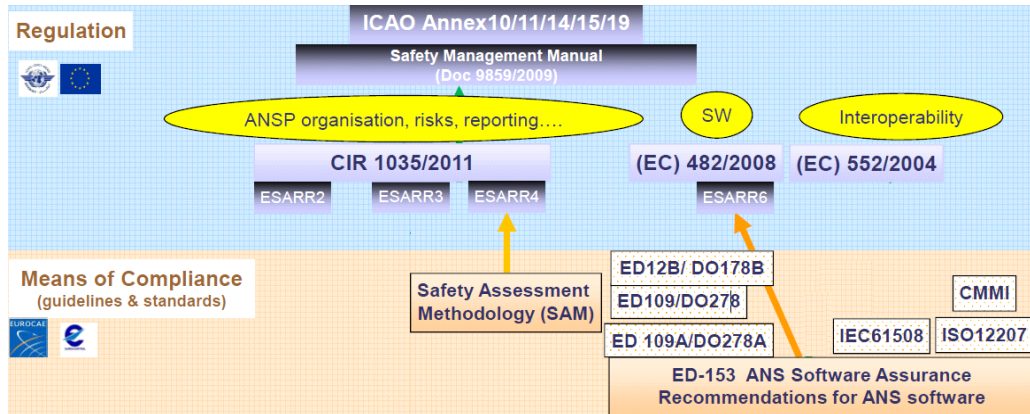


Figure 123: EU Regulation Structures, an Air Traffic Control point of view (Pauly, 2014)

From a ground-based Air Traffic Control perspective, the view over the same regulation framework is slight different, as pictured in Figure 123. The acceptable means of compliance of on-board avionics systems and ground-based CNS/ATM systems are detailed below, after a brief overview of the US Federal Aviation Regulations.

3.1.3.2 US Federal Aviation Regulations (FARs)

The Federal Aviation Regulations (FARs) are rules prescribed by the Federal Aviation Administration (FAA) governing all aviation activities in the United States. The FARs are part of *Title 14 - Aeronautics and Space* of the Code of Federal Regulations (CFR). They are structured in 6 chapters and 1399 parts (cf. Figure 124) and are available online (14 CFR, 2014). A wide variety of activities are regulated, such as aircraft design and maintenance, typical airline flights, pilot training activities, hot-air ballooning, lighter-than-air aircraft, man-made structure heights, obstruction lighting and marking, and even model rocket launches, model aircraft operation, and kite flying. The rules are designed to promote safe aviation, protecting pilots, flight attendants, passengers and the general public from unnecessary risk.

Title	Volume	Chapter	Browse Parts	Regulatory Entity
Title 14 Aeronautics and Space	1	I	1-59	FEDERAL AVIATION ADMINISTRATION, DEPARTMENT OF TRANSPORTATION
	2		60-109	
	3		110-199	
	4	II	200-399	OFFICE OF THE SECRETARY, DEPARTMENT OF TRANSPORTATION (AVIATION PROCEEDINGS)
			400-1199	COMMERCIAL SPACE TRANSPORTATION, FEDERAL AVIATION ADMINISTRATION, DEPARTMENT OF TRANSPORTATION
	5	V	1200-1299	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
	1300-1399		AIR TRANSPORTATION SYSTEM STABILIZATION	

Figure 124: US Federal Aviation Regulations (FARs)

Note: since 1958, the Federal Aviation Regulations have typically been referred to as "FARs". However, another set of regulations (Title 48) is titled "Federal Acquisitions Regulations", and this has led to confusion with the use of the acronym "FAR". Therefore, the FAA has begun to refer to specific regulations by the term "14 CFR part XX".

Of particular interest for this state of the art is 14 CFR Part 25—Airworthiness Standards: Transport Category Airplanes.

Via Advisory Circular AC20-174, the FAA recognises (SAE ARP 4754A, 2010) the Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A, Guidelines for Development of Civil Aircraft and

Systems, dated December 21, 2010, as an acceptable method for establishing a development assurance process.

Via Advisory Circular AC20-115C, the FAA recognises (RTCA DO-178C, 2011), (RTCA DO-330, 2011), (RTCA DO-331, 2011), (RTCA DO-332, 2011) and (RTCA DO-333, 2011) as acceptable means⁵¹ for showing compliance with the applicable airworthiness regulations for the software aspects of airborne systems and equipment certification.

Via Advisory Circular AC20-152, the FAA recognises (RTCA DO-254, 2000) as acceptable means for showing compliance with hardware design assurance levels A, B, and C for manufacturers and installers of products or appliances incorporating complex custom micro-coded components.

3.1.3.3 Means of compliance for on-board avionics systems

(RTCA DO-178C, 2011) and (RTCA DO-254, 2000), with their European counterparts (EUROCAE ED-12C, 2012) and (EUROCAE ED-80, 2000), are the two main *de facto* standards for developing avionics as part of a commercial civil airplane type certificate. Besides being respectively for software and hardware, both documents are very similar.

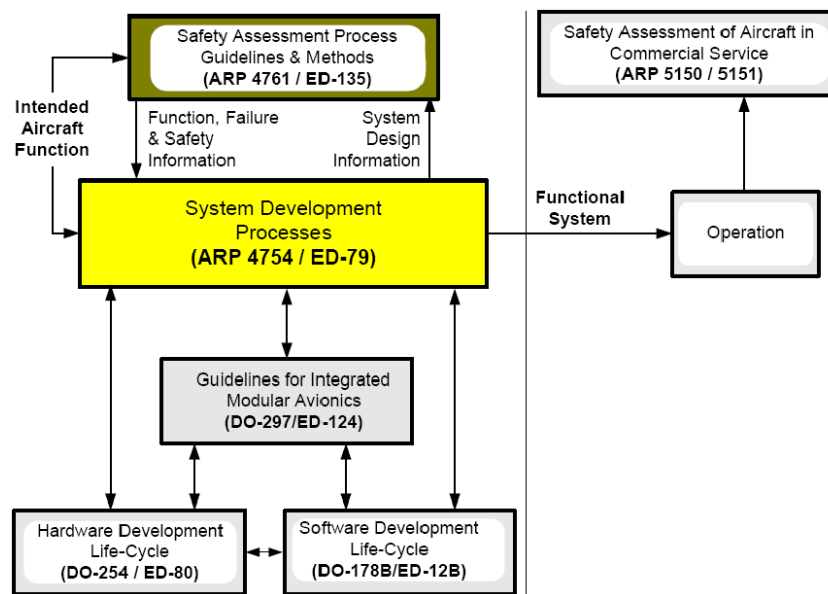


Figure 125: Relation between standards in the avionics domain (SAE ARP 4754A, 2010)

(RTCA DO-178C, 2011) / (EUROCAE ED-12C, 2012) provide recommendations for the production of software for airborne systems and equipment that performs its intended function with a level of confidence in safety that complies with airworthiness requirements. They are process-based software development assurance standards that define five software criticality levels, a.k.a. Development Assurance Levels (DALs), from E to A upwards. Through a DAL dependent set of activities, quality objectives and development work products, the standards strive to ensure that all the system requirements allocated to a given piece of software are implemented in the executable code loaded in a defined equipment, and nothing else, i.e. no dead code, no unintended function.

(RTCA DO-254, 2000) / (EUROCAE ED-80, 2000) provide guidance to be used by aircraft manufacturers and suppliers of electronic hardware items used in aircraft systems. These documents are similar to their software counterparts (see above). The assurance level is also defined as A, B, C, D or E.

(SAE ARP 4754A, 2010) / (EUROCAE ED-79A, 2010) have for main goal ensuring that the aircraft functions are correct and complete. They provide additional certification considerations for highly integrated or complex aircraft systems. They address the total life cycle for systems that implement aircraft level functions. They exclude specific coverage of detailed systems, software and hardware design processes beyond those of significance in establishing the safety of the implemented system. The process includes validating requirements and verifying that requirements are met, together with the necessary configuration management and process assurance activities. As development assurance level assignments are dependent on classification of failure conditions, the safety analysis process is used in conjunction with the development assurance process to identify failure conditions and severity classifications which are used to derive the level of rigor required for development. The level of validation and verification rigor is determined by the function development assurance level(s) for the aircraft or system (FDAL) and item development assurance level(s) for the item (IDAL).

⁵¹ But not as the only means.

(SAE ARP 4761A, 2004) provides guidelines to perform the safety assessment for certification of civil aircraft, consisting of a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA), and a System Safety Assessment (SSA). It also presents information on the safety analysis methods needed to conduct the safety assessment.

(EUROCAE ED-14G, 2011) / (RTCA DO-160G, 2010) provide standard procedures and environmental test criteria for testing airborne equipment for the entire spectrum of aircraft.

3.1.3.4 Means of compliance for ground-based CNS/ATM systems

For the development of ground-based Communication, Navigation, Surveillance (CNS) and Air Traffic Management (ATM) systems, there are two key standards: (EUROCAE ED-109A, 2012) / (RTCA DO-278A, 2011) and (EUROCAE ED-153, 2009).

(EUROCAE ED-109A, 2012) / (RTCA DO-278A, 2011) are the ground-based complements to the (EUROCAE ED-12C, 2012) / (RTCA DO-178C, 2011) airborne standards (cf. Figure 126). The standards define a set of objectives recommended to establish assurance that the developed non-airborne CNS/ATM software has the integrity needed for use in a safety-related application. The guidelines are in the form of: (i) objectives of software life cycle processes; (ii) description of activities and design considerations for achieving these objectives; (iii) description of the evidence that indicate that the objectives have been satisfied. The documents discuss those aspects of certification that pertain to the production of software for ground based avionics systems and used in CNS or ATM equipment.

DO-278 / ED109 Assurance Levels	Corresponding DO-178B / ED-12 Safety Levels	
AL1	Level A:	Catastrophic: prevents continued safe flight or landing, many fatal injuries
AL2	Level B:	Hazardous/Severe: potential fatal injuries to a small number of occupants
AL3	Level C:	Major: impairs crew efficiency, discomfort or possible injuries to occupants
AL4	<i>No equivalent</i>	
AL5	Level D:	Minor: reduced aircraft safety margins, but well within crew capabilities
AL6	Level E:	No Effect: does not effect the safety of the aircraft at all

Figure 126: Mapping of levels between ground and airborne software safety standards

(EUROCAE ED-153, 2009) applies to software that forms part of an Air Navigation Service (ANS) system. The scope of this standard extends to the overall lifecycle of software within an ANS system; however this document considers aircraft software out of scope and is therefore limited to the “ground” segment of ANS. This document assumes that a risk assessment and mitigation process has been undertaken along with an a priori system (where system includes people, procedure and equipment) safety assessment (e.g. a SAM-FHA and SAM-PSSA) with the results forming an input to this document. This document covers: (i) guidance for an ANSP to establish a software safety assurance system; (ii) guidance for software suppliers on the necessary software safety assurance regarding products and processes; (iii) a reference against which stakeholders can assess their own practices for software safety assurance of: specification, design, development, operation, maintenance, and decommissioning; (iv) a software assurance process that will promote interoperability through its common application to ANS software development.

3.1.3.5 Other means of compliance for both on-board avionics systems and ground-based CNS/ATM systems

(RTCA DO-330, 2011) / (EUROCAE ED-215, 2012) provide software tool qualification guidance for airborne and ground-based software. They explain the process and objectives for qualifying tools. They may also be used by other domains, such as automotive, space, systems, electronic hardware, aeronautical databases and safety assessment processes.

(RTCA DO-331, 2011) / (EUROCAE ED-218, 2012) contain modifications and additions to (RTCA DO-178C, 2011) / (EUROCAE ED-12C, 2012) and (RTCA DO-278A, 2011) / (EUROCAE ED-109A, 2012) objectives, activities, explanatory text and software life cycle data that should be addressed when model-based development and verification are used as part of the software life cycle. This includes the artefacts that would be expressed using models and the verification evidence that could be derived from them. Therefore, these supplements also apply to the models developed in the system process that define software requirements or software architecture.

(RTCA DO-332, 2011) / (EUROCAE ED-217, 2012) identify the additions, modifications and deletions to (RTCA DO-178C, 2011) / (EUROCAE ED-12C, 2012) and (RTCA DO-278A, 2011) / (EUROCAE ED-109A, 2012) ob-

jectives when object-oriented technology or related techniques are used as part of the software development life cycle and additional guidance is required. These supplements, in conjunction with (RTCA DO-178C, 2011) / (EUROCAE ED-12C, 2012), are intended to provide a common framework for the evaluation and acceptance of object-oriented technology (OOT) and related techniques-based systems.

(RTCA DO-333, 2011) / (EUROCAE ED-216, 2012) identify the additions, modifications and substitutions to (RTCA DO-178C, 2011) / (EUROCAE ED-12C, 2012) and (RTCA DO-278A, 2011) / (EUROCAE ED-109A, 2012) objectives when formal methods are used as part of a software life cycle, and additional guidance is required.

3.1.4 Space safety standards

All European Cooperation on Space Standardization (ECSS) standard are available on-line at (ECSS Web page, 2014). The three main space safety standards are (ECSS-Q-ST-30C, 2009), (ECSS-Q-ST-40C, 2009) and (ECSS-Q-ST-80C, 2009).

(ECSS-Q-ST-30C, 2009) defines the dependability assurance programme and the dependability requirements for space systems. Dependability assurance is a continuous and iterative process throughout the project life cycle. The ECSS dependability policy for space projects is applied by implementing a dependability assurance programme, which comprises: (i) identification of all technical risks with respect to functional needs which can lead to non-compliance with dependability requirements; (ii) application of analysis and design methods to ensure that dependability targets are met; (iii) optimization of the overall cost and schedule; (iv) inputs to serial production activities. The dependability requirements for functions implemented in software, and the interaction between hardware and software, are identified in this standard. The requirements for the product assurance of software are defined in (ECSS-Q-ST-80C, 2009). The dependability assurance programme supports the project risk management process as described in (ECSS-Q-ST-80C, 2009).

(ECSS-Q-ST-40C, 2009) defines the safety programme and the safety technical requirements aiming at protecting flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, the space system and associated segments and the environment from hazards associated with European space systems. This standard is applicable to all European space projects. This standard may be tailored for the specific characteristic and constraints of a space project in conformance with ECSS-S-ST-00.

(ECSS-Q-ST-80C, 2009) defines a set of software product assurance requirements to be used for the development and maintenance of software for space systems. Space systems include manned and unmanned spacecraft, launchers, payloads, experiments and their associated ground equipment and facilities. Software includes the software component of firmware. This standard also applies to the development or reuse of non-deliverable software which affects the quality of the deliverable product or service provided by a space system, if the service is implemented by software. It interfaces with space engineering and management, which are addressed in the Engineering (-E) and Management (-M) branches of the ECSS System, and explains how they relate to the software product assurance processes. This standard may be tailored for the specific characteristic and constraints of a space project in conformance with ECSS-S-ST-00. Tailoring of this standard to a specific business agreement or project, when software product assurance requirements are prepared, is also addressed.

Other relevant standards include:

- ECSS-E-ST-32-10C Rev.1 Structural factors of safety for spaceflight hardware;
- ECSS-Q-ST-20-07C Quality and safety assurance for space test centres;
- ECSS-Q-ST-30-02C Space product assurance — Failure modes, effects, and criticality analysis (FMECA);
- ECSS-Q-ST-30-11C Rev.1 Space product assurance — Derating - EEE components;
- ECSS-Q-ST-40-02C Space product assurance – Hazard analysis;
- ECSS-Q-ST-40-12 Space product assurance — Fault tree analysis, Adoption notice ECSS/IEC 61025;
- ECSS-M-ST-80 Space project management – Risk management;
- ISO 14620-1:2002 Space systems — Safety requirements — Part 1: System safety;
- ISO 14620-2:2011 Space systems — Safety requirements — Part 2: Launch site operations;
- ISO 14620-3:2005 Space systems — Safety requirements — Part 3: Flight safety systems.

3.1.5 Railway safety standards

3.1.5.1 Regulation

The European railway interoperability Directive 2008/57/EC of 17 June 2008 (Directive 2008/57/EC, 2008) sets out the conditions to be met to achieve interoperability within the Union rail system. These conditions concern the design, construction, placing in service, upgrading, renewal, operation and maintenance of the parts of this

system as well as the professional qualifications and health and safety conditions of the staff who contribute to its operation and maintenance. This Directive repeals Directive 96/48/EC on the interoperability of the European high-speed rail system and Directive 2001/16/EC on the interoperability of the European conventional rail system.

Mandates, also called standardization requests, are the mechanism by which the European Commission (EC) and the EFTA Secretariat request the European Standards Organizations (ESOs) to develop and adopt European standards in support of European policies and legislation.

CENELEC	IEC
50126:1999	62278:2002
50129:2003	62425:2007
50128:2001	62279:2002
50128:2011	62279:2014-draft
50159:2011	62280:2014
50155	60571

Figure 127: Traceability between CENELEC and IEC standards

Through mandate (EC M/483 EN, 2011) CEN, CENELEC and ETSI were asked to draw up a common standardisation programme in support of (Directive 2008/57/EC, 2008) and to undertake to produce the identified standards. As such, the European EN5012x family of railway standards including (CENELEC EN 50126-1, 2010), (CENELEC EN 50128, 2014), (CENELEC EN 50129, 2010), (CENELEC EN 50155, 2012) and (CENELEC EN 20159, 2010) have been developed by the European Committee for Electro-technical Standardization as acceptable means of compliance for (Directive 2008/57/EC, 2008). These European standards apply to both heavy rail systems and light rail and urban mass transportation including people mover systems. Their IEC counterparts (cf. Figure 127) give then an international aura.

3.1.5.2 Acceptable means of compliance

(CENELEC EN 50126-1, 2010) defines RAMS in terms of reliability, availability, maintainability and safety and their interaction; defines a process, based on the system lifecycle and tasks within it, for managing RAMS; enables conflicts between RAMS elements to be controlled and managed effectively; defines a systematic process for specifying requirements for RAMS and demonstrating that these requirements are achieved; addresses railway specifics; does not define RAMS targets, quantities, requirements or solutions for specific railway applications; does not specify requirements for ensuring system security; does not define rules or processes pertaining to the certification of railway products against the requirements of this standard; does not define an approval process by the safety regulatory authority. This European Standard is applicable: to the specification and demonstration of RAMS for all railway applications and at all levels of such an application, as appropriate, from complete railway routes to major systems within a railway route, and to individual and combined sub-systems and components within these major systems, including those containing software; in particular: to new systems; to new systems integrated into existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system; to modifications of existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system at all relevant phases of the lifecycle of an application; for use by Railway Authorities and the railway support industry.

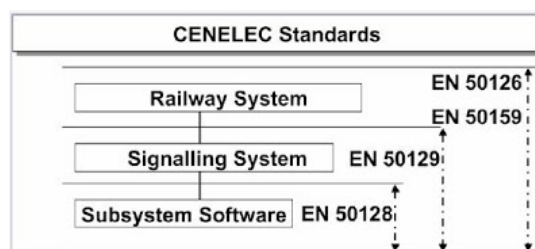


Figure 128: The European EN5012x family of railway signalling standards

(CENELEC EN 50128, 2014) specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications. It is aimed for use in any

area where there are safety implications. These may range from the very critical, such as safety signalling to the non-critical, such as management information systems. These systems may be implemented using dedicated microprocessors, programmable logic controllers, multiprocessor distributed systems, larger scale central processor systems or other architectures.

(CENELEC EN 50129, 2010) applies to the specification, design, construction, installation, acceptance, operation, maintenance and modification / extension phases of complete signalling systems, and also to individual sub-systems and equipment within the complete system. The hazard analysis and risk assessment processes defined in (CENELEC EN 50126-1, 2010) and this standard are necessary for all railway signalling systems / sub-systems / equipment, in order to identify any safety requirements.

(CENELEC EN 50155, 2012) applies to all electronic equipment for control, regulation, protection, supply, etc., installed on rail vehicles and associated with either the accumulator battery of the vehicle or a low voltage power supply source with or without a direct connection to the contact system (transformer, potentiometer device, auxiliary supply); with the exception of electronic power circuits, which conform to EN 50207. This standard covers the conditions of operation, design, construction, and testing of electronic equipment, as well as basic hardware and software requirements considered necessary for competent, reliable equipment. Specific requirements related to practices necessary to assure defined levels of functional safety are to be determined in accordance with §4.6.3.1 and §4.6.3.2 of (CENELEC EN 50126-1, 2010) and its informative Annex A. Software safety integrity level of 1 or higher shall only be considered when it is shown that a residual safety risk remains and that it has to be carried by the software driven programmable electronic system. In such a case, (CENELEC EN 50128, 2014) is applicable. For the purpose of this standard, electronic equipment is defined as equipment mainly composed of semiconductor devices and recognized associated components. These components will mainly be mounted on printed boards.

(CENELEC EN 20159, 2010) is applicable to safety-related electronic systems using for digital communication purposes a transmission system which was not necessarily designed for safety-related applications and which is – under the control of the designer and fixed during the lifetime, or – partly unknown or not fixed, however unauthorised access can be excluded, or – not under the control of the designer, and also unauthorised access has to be considered. Both safety-related equipment and non-safety-related equipment can be connected to the transmission system. This standard gives the basic requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system. This European standard is applicable to the safety requirement specification of the safety-related equipment connected to the transmission system, in order to obtain the allocated safety integrity requirements. Safety requirements are generally implemented in the safety-related equipment, designed according to (CENELEC EN 50129, 2010). In certain cases these requirements may be implemented in other equipment of the transmission system, as long as there is control by safety measures to meet the allocated safety integrity requirements. The safety requirement specification is a precondition of the safety case of a safety-related electronic system for which the required evidence is defined in (CENELEC EN 50129, 2010). Evidence of safety management and quality management has to be taken from the latter. The communication-related requirements for evidence of functional and technical safety are the subject of this standard.

(IEC 62278, 2002) provides Railway Authorities and railway support industry with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS. Processes for the specification and demonstration of RAMS requirements are the cornerstones of this standard. This standard aims to promote a common understanding and approach to the management of RAMS.

3.1.6 Medical devices safety standards

A medical device is an instrument, apparatus, implant, in vitro reagent, or similar or related article that is used to diagnose, prevent, or treat disease or other conditions, and does not achieve its purposes through chemical action within or on the body (which would make it a drug).

3.1.6.1 Regulation

Rules that relate to safety and performance of medical devices were harmonised in the EU in the 1990s. The *New Approach* was defined in a European Council Resolution of May 1985

In Europe, the core legal framework consists of three directives (EC DG Health & Consumers, 2014) elaborated in the 90s: (i) Directive 90/385/EEC regarding active implantable medical devices; (ii) Directive 93/42/EEC regarding medical devices; and (iii) Directive 98/79/EC regarding in vitro diagnostic medical devices. These three main directives have been supplemented over time by several modifying and implementing directives, including Directive 2007/47 EC, and in September 2012, new legislation aimed at enhancing safety, traceability, and transparency.

In the US, Title 21 of the Code of Federal Regulations (CFR) is reserved for rules of the Food and Drug Administration (FDA). The classification of medical devices is described under (21 CFR 860, 2014), whilst a series of guidance for industry is provided under (21 CFR 820, 2014).

3.1.6.2 Acceptable means of compliance

(IEC 62304, 2006) defines the life cycle requirements for medical device software. The set of processes, activities, and tasks described in this standard establishes a common framework for medical device software life cycle processes. It applies to the development and maintenance of medical device software when software is itself a medical device or when software is an embedded or integral part of the final medical device. This standard does not cover validation and final release of the medical device, even when the medical device consists entirely of software.

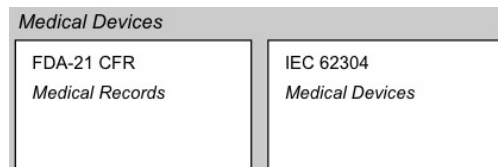


Figure 129: Some safety standards for medical devices

As shown in Figure 120 on page 93, (IEC 60601-1-SER, 2014) is one of the domain specific standard derived from (S + IEC 61508, 2010). It groups in its 1368 pages a set of technical standards for the safety and effectiveness of medical electrical equipment, consisting of a general standard, about 10 collateral standards, and about 60 particular standards. It has become a widely accepted benchmark for medical electrical equipment and compliance with the general standard has become a requirement for the commercialisation of electrical medical equipment in many countries.

Recognizing that medical devices are incorporated into IT-networks to achieve desirable benefits (for example, interoperability), (IEC 80001-1, 2010) defines the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security (the key properties). It does not specify acceptable risk levels. It applies after a medical device has been acquired by a responsible organization and is a candidate for incorporation into an IT-network. It applies throughout the life cycle of IT-networks incorporating medical devices. The standard applies where there is no single medical device manufacturer assuming responsibility for addressing the key properties of the IT-network incorporating a medical device. It applies to responsible organizations, medical device manufacturers and providers of other information technology for the purpose of risk management of an IT-network incorporating medical devices as specified by the responsible organization. It does not apply to personal use applications where the patient, operator and responsible organization are one and the same person.

(ISO 14971, 2007) specifies a process for a manufacturer to identify the hazards associated with medical devices, including in vitro diagnostic medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls. The requirements are applicable to all stages of the life-cycle of a medical device.

3.1.7 Nuclear safety standards

At system level, the main international standards are (IEC 61226, 2009), (IEC 61513, 2011), (IAEA NS-G-1.3, 2002) and (IAEA SSR-2/1, 2012)⁵². At software level, the main international standards are (IEC 60880, 2006), (IEC 62138, 2004) and (IAEA NS-G-1.1, 2000).

(IEC 61226, 2009) establishes a method of classification of the information and command functions for nuclear power plants, and the instrumentation and control systems and equipment that provide those functions, into categories that designate the importance to safety of the function. The resulting classification then determines relevant design criteria. It is applicable to all the information and command functions and the instrumentation and control systems and equipment that provide those functions.

Instrumentation and control (I&C) systems important to safety may be implemented using conventional hard-wired equipment, computer-based (CB) equipment or by using a combination of both types of equipment. (IEC 61513, 2011) provides requirements and recommendations for the overall I&C architecture which may contain either or both technologies. It refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with

⁵² Supersedes (IAEA NS-R-1, 2000).

(IEC 61513, 2011) as a consistent document set. At a third level, IEC SC 45A standards not directly referenced by (IEC 61513, 2011) are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own. A fourth level extending the IEC SC 45A standard series corresponds to the Technical Reports which are not normative.

(IEC 61513, 2011) calls for the establishment of an overall security plan to specify the procedural and technical measures to be taken to protect the architecture of I&C systems from digital attacks that may jeopardise functions important to safety. For more details, please refer to (IEC 62645, 2014) as described in §3.2.5.

(IAEA SSR-2/1, 2012) establishes design requirements for the structures, systems and components of a nuclear power plant, as well as for procedures and organizational processes important to safety, that are required to be met for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events, were they to occur. This publication is intended for use by organizations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning for nuclear power plants, in analysis, verification and review and in the provision of technical support, as well as by regulatory bodies.

(IAEA NS-G-1.3, 2002) provides general guidance on I&C systems important to safety which is broadly applicable to many nuclear power plants. More detailed requirements and limitations for safe operation specific to a particular plant type should be established as part of the design process. The present guidance is focused on the design principles for systems important to safety that warrant particular attention, and should be applied to both the design of new I&C systems and the modernization of existing systems. Guidance is provided on how design principles should be applied, on the basis of a method of classifying systems by their importance to safety.

(IAEA NS-R-1, 2000) establishes safety requirements that define the elements necessary to ensure nuclear safety. These requirements are applicable to safety functions and the associated structures, systems and components, as well as to procedures important to safety in nuclear power plants.

(IEC 60880, 2006) provides requirements for the software of computer-based instrumentation and control (I&C) systems of nuclear power plants performing functions of safety category A as defined by (IEC 61226, 2009). The standard provides requirements for the purpose of achieving highly reliable software. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation.

(IEC 62138, 2004) provides requirements for the software of computer-based I&C systems performing functions of safety category B or C as defined by (IEC 61226, 2009). This standard complements (IEC 60880, 2006), which provides requirements for the software of computer-based I&C systems performing functions of safety category A. It is also consistent with, and complementary to (IEC 61513, 2011).

(IAEA NS-G-1.1, 2000) provides guidance on the collection of evidence and preparation of documentation to be used in the safety demonstration for the software for computer based systems important to safety in nuclear power plants, for all phases of the system life cycle.

3.1.8 Process industry safety standards

The Functional safety - Safety instrumented systems for the process industry sector (IEC 61511-SER, 2004) standard comprises 3 parts. This standard has been developed as a process sector implementation of (S + IEC 61508, 2010). Part 1 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and / or maintain the process in a safe state. Part 2 provides guidance on the specification, design, installation, operation and maintenance of Safety Instrumented Functions and related safety instrumented system as defined in Part 1. Part 3 provides information on the underlying concepts of risk, the relationship of risk to safety integrity, the determination of tolerable risk, a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined.

3.2 Overview of security standards

3.2.1 Regulation

(Obama, 2013) establishes 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. This Executive Order is at the origin of the creation of the (NIST Cybersecurity Framework, 2014), cf. §3.2.3, with significant impacts on the overall security engineering domain, e.g. (Boeing Cybersecurity Framework, 2013).

In Europe, security is a National sovereignty prerogative, therefore, to our knowledge, there is no relevant regulation, with the exception of regulation related to privacy, including the processing of personal data and the free movement of such data (Directive 95/46/EC, 1995), (EU COM(2012) 11 final, 2012). In that respect, it is interesting to see that a number of industrial standards are emerging in advance to the regulation.

3.2.1.1 Aerospace domain specific regulation

Aircraft type certification currently acts in the absence of comprehensive rules and guidance for how cybersecurity 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 model, e.g. for the Boeing 787-8 whose digital systems architecture may allow connection to and access from external sources and airline operator networks to the previously isolated Aircraft Control Domain and Airline Information Domain (25-356-SC, 2008), (25-357-SC, 2007). Thus, these Special Conditions establish new requirements for: (i) the protection of the Aircraft Control Domain and Airline Information Domain systems, hardware, software, and databases from unauthorized access; (ii) the protection of field-loadable software applications and databases that are electronically transmitted from external sources to the on-aircraft networks and storage devices, and used within the Aircraft Control Domain and Airline Information Domain; and (iii) the test and evaluation of security protection means and change control procedures of aircraft systems, hardware, software, and databases, especially for critical systems and those areas that could affect safety of flight.

Another set of regulations, related to Civil Aviation Security, is available under (49 CFR XII-C, 2014). This regulation is referenced by 14 CFR Part 121 - Operating Requirements: Domestic, Flag, and Supplemental Operations (14 CFR, 2014), but it deals essentially with physical security.

3.2.2 Scope

The number of international and national security standards is rather overwhelming (cf. Figure 130 and Figure 131).

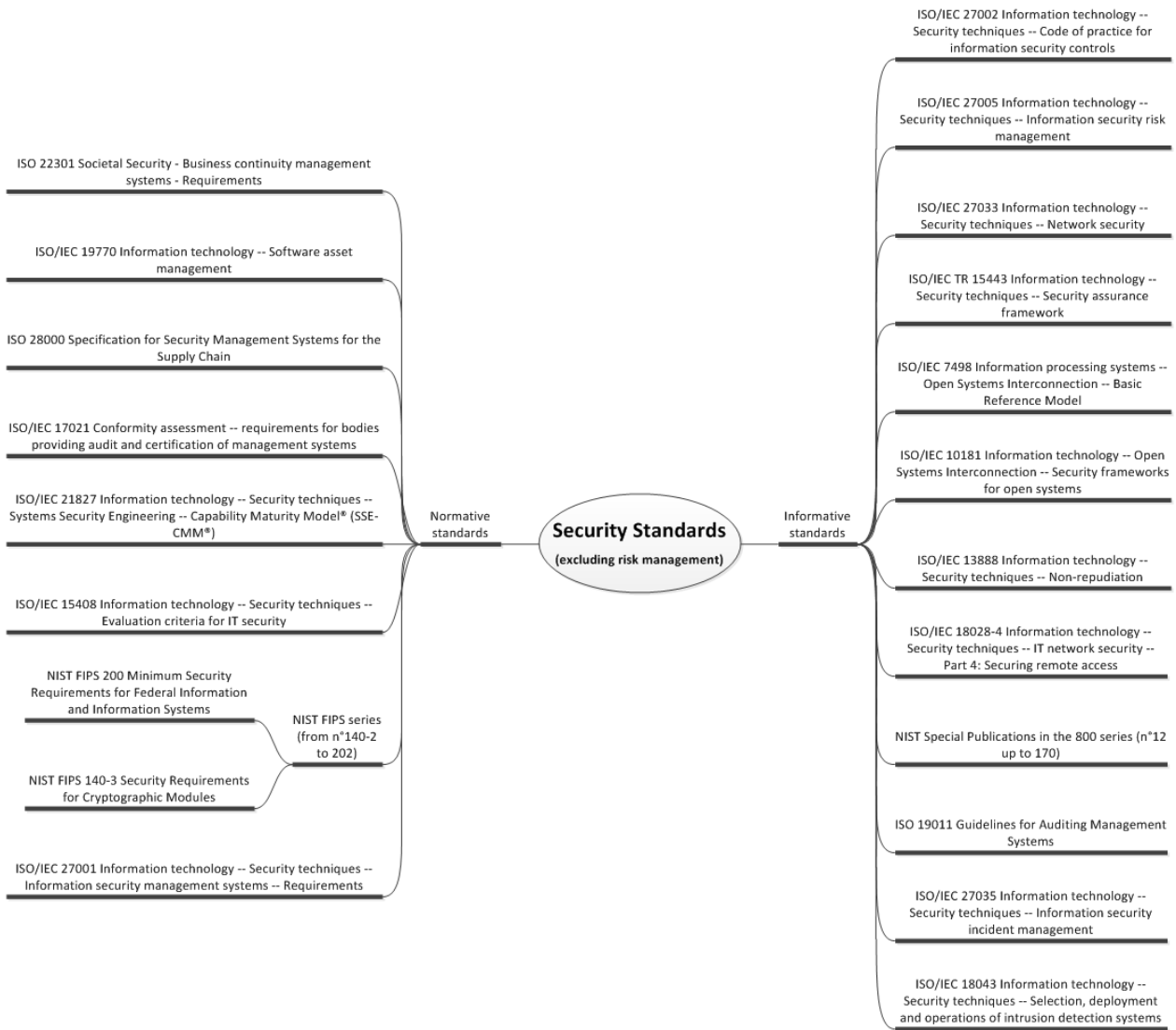


Figure 130: Some significant security standards

To keep this state of the art within reasonable bounds, this overview only encompasses the standards that have been cited elsewhere in this document, and in particular in the research state of the art (cf. §2), thus addressing only those standards for which some form of integration has been envisaged by the safety and / or security communities.

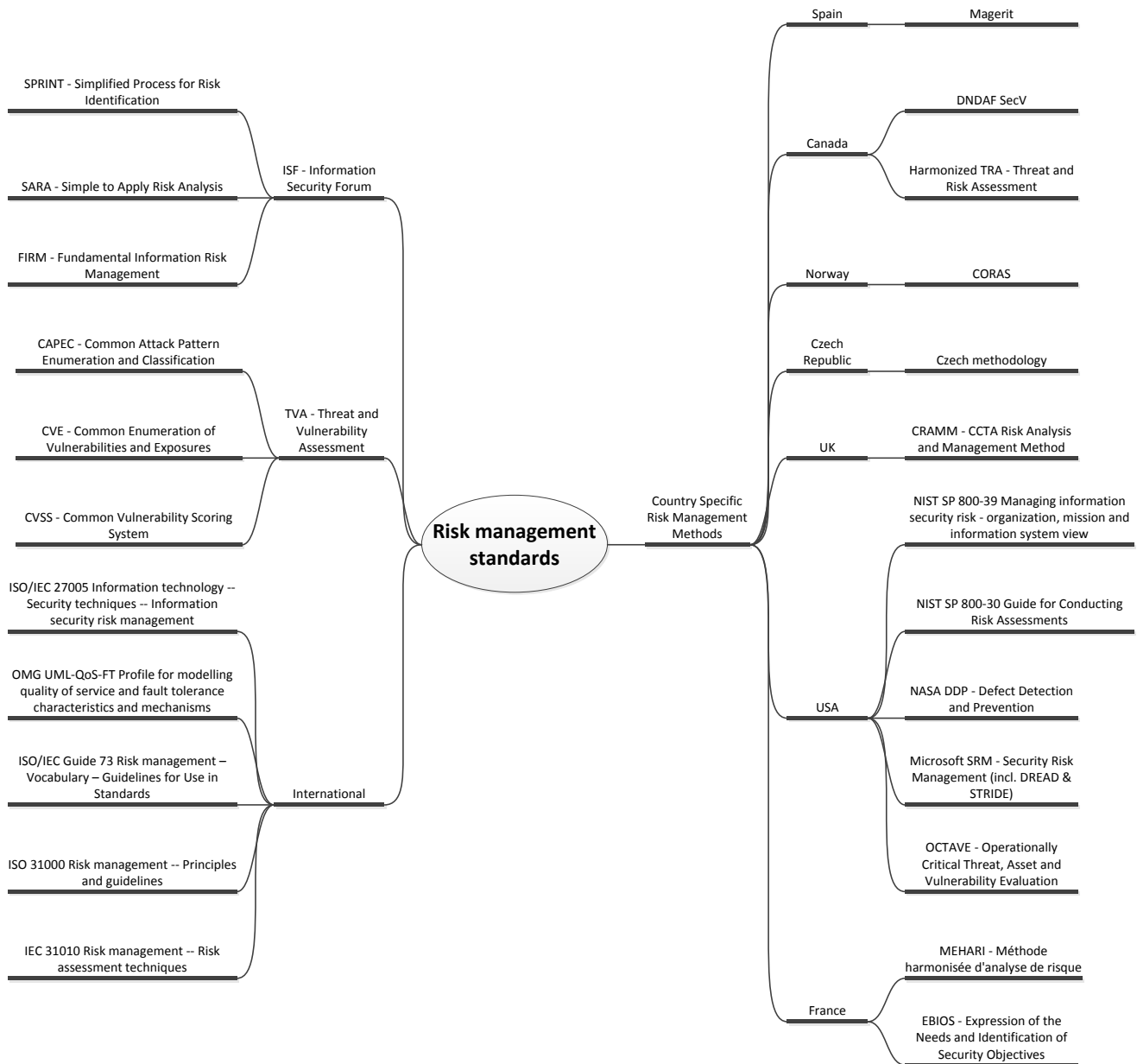


Figure 131: Some significant (security) risk management standards

3.2.3 Cross-domain standards

3.2.3.1 Cyber-security frameworks

The (NIST Cybersecurity Framework, 2014) was published as a result of Executive Order 13636 (Obama, 2013). It focuses on using business drivers to guide cyber-security activities and considering cyber-security risks as part of the organization’s risk management processes. The framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cyber-security activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help organizations align the cyber-security activities with their business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cyber-security risk.

3.2.3.2 Security evaluation standards and related documents

The root of the activities on security evaluation can be traced back to the development of Trusted Computer System Evaluation Criteria (TCSEC, 1985), a.k.a. the Orange Book, by the US National Computer Security Council (NCSC), which was then adopted by the US DoD. The document is mainly concerned by the data confi-

deniality problem, considering data integrity and availability as secondary issues. This was a typical military approach at the release time of these criteria.

In Europe, around the end of the 1980s, some countries started defining their own national security evaluation programs, developing and publishing country-specific security evaluation criteria. Later, with the support of the European Commission, the Information Technology Security Evaluation Criteria (ITSEC, 1991) was derived as a harmonised approach from the schemes that had been defined in the UK, France, Germany and the Netherlands.

Together (TCSEC, 1985) and (ITSEC, 1991) were the major input documents for the Common Criteria (ISO/IEC 15408-1, 1999), (ISO/IEC 15408-2, 1999), (ISO/IEC 15408-3, 1999), in which the IT Security Evaluation approaches of North America and Europe were harmonised.

(ISO/IEC 15408-1, 2009) establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products. Part 1 describes the various parts of ISO/IEC 15408, defines the terms and abbreviations to be used, establishes the core concepts of a Target of Evaluation (TOE) and evaluation context, and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is also given. Part 1 defines the various operations by which the functional and assurance components given in (ISO/IEC 15408-2, 2008) and (ISO/IEC 15408-3, 2008) may be tailored through the use of permitted operations. The key concepts of Protection Profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. (ISO/IEC 15408-1, 2009) gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology is given in (ISO/IEC 18045, 2008) and the scope of evaluation schemes is provided.

(ISO/IEC 15408-2, 2008) defines the content and presentation of the security functional requirements to be assessed in a security evaluation using the Common Criteria. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes. Part 2 also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.

(ISO/IEC 15408-3, 2008) defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets. Part 3 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

(ISO/IEC 18045, 2008) is a companion document to the Common Criteria standard. It defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation. The standard does not define evaluator actions for certain high assurance components.

(ETR 367, 1997) describes and investigates existing relationships between security evaluation procedures and the production of European Telecommunications Standards Institute (ETSI) standards including security features.

3.2.3.3 The ISO/IEC 27k series

(ISO/IEC 27000, 2014) provides the overview of Information Security Management Systems (ISMS), and terms and definitions commonly used in the ISMS family of standards.

(ISO/IEC 27001, 2013) formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted this standard can therefore be formally audited and certified compliant with the standard.

(ISO/IEC 27002, 2013) gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: (i) select controls within the process of implementing an Information Security Management System based on (ISO/IEC 27001, 2013); (ii) implement commonly accepted information security controls; (iii) develop their own information security management guidelines.

(ISO/IEC 27005, 2011) provides guidelines for information security risk management. It supports the general concepts specified in (ISO/IEC 27001, 2013) and is designed to assist the satisfactory implementation of information security based on a risk management approach.

3.2.3.4 The IEC 62443 series

The Industrial Communication Networks - Network and System Security series is a set of twelve standards currently elaborated by the International Society for Automation (ISA). The individual parts of the standard are at different stages of development, some being published (IEC/TS 62443-1-1, 2009), (IEC 62443-2-1, 2010), (IEC/TR 62443-3-1, 2009), (IEC 62443-3-3, 2013), while others are still drafts. The core goal of the standard is to define Foundational Requirements (FRs) and Security Levels (SLs). The seven FRs are⁵³: (i) identification and authentication control; (ii) use control; (iii) system integrity; (iv) data confidentiality; (v) restricted data flow; (vi) timely response to events; and (vii) resource availability. For each FR, a different SL may be assigned. The four SLs, based on attacker capabilities and motivation, are: (i) casual or unintended; (ii) simple means: low resources, generic skills and low motivation; (iii) sophisticated means: moderate resources, IACS-specific skills and moderate motivation; and (iv) sophisticated means: extended resources, IACS-specific skills and high motivation. If the SL of the design or the SL of the implementation does not match the targeted SL, then additional countermeasures must be taken.

It can also be noted that there currently is a German initiative to apply the IEC 62443 series to railway. See (Braband, 2016) for details.

3.2.4 Aerospace domain specific security standards

The Airworthiness Security Process Specification (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014) is a resource for Airworthiness Authorities (AA) and the aviation industry for certification when the development or modification of aircraft systems and the effects of intentional unauthorized electronic interaction can affect aircraft safety. It deals with the activities that need to be performed in support of the airworthiness process when it comes to the threat of intentional unauthorized electronic interaction (the "What"). As key documents in this state of the art, an extended description of (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014) is given in appendix, cf. §9.1.

The Airworthiness Security Methods and Considerations standard (RTCA DO-356, 2014) was developed in the context of the Airworthiness Security Process Specification (RTCA DO-326A, 2014) / (EUROCAE ED-202A, 2014) which addresses type certification considerations during the first three life cycle stages of an aircraft type (i.e. Initiation, Development or Acquisition, and Implementation) and in the context of the Information Security Guidance for Continuing Airworthiness (RTCA DO-355, 2014) which addresses airworthiness security for continued airworthiness. The methods and considerations of this document address the assessment of the acceptability of the airworthiness security risk and the design and verification of the airworthiness security attributes as related to system safety and airworthiness. More specifically, this guidance addresses the following areas: (i) it provides guidance for accomplishing the activities identified in (RTCA DO-326A, 2014) in the areas of Security Risk Assessment and Effectiveness Assurance; (ii) it provides specific methods for Security Risk Analysis and Network Security Domains. The document is intended to be used in conjunction with other applicable guidance material, including (SAE ARP 4754A, 2010), (SAE ARP 4761A, 2004), (RTCA DO-178C, 2011), and (RTCA DO-254, 2000) and with the advisory material associated with FAA AC 25.1309-1A (14 CFR, 2014) and EASA AMC 25.1309 (EASA CS-25, 2014). As key document in this state of the art, an extended description of (RTCA DO-356, 2014) is given in appendix, cf. §9.2. It is to be noted that the European Organization for Civil Aviation Equipment (EUROCAE) counterpart standard has not yet been published.

The Information Security Guidance for Continuing Airworthiness (EUROCAE ED-204, 2014) / (RTCA DO-355, 2014) are a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. They deal with the activities that need to be performed in operation and maintenance of the aircraft related to information security threats. These documents also provide guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects). Thus, they also supports harmonizing security guidance documents among Design Approval Holders (DAHs), which is deemed beneficial to DAHs, operators and civil aviation authorities. They are companion documents to (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014) that supports security in the development and modification part of the airworthiness process.

The ARINC 653 series is a software specification for space and time partitioning in Safety-critical avionics real-time operating systems. It allows to host multiple applications of different software levels on the same hardware in the context of an Integrated Modular Avionics architecture. In order to decouple the RTOS platform from the application software, ARINC 653 defines an API called APplication EXecutive (APEX). Each application software is called a partition and has its own memory space. It also has a dedicated time slot allocated by the APEX API. Within each Partition, multitasking is allowed. The APEX API provides services to manage partitions, pro-

⁵³ This approach is similar to the one in the Common Criteria.

cesses and timing, as well as partition/process communication and error handling The series is currently organised in 5 parts: overview (ARINC 653P0, 2013), required services (ARINC 653P1-3, 2010), extended services (ARINC 653P2-2, 2012), conformity test specification (ARINC 653P3A, 2014) and subset services (ARINC 653P4, 2012).

The purpose of (ARINC 811, 2005) is to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts (cf. Figure 132). This common understanding was found important in the early 2000's, since a number of subcommittees and working groups within the aeronautical industry were considering aircraft information security⁵⁴. This document also provides an aircraft information security process framework relating to airline operational needs that, when implemented by an airline and its suppliers, will enable the safe and secure dispatch of the aircraft in a timely manner. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.

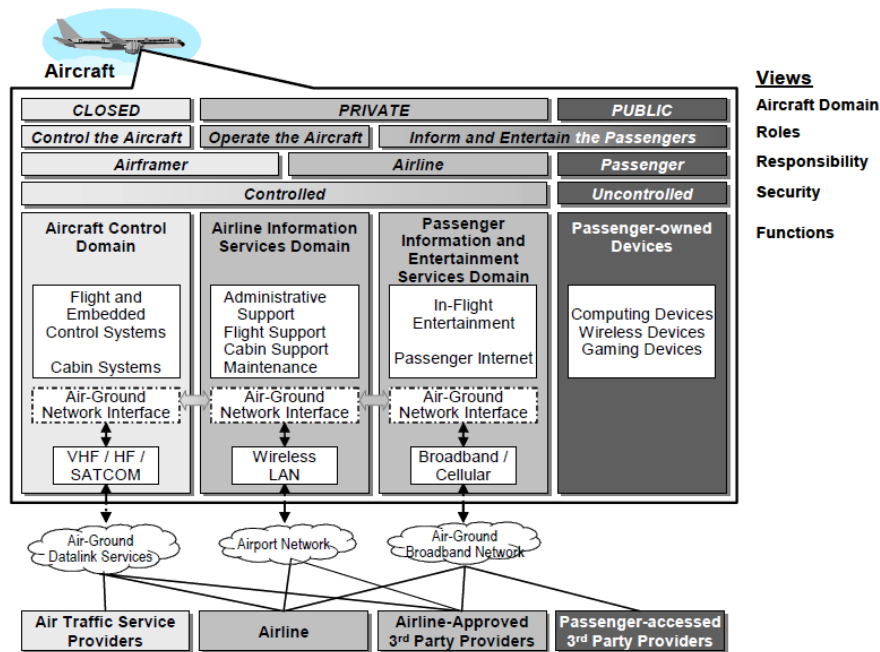


Figure 132: Aircraft Network Domains and Interconnections among Domains (ARINC 811, 2005)

In Australia, the Administration of Aircraft & Related Ground Support Network Security Programs (CASA CAAP 232A, 2013) provides guidance material for the introduction and continued airworthiness of aircraft network security programs.

3.2.5 Nuclear domain specific security standards

The (IEC 62645, 2014) standard specifically focuses on the issue of requirements for computer security programmes and system development processes to prevent and/or minimize the impact of attacks against I&C computer-based systems possibly integrating HPD, i.e. Hardware Description Language (HDL) Programmed Devices. (IEC 62645, 2014) has been developed using the ISO/IEC 27000 series, IAEA and country specific guidance as sources of information along with a dedicated working group which contributed to the standard development. (IEC 62645, 2014) is expected to be stabilised in 2015. This standard provides mapping with (ISO/IEC 27001, 2013) and (NIST SP 800-82, 2013) on a structural level.

(IEC 62645, 2014) identifies that the consequences of cyber-attack regarding safety shall be assumed as more serious than those regarding plant performance. The standard considers the link between safety categories, safety classes and security degrees. It provides insights to security graded approach in order to defend plant safety and performance against cyber threats. This approach is built on a consequence-based analysis.

⁵⁴ Typically, in November 2005, the European Organization for Civil Aviation Equipment (EUROCAE) approved formation of Working Group 72, *Aeronautical Systems Security*, to address how information security impacts and augments the safety of aeronautical information systems. WG-72 was tasked with developing guidance material for manufacturers and airworthiness/regulatory authorities, which are responsible for evaluating, assessing, and certifying aircraft information security architectures and implementations.

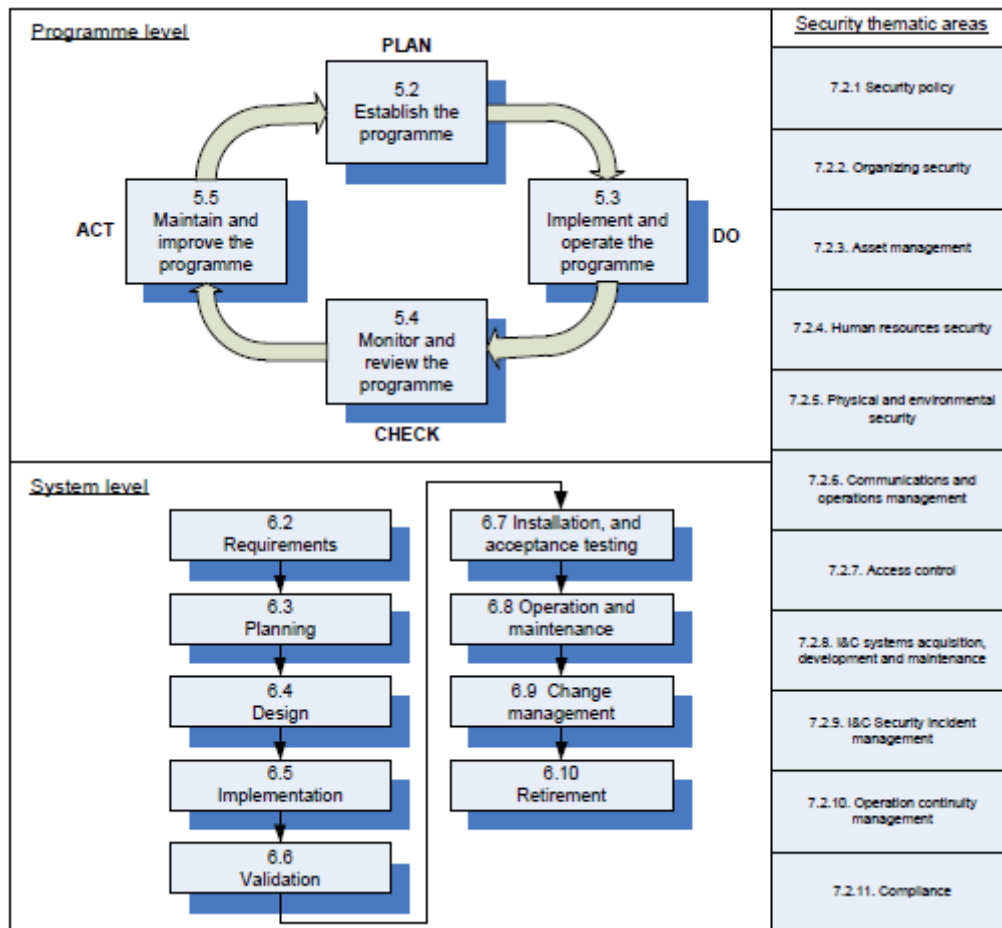


Figure 133: Overall framework of (IEC 62645, 2014)

(IEC 62645, 2014) identifies that compliance with (IEC 61513, 2011) and (IEC 61226, 2009) is needed and it argues that security may benefit from safety provisions implemented to comply with requirements of (IEC 61513, 2011) and of other IEC standards that are safety-relevant. (IEC 62645, 2014) inherits the PDCA-model as depicted in Figure 133.

The International Electrotechnical Commission has considered that 3 security degrees⁵⁵ were necessary and sufficient to grade security measures for all I&C CB&HPD systems: S1 for I&C CB&HPD systems processing safety category A functions and functions which could have the same impact on safety when manipulated maliciously; S2 for I&C CB&HPD systems processing safety categories B functions or functions which could have the same impact on safety when manipulated maliciously and systems processing functions necessary to operate the plant; S3 for I&C CB&HPD systems which cannot impact in real time either plant safety or plant availability.

3.3 Overview of standards transverse to safety and security

(ISO/IEC 15026-1, 2013) defines assurance-related terms and establishes an organized set of concepts and their relationships, thereby establishing a basis for shared understanding of the concepts and principles central to all parts of this standard across its user communities.

Assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security, although these assurance cases are often called by more specific names, e.g. safety case or security case. (ISO/IEC 15026-2, 2011) specifies minimum requirements for the structure and contents of an assurance case. An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underlie this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions.

⁵⁵ Similar to the 3 safety categories defined in (IEC 61226, 2009).

(ISO/IEC 15026-3, 2011) specifies the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their integrity level requirements, including the assignment of integrity levels to systems, software products, their elements, and relevant external dependencies. One important use of integrity levels is to aid in assuring safety, economic, or security characteristics between suppliers and acquirers of a system or product.

To support the systems assurance process (ISO/IEC 15026-2, 2011), the Object Management Group (OMG) has standardised a meta-model for representing structured assurance cases, called the Structured Assurance Case Meta-model (OMG SACM, 2013). The SACM combines previous OMG specifications, in particular the ARGument Meta-model (ARM) and the Software Assurance Evidence Meta-model (SAEM). In ARM, a structured argument comprises a graph of assertions (claims), ultimately supported by evidence, and links are asserted relationships between claims, context and evidence. ARM harmonises common elements from the Claims-Arguments-Evidence (CAE) notation and the Goal Structuring Notation (GSN). Version 1.0 of SACM is a recommended OMG specification for adoption, for which tool support is readily available.

(ISO 31000, 2009) is a short document (24 pages) that provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

(IEC 31010, 2009) is a dual logo IEC/ISO, single prefix IEC, supporting standard for (ISO 31000, 2009) and provides guidance on selection and application of systematic techniques for risk assessment. This standard is not intended for certification, regulatory or contractual use. This standard does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature. Guidance on the introduction of safety aspects into IEC standards is laid down in ISO/IEC Guide 51.

(IEC 62859, 2015) aims at optimising the integration of cyber-security provisions in nuclear I&C architecture and systems, to prevent conflicts between safety and cyber-security provisions, and to aid the identification and the leveraging of the potential synergies between safety and cyber-security.

3.4 Analysis of standards w.r.t. safety and security co-engineering concerns

Above, we listed and briefly described a large number of safety and security standards and regulation. Because this enumeration may be difficult to read, this section highlights how safety and security co-engineering is considered in different safety-critical domains.

3.4.1 Analysis of transverse safety standards

It is interesting to trace the evolution of the IEC 61508 standard in terms of security concerns. In (IEC 61508-1, 1998), clause 1.2.j states 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/PE⁵⁶ safety-related systems.”*

By contrast, (S + IEC 61508, 2010) 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 security required for the achievement of functional safety.”
- In clause 7.4.2.3: “[...] If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out”.
- In clause 7.5.2.2: “If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements.”

Multiple papers discuss the IEC 61508 standard and its evolution, e.g.: (Corneillie, et al., 1999), (Ibrahim, et al., 2004), (Novak, et al., 2007), (Hansen, 2009), (PARSEC, 2009), (Mc Guire, 2011), (Reichenbach, et al., 2012), (Mazzini, et al., 2014), (Schoitsch, 2014), (Favaro, et al., 2014).

3.4.2 Analysis of automotive safety standards

The 10 parts Road vehicles -- Functional safety standard (ISO 26262-1, 2011) - (ISO 26262-10, 2012) does not yet include security considerations. However, this point is becoming a hot topic, cf. (Czerny, 2013) and (Gebauer, 2014).

⁵⁶ Electrical / Electronic / Programmable Electronic.

3.4.3 Analysis of aviation safety standards

Together with automotive and electrical/electronic/programmable electronic safety standards, the avionics safety standards are amongst the most discussed standards (cf. §2) in the community, especially in relation to security concerns, e.g. (Corneillie, et al., 1999), (SEISES, 2008), (PARSEC, 2009), (Gutgarts, et al., 2010), (Bieber, et al., 2012), (Blanquart, et al., 2012), (Casals, et al., 2012), (Rowe, 2013), (Joyce, et al., 2014), (Schoitsch, 2014).

In particular (Joyce, et al., 2014) discusses the evolution of the airworthiness security process between the old (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010) and the new (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014). The authors show a move from an integrated process towards more independent safety and security processes with interaction points, as recommended by (SeSaMo D4.1, 2014).

Another significant update between the 2010 and 2014 editions of the Airworthiness Security Process Specification standards relates to the Security Levels. In (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010) the Security Level is used to classify the effectiveness of a security countermeasure or of a design change as required to reach an acceptable risk level, by reducing the threat scenario likelihood, cf. Figure 62. This definition was deemed important because it had a direct impact on the underlying analyses. All discussions on security levels have now been removed from (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014), and inserted under another terminology in (RTCA DO-356, 2014) – see §9.2 for details.

3.4.4 Analysis of space safety standards

Section §5.3 of (ECSS-Q-ST-40C, 2009) reads: “*The implementation of safety requirements shall not be compromised by other requirements. NOTE For example: security requirements*”.

3.4.5 Analysis of railway safety standards

(CENELEC EN 20159, 2010) acknowledges that a safety-related equipment connected through an open transmission system can be subjected to many different IT security threats. In this standard, intentional attacks by means of messages to safety-related applications are thus considered. However, this standard 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.

The scope of the (CENELEC EN 50126-1, 2010) safety standard states in §1.7 that: “*This part of EN 50126 [...] does not specify requirements for ensuring system security.*” However, the standard recalls in a note of §8.1.14.4 that sabotage, vandalism and loss of security may be valid faults to be considered during the System Hazard Analysis.

3.4.6 Analysis of medical devices safety standards

As discussed in (Wikipedia Medical Device, 2014), some medical devices (e.g. pacemakers, insulin pumps, etc.) can be remotely controlled, engendering concern about privacy and security issues around human error and technical glitches. In August 2013, the Food and Drug Administration (FDA) released over 20 regulations (FR-78-151-47712, 2013) aiming to improve the security of data in medical devices, in response to the growing cyber-security risks.

3.4.7 Analysis of nuclear safety standards

The scope of the (IAEA SSR-2/1, 2012) safety standard states in §1.7 that: “*This publication does not address: [...] ; (b) Matters relating to nuclear security [...]*”. However, in the same standard, requirement n°8 – Interfaces of safety with security and safeguards, reads: “*Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.*” The standard does not address how this co-engineering is to be performed. On the contrary, the standard specifies that: “*Security related publications are issued in the IAEA Nuclear Security Series.*”

The (IAEA NS-G-1.3, 2002) safety standard includes provisions of control of access to equipment. In §4.51, it is stated that: “*Access to equipment in systems important to safety should be appropriately limited, in view of the need to prevent both unauthorized access and the possibility of error by authorized personnel. Effective methods include appropriate combinations of physical security (locked enclosures, locked rooms, alarms on panel doors) and administrative measures according to the degree of supervision in the area where the equipment is located.*”

In the (IAEA NS-G-1.1, 2000) safety standard, there are multiple references to security:

- In §3.15 – Security, it is written that: “*It should be demonstrated that measures have been taken to protect the computer based system throughout its entire lifetime against physical attack, intentional and non-*

intentional intrusion, fraud, viruses and so on [12, 13]. Safety systems should not be connected to external networks when justification cannot be made that it is safe to do so.”

- In §5.20 – Non-functional requirements, it is written that: *“The security requirements should be derived from the safety policy that has been defined for the computer based system environment and [...]”*
- In §6.38 – Security considerations, it is stated that: *“As part of the need to maintain strict configuration control of the computer system, the computer system design should determine how intentional or inadvertent corruption of the computer system’s functionality (for example by unauthorized access, unauthorized code or a virus) is to be prevented [12, 13]. This should include details of procedural or other controls on how changes to the system are to be made and verified and how unauthorized changes are to be prevented. There should be an analysis of the threats to security together with a justification of the level of security to be implemented.”*

Thus, (IAEA NS-G-1.1, 2000) is a typical case of safety-informed security engineering process, where the minimal security requirements include password management, and secure software storage arrangements and procedural controls for software updates.

In the forthcoming IAEA and IEC guidance, it can be seen that the integration of safety and security is evolving. The draft technical guide (NST036, 2014) has a dedicated chapter that deals with the relationship between computer security and safety. It also uses as a reference IAEA safety guidance (IAEA DSSR, 2012).

Furthermore, IAEA is nowadays talking about the 3S⁵⁷ concept where the S’s stand for Safety, Security and Safeguards. This is also visible in (NST036, 2014), as it states that cyber-attacks that directly cause sabotage and cyber-attacks that collect information that can facilitate sabotage of the nuclear facility (security issue) or theft of nuclear material are subjects of consideration (safeguards issue).

The International Electrotechnical Commission asserts that standards such as (ISO/IEC 27001, 2013) and (ISO/IEC 27002, 2013) are not directly applicable to the cyber protection of nuclear I&C CB&HPD systems. The main reason behind this assertion is that cyber-security cannot be handled independently from safety. In particular:

- §1.3 states that the overall security plan must specify the procedural and technical measures to be taken to protect the architecture of I&C systems from digital attacks that may jeopardise functions important to safety;
- §5.1.2 states that the computer security programme must not inadvertently affect the systems important to safety;
- §5.2.3.1.1 states that consequences of cyber-attacks regarding safety shall be assumed as more serious than those regarding plant performance.

For more details, please refer to:

- (IEC 60880, 2006), which has 2 sections, namely §5.7 and §12.2, that discuss software security;
- (Pietre-Cambacedes, et al., 2013b) and (Pietre-Cambacedes, et al., 2015), which presents some standardisation activities in the nuclear business which is not discussed above, e.g. (IEC 62645, 2014) and (IEC 62859, 2015);
- (Abousahl, et al., 2015), which provides practical feedback on 3S implementation, and to which MERgE partners have significantly contributed.

3.4.8 Overall analysis

Requirement and assurance levels are an important contribution of standards towards safety and security engineering, e.g.

- the IEC 61508 series⁵⁸ defines four Safety Integrity Levels (SILs),
- the Road vehicles -- Functional safety standard (ISO 26262-1, 2011) - (ISO 26262-10, 2012) provides an automotive specific adaptation of these levels called the Automotive Safety Integrity Levels (ASILs),
- the IEC 62443⁵⁹ series defines four Security Levels (SLs),

⁵⁷ The IAEA Safety Glossary defines **Safety** as “the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards.” **Security** is according to IAEA definition, “the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.” **Safeguards** is defined as the control regime for ensuring non-proliferation of nuclear materials and sensitive technology and as such a precondition for the peaceful use of nuclear technology. In addition to the classic ideas of a State System for Accounting and Control (SSAC) of nuclear materials, modern integrated safeguards encompass the State nuclear fuel cycle and related research & development, manufacturing, and import & export.

⁵⁸ From (IEC 61508-1, 1998) to (IEC 61508-7, 2000).

⁵⁹ See (IEC/TS 62443-1-1, 2009), (IEC 62443-2-1, 2010), (IEC/TR 62443-3-1, 2009), and (IEC 62443-3-3, 2013).

- the (RTCA DO-178C, 2011) / (EUROCAE ED-12C, 2012) define five Development Assurance Levels (DALs),
- the (EUROCAE ED-109A, 2012) / (RTCA DO-278A, 2011) define six Assurance Levels (ALs),
- the (ISO/IEC 15408-3, 2008) defines seven Evaluation Assurance Levels (EALs).

Safety and security levels have in common to define scales by which safety, security and / or process assurance can be enforced and measured, so as to reduce risk to a tolerable level. Enforcement is attained by linking methods & techniques to levels.

However, there is neither common scale throughout the standards, with major differences in terms of number of levels, and in terms of qualitative versus quantitative levels, nor a common mapping of levels to sets of required methods & techniques.

In the aeronautical domain, (RTCA DO-356, 2014) establishes a mapping between safety and security levels, cf. §9.2 for more details.

3.5 Detailed analysis of the taxonomy of safety and security standards

This section initially aimed at analysing the taxonomy of concepts in different safety and security standards, with the goal of identifying potential commonalities. As shown in §3, a significant number of safety and security standards were considered. Considering the time and effort available on the project, we short-listed four standards for detailed analysis: two safety-related, i.e. (S + IEC 61508, 2010) and (RTCA DO-178C, 2011) / (EUROCAE ED-12C, 2012), and two security-related, i.e. (ISO/IEC 27000, 2014) and (ISO/IEC 15408-1, 2009).

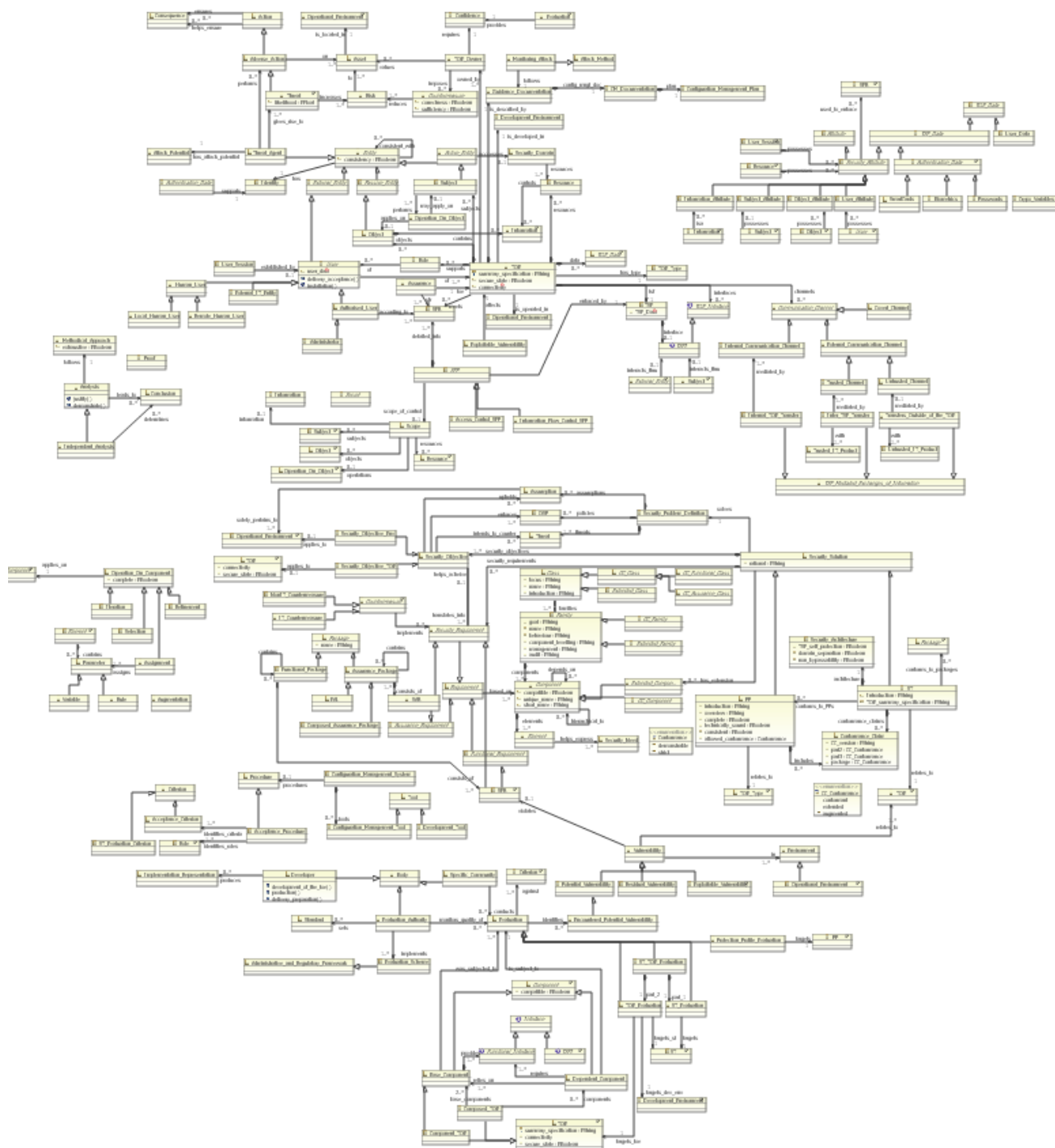


Figure 134: Taxonomy of security terms in (ISO/IEC 15408-1, 2009)

Work started on (ISO/IEC 15408-1, 2009) using the MERgE platform as modelling tool. However, considering the complexity of the taxonomy (cf. Figure 134) comprising some 200 classes, it appeared rapidly that not much could be gained from this detailed analysis, so this analysis was stopped.

Instead, two experiments were led in parallel:

- the development of an extension of a Failures Modes, Effects and Criticality Analysis (FMECA) commercial tool, namely SafetyArchitect, to deal with security concerns (cf. Part B, §3);
- the detailed assessment of an academic tool, namely TTool/AVATAR (AVATAR, 2015) allowing for the modelling and formal verification of safety and security properties (cf. Part B, §4).

4 A state of the art in safety and security co-engineering in industry

A state of the art in safety and security co-engineering research has been covered in §2 and a state of the art in safety and security co-engineering in education has been covered in §5. This section examines industrial safety and security co-engineering offers currently available on the market. An insight is also given on safety and security co-engineering in the computing domain at Thales. Note that turnkey safety and security solutions are excluded from this state of the art; the focus is exclusively on co-engineering offers.

4.1.1 Market offers

4.1.1.1 Commercial safety and security frameworks

Surety (Hessami) is a practical case of safety and security analysis and assurance framework deployed and used by industry. Atkins is one of the world's leading design, engineering and project management consultancies, with over 17.000 employees and £1.7 billion in revenue. Surety is an umbrella approach to identification, assessment and management of risks in safety, security and environmental performance of products, processes, systems and services. It is targeted at 3 key sectors: (i) multimodal transportation; (ii) critical assets and infrastructures; and (iii) information systems.

Honeywell claims that its Safety Manager (Honeywell, 2008) is a robust, safe, high availability controller for Safety Instrumented Systems (SIS) applications that delivers enhanced safety assurance for industrial plant operators. Honeywell employs a layered approach to safety and security. Every Safety Manager includes an embedded and certified safety firewall; this firewall isolates the safety application during runtime execution from external devices. Separate databases store the safety and control strategies, and separate software modules are available through dedicated tools such as Safety Builder and Control Builder; maintaining separate tools with separate databases prevents unauthorized changes or corruptions, decreases safety risks and prevents common cause failures. All Safety Builder modules are protected from viruses and harmful hacking by a built-in protection mechanism that checks the integrity of the software before installation, after installation and during run time. Using dedicated and specifically developed hardware and software, according the IEC61508 safety standard, reduces the risk of a common cause failure.

The Health, Safety, Environment and Quality Assessment Procedure (HSEQ AP, 2012) is an assessment method which was developed by five Northern Finnish process industry principal companies, the University of Oulu, Excellence Finland and POHTO (The Institute for Management and Technological Training). It focuses on industrial companies, branch offices and local organizations and their units, as defined by local principal companies. The HSEQ AP is open to all the above-mentioned supplying companies or to the ones who wants to be assessed. HSEQ covers health, safety, environment and quality standards (namely ISO/IEC) and selected key areas are covered in the supporting assessment tool. The national competition legislation is taken into account in the HSEQ AP. The criteria and principles of the HSEQ AP have been agreed between the principal companies. HSEQ AP is managed by the HSEQ assessment management group. The HSEQ assessment management group (HSEQ cluster) consists of representatives of the Inspecta, principal companies, POHTO and the University of Oulu. The HSEQ cluster acts as an organizer of the assessments, the supervisor of the HSEQ AP and leader of the development of HSEQ AP. The major assessors are always Inspecta's assessors and assessors are appointed by the principal companies and who have been trained in HSEQ AP. The register is maintained by an impartial administrator (currently POHTO). The principal companies decide how they use the results of assessments. There is a foreseen need to develop this tool further and this could be a topic of an ITEA3 research project.

4.1.1.2 Commercial Real Time embedded Operating Systems (RTOS) for safety and security

There are multiple companies selling Real Time embedded Operating Systems (RTOS) and / or hypervisors for safety and security. The main ones are: (Green Hills Software, 2014), (Lynx Software Technologies, 2015), (QNX, 2015), (Sysgo, 2014) and (Wind River, 2015).

4.1.2 Insight on security management in a safety-first industry: Nuclear Energy domain at STUK

In Finland there are four nuclear power plant units, two in Loviisa and two in Olkiluoto. The fifth power plant unit that is under construction in Olkiluoto, two new nuclear power plant projects and the Otaniemi research reactor of the Technical Research Centre of Finland in Espoo are also under the regulation of the Radiation and Nuclear Safety Authority (STUK). The main objective of the regulation of power plants is to ensure that the reactor is under control in all conditions. According to Section 7 of the Nuclear Energy Act (990/1987), STUK shall specify detailed safety requirements (a.k.a. YVL Guides) for the implementation of the safety level in accordance with the Nuclear Energy Act. Individual YVL Guides have been continuously updated, but a major overhaul was needed to improve the usefulness of the Guides and to amend the technical requirements, among other things.

The YVL Guides cover all matters and functions that have a bearing on the safety of nuclear facilities: design, operation, environmental safety, nuclear material and waste, structures and equipment. The licensees, who are responsible for the safety of the respective nuclear facilities, will have 44 new Guides to adhere to. Four of these will not come into effect until later. In the meantime, the old regulations remain in force.

The new Finnish safety requirements, which are up-to-date and strict from an international standpoint, ensure a high level of safety. It has taken approximately 50 man-years of work to update these guides, only in STUK. In the project, the relevant laws, government decrees and YVL Guides have been revised. For the laws, the revision process started in 2006 and for the YVL Guides, in 2008.

The main objectives of the YVL Guide revision project were to simplify the structure of the collection of nuclear safety rules, harmonise the Guides and apply the lessons of the Olkiluoto 3 project. In addition, the lessons learnt from the Fukushima accident as well as the objectives set for new facilities by the Western European Nuclear Regulators Association (WENRA) were taken into account in the project.

One of the lessons of the Fukushima accident is that nuclear facilities will be required to withstand more severe natural phenomena and power failures. The new Guides also emphasise that the applicant's plans have to be at an advanced stage and of high enough quality when the construction licence for the nuclear facility is being applied. This change has been brought about primarily by lessons learnt from the Olkiluoto 3 construction project. The new Guides also describe more closely than before how STUK is to oversee the safety of the nuclear facilities during the different stages of design, construction and operation.

In all of the guides there is a mention of the applicability of the guides in the following fashion. When considering how the new safety (and security) requirements presented in the YVL Guides shall be applied to the operating nuclear facilities, or to those under construction, STUK will take due account of the principles laid down in Section 7a of the (Finnish) Nuclear Energy Act (990/1987): *The safety of nuclear energy use shall be maintained at as high a level as practically possible. For the further development of safety, measures shall be implemented that can be considered justified considering operating experience, safety research and advances in science and technology.*

Special attention is paid to the requirement that, even in the case of a failure, the safety systems of a nuclear facility shall not interfere with each other. Furthermore, requirements on management systems have been revised (these are interlinked with IAEA guides and ISO/IEC 9001), and a new guide on Information Security Management of a Nuclear Facility (YVL A.12, 2013) has been issued. (YVL A.12, 2013) is meant to be used along with (YVL A.11, 2013) Security of a Nuclear Facility, which sets requirements for physical security arrangements.

Within MERgE, these two of the new YVL guides will be considered from the safety and security viewpoints.

These guides have utilized different standards and frameworks when developing requirements. As an example, YVL A.12 has been developed using ISO/IEC-27k series⁶⁰, IEC 62443 series⁶¹, National VAHTI guidance⁶², Control Objectives for Information and related Technology (COBIT), KATAKRI II National Security Auditing Criteria, and NIST-800 series alongside with International Atomic Energy Agency (IAEA) NSS-17⁶³. NSS-17 has, in turn, been developed by using some of the aforementioned standards and frameworks.

As an example, the STUK Regulatory Guide YVL B.1 has the following requirements on industrial control systems (I&C):

- Security countermeasures **shall** be planned based on risk assessments,
- Unauthorised access to the software of I&C systems and computers **shall** be prevented through adequate physical, technical and administrative security arrangements.
- The installation of unauthorised components including software **shall** be reliably prevented.
- Any modifications made to the software **shall** be detectable and traceable.

⁶⁰ In particular (ISO/IEC 27000, 2014), (ISO/IEC 27001, 2013), (ISO/IEC 27002, 2013) and (ISO/IEC 27005, 2011).

⁶¹ See (IEC/TS 62443-1-1, 2009), (IEC 62443-2-1, 2010), (IEC/TR 62443-3-1, 2009), and (IEC 62443-3-3, 2013).

⁶² Implementing guides/requirements on information security set by Finnish government.

⁶³ Computer Security at Nuclear Facilities.

- The interface of the I&C architecture to administrative computer systems **shall** be implemented by making the transmission of data unidirectional in such a way that any transmission of data towards the I&C architecture is prevented through separation at the physical level.

These requirements were laid from the safety viewpoint. In YVL B.1 is a reference to the A.12 which is a new guide specific to information security. A.12 in turn lays more specific requirements for the operator and the designers of automation systems. Regarding the networked systems⁶⁴ more detailed information security requirements are set:

- The related cabling and communications **shall** be protected against unlawful actions.
- The physical and logical separation of the networks and the monitoring of the communication taking place in the networks **shall** be implemented as well as is practically achievable, while taking the security significance of the networks into consideration.
- The dependencies between systems and their subcomponents **shall** be identified, their effect on information security **shall** be analysed and assessed, and any harmful dependencies **shall** be removed.
- For networked systems, the interfaces and connections between different systems, the protocols used, and the communicating parties **shall** be described in a comprehensive and unambiguous manner.

The overall approach for I&C supervision is depicted in Figure 135.

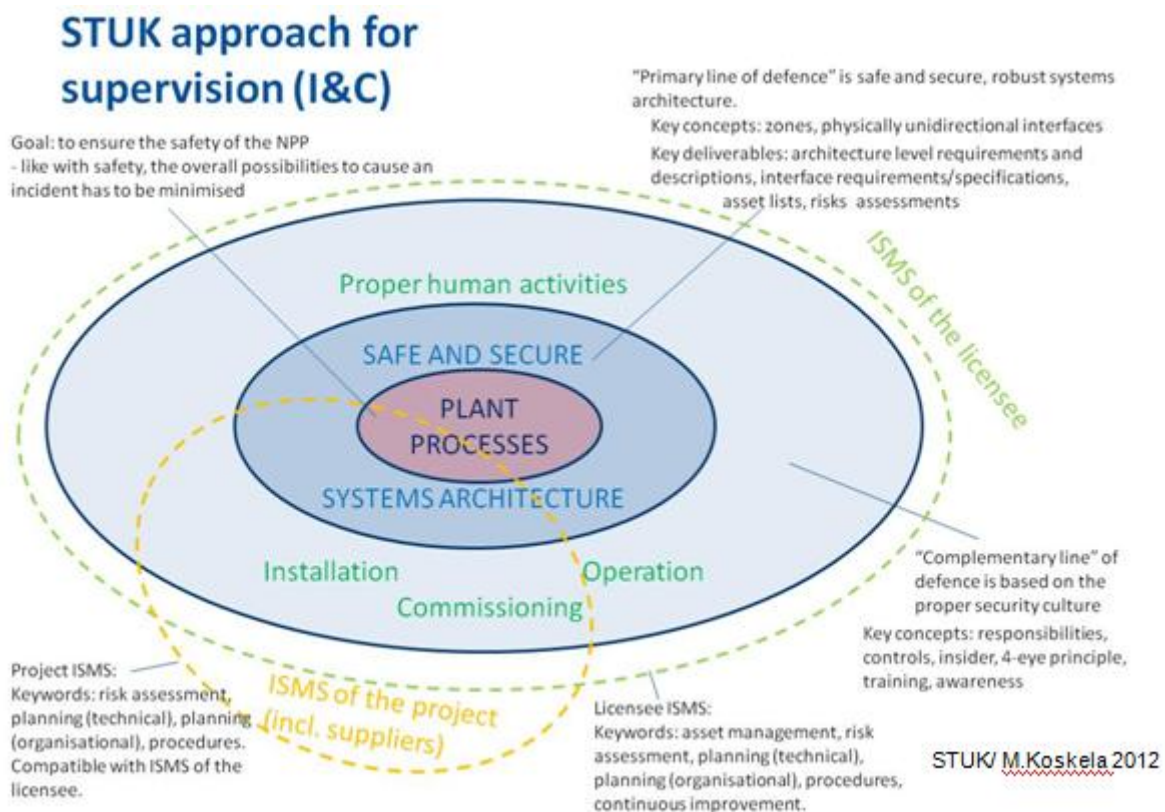


Figure 135: Model for overall I&C supervision in Finland

STUK is now in process of creating a repository where all requirements are stored. This repository can be used by the operator in order to identify relevant requirements on certain life cycle state, or requirements set for a certain system.

⁶⁴ Networked equipment means all devices that are connected to other devices by means of a network or of a cable that can be used for communication.

4.1.3 Insight on computing safety and security co-engineering at Thales

At Thales, there are processes for safety engineering and processes for security engineering, but the “Safe and Secure Computing Platform⁶⁵ Engineering Process” is not yet formalised and therefore not yet integrated in the Thales CHORUS Reference System. However, best practices are shared between computing experts.

The following gives an insight on some existing security engineering and safety engineering processes, and then provides a high-level overview of the process currently being applied for the design of new safe and secure computing platforms within the Thales Business Units.

The Thales *Evaluate the Common Criteria* process (Chorus 2.0 ECC, 2011) is adapted to meet the requirements of the Common Criteria. For each proof expected by the (ISO/IEC 15408-1, 2009) standard, a corresponding answer is proposed based on the software development process from the Thales Reference System, a.k.a. Chorus 2.0. Thales security experts typically perform a security analysis and define a Protection Profile (PP) for the Target of Evaluation (TOE). The PP describes the security problem, the assets to be protected, the threats taken into account, the security hypotheses regarding the TOE environment and identifies means to protect the system from these threats, e.g. with organisational security policies. The PP defines the security requirements to be satisfied during the software development to guarantee the targeted security level.

Security requirements are identified to guarantee: (i) the integrity of user data, platform firmware and applications; (ii) the authentication of users and applications; and (iii) the confidentiality of user data and communications between applications at different security levels. Thales products and systems mainly target EAL3+ and EAL4+ assurance levels, even if a certification is not always required. The “+” sign indicates that more assurance requirements are needed in addition to the minimum requirements designated by the assurance level. EAL3+ is EAL3 plus “systematic flaw remediation” (ALC_FLR.3) and “focused vulnerability analysis” (AVA_VAN.3). EAL4+ includes “Complete mapping of the implementation representation of the TSF” (ADV_IMP.2), “Sufficiency of security measures” (ALC_DVS.2), “systematic flaw remediation” (ALC_FLR.3) and “Advanced methodical vulnerability analysis” (AVA_VAN.5). Some assurance proofs are Not Applicable (NA).

New in 2016, the Chorus 2.0 security instruction is being completed with 3 security guides aimed specifically at security engineering (Feyt, et al., 2016), security risk assessment (Jacquet, et al., 2016), and architecting a secure system (Ksinant, et al., 2016).

The Thales *Design, Develop and Qualify the Solution* process (Chorus 2.0 DDQS, 2013) is adapted with guidance to write specification documents (Chorus 2.0 SSDV, 2011) as expected by the (RTCA DO-178B, 1992) / (EUROCAE ED-12B, 1992) standard and to apply the DDQS process to obtain the software certification. Traceability is established between DO-178 objectives and the rules defined by the Thales Software Specification, Design and Verification processes. In the specification and design process, the requirements phase defines High-Level Requirements (HLRs) from the input technical requirements. During the preliminary design process, a real-time and functional architecture is defined to indicate the partitions, scheduling, data and control flows between components. The HLRs are then allocated to architecture partitions. In the detailed design process, non-implementable HLRs are refined into implementable Low-Level Requirements (LLRs). The implementable HLRs and LLRs are allocated to software components, while all LLRs are allocated to architecture partitions. Finally, the components of the functional architecture are mapped to the partitions of the real-time architecture. In the verification process, activities are realized to detect errors by reviews, analyses and tests. The verification process is performed by the analysis of requirement-based coverage and/or structural coverage.

The design of safe and secure computing platforms results from several trade-offs between functional and non-functional requirements. In order to make these trade-offs, the Safe and Secure Computing Platform Engineering Process follows two stages:

- top-down requirements analysis and platform design, and
- bottom-up performance evaluation.

The top-down stage allows for:

- the specification of requirements;
- the allocation of requirements to different sub-systems and metiers (a.k.a. software and hardware);
- the identification of potential dependencies, i.e. connections, contradictions...;
- the elaboration of a traceability matrix;
- the building of Decision, Analysis and Resolution (DAR) reports;
- based on the DAR reports, the selection of components compatible with the relevant safety or/and security standards; the components may be in-house building blocks, COTS or new developments.

⁶⁵ The term “Computing Platform” encompasses the hardware and the software architectures that operate applications. As an embodiment of a Computing Platform, the hardware maybe a General Purpose Processor (GPP), and the software, an Operating System (OS). Both hardware and software contribute to the satisfaction of the required safety and security requirements.

The top-down engineering activities are tooled-up to deal with the complexity of textual⁶⁶ specifications, particularly in terms of requirements completeness assurance and change-management: DOORS, REQTIFY or Ms. Word / Excel macros.

The bottom-up stage makes an inventory of all technical options, and feeds the DAR reports with figures coming from in-house and / or well-known hardware benchmarks, algorithm prototyping, security and / or safety requirements compliance assessment, and other field activities, e.g. projects feedbacks or best practices.

⁶⁶ Specifications are mainly textual today but the trend is towards model-based ones.

5 A state of the art in safety and security co-engineering in education

A state of the art in safety and security co-engineering research has been covered in §2. This section examines academic initiatives, in particular in terms of education courses.

According to (Weiss, 2010), the general lack of security for industrial control systems (ICS) is due to a hole in academia, since security is taught in computer science departments, whereas control systems are taught in various engineering departments. According to (Axelrod, 2013b), subsequent job and research opportunities intensify this gap.

In France, the CLUSIF has a portal to French cyber-security master courses (CLUSIF). None of the seven referenced cyber-security master course addresses safety engineering.

However, some interdisciplinary education programmes for engineers in the fields of security and safety do exist, as shown below.

The Homeland Security and Emergency Management programme at San Diego's National University (Viswanathan) is designed in such a way that anyone successfully completing this programme would be academically trained to apply for Certified Protection Professional (CPP), Certified Safety Professional (CSP), and / or Certified Emergency Manager (CEM) credentialing.

The Security & Safety Engineering programme at Furtwangen University in Germany (Furtwangen University) addresses technology, management and psychology. In this Bachelor of Science, taught in German and English, the security aspect deals with specific attacks, including industrial espionage, product piracy, damage to production plants or processes through intentional interventions and IT-based crime. The safety aspect focuses in particular on occupational health and safety, ergonomics, fire prevention, hazardous materials, defence against dangers, management of crises and catastrophic events.

6 Other safety and security co-engineering focal points

This section lists journals, conferences, workshops, forums, etc. that explicitly relate to safety and security co-engineering. This section does not claim to be comprehensive.



IET System Safety and Cyber Security Conference (SSCS): In 2016, SSCS will be in its 11th edition. SSCS claims to be the largest conference for system safety specialists held in the UK, and the only conference where both safety and security engineers from around the world can meet and share ideas, new research and network. Until its 6th edition, the conference was called “International System Safety Conference”. For 2 years, starting from the 7th edition, in 2012, the System Safety conference incorporated the IET Cyber Security conference (under the name “System Safety Conference Incorporating the Cyber Security Conference”), giving participants the opportunity to network with and showcase their latest work among both disciplines. From the 9th edition, the conference’s name reached its current dual speciality title.



European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS): The mission of EWICS is to promote the economical and efficient realisation of programmable industrial systems through education, information exchange, and the elaboration of standards and guidelines. EWICS is active in the field of Programmable Electronic Systems reliability, safety and security. It has members from most European countries, covering various fields

of interests and affiliations, as well as from the USA. To achieve the above goals EWICS: (i) assesses the state of the art in methods and tools for critical software development and maintenance in industrial environments; (ii) develops standards and guidelines for the development and assessment of safe and secure systems; (iii) disseminates information and knowledge in this field; and (iv) exchanges technical knowledge between its members.

Within EWICS, work is organised in subgroups. One of the subgroups relates to the Security of Safety-Critical Computer Systems (SEC). The objective of this subgroup is to provide guidance: (a) to purchasers and groups responsible for secure operation on what to specify with regard to security and how to undertake the specification process; (b) to suppliers on how to satisfy the security requirements, while maintaining project security during the project lifecycle; and (c) to users on how to manage and maintain security in their industrial safety critical computer systems. However, this sub-group does not seem very active.

EWICS TC7 organises SafeComp, the Annual International Conference on Computer Safety, Reliability and Security Conference.

Ref: <http://www.ewics.org/docs/system-security-subgroup>



International Journal of Safety and Security Engineering: This journal provides a forum for publication of papers on the most recent developments in the theoretical and practical aspects of Safety and Security Engineering. It covers areas such as crisis management; security engineering; natural disasters and emergencies; terrorism; IT security; man-made hazards; risk management; control; protection and mitigation issues. The 1st volume, with 4 issues, was published in 2011 by WITpress. The International Journal of Safety and Security Engineering is associated with the SafeComp conference.

International Conference on Computer Safety, Reliability & Security (SafeComp): This conference was established in 1979 by the European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS), Technical Committee 7 (TC7). SafeComp is an annual event covering the state-of-the-art, experience and new trends in the areas of safety, security and reliability of critical computer applications. This conference achieved its 32nd edition in 2013.

International Conference on Safety and Security Engineering (SAFE): The purpose of the SAFE conference is to provide a forum for the presentation and discussion of the most recent academic and industrial developments in theoretical and practical aspects of safety and security engineering. The conference does not specifically address the issue of co-engineering, but this topic is occasionally addressed, as with (Axelrod, 2013a). This conference, organised by the Wessex Institute (UK), has currently achieved its 5th edition. The successive

conferences were held in Rome in 2005, Malta in 2007, Rome in 2009, Antwerp in 2011, and Rome again in Sept. 2013. The sixth meeting is planned for the 6 - 8 May, 2015, in Opatija, Croatia.

The Relationship between Safety and Security in Software-Based Systems: This workshop was held on September 25th, 2008, in Newcastle, in conjunction with the SafeComp conference, by the Safety-Critical Systems Club (SCSC) and the European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS).

Human Factors in the Safety and Security of Critical Systems: This workshop was held on March 18th, 2013, at the School of Computing Science, University of Glasgow, Scotland. It provided a common forum for researchers working on the human factors of safety and security critical systems, including usability studies; application of human factors studies from safety-critical to secure systems (and vice versa); interactions between safety, security, dependability and the usability of complex systems; common organisational issues in safety and security critical systems; studies of resilience across both safety and security critical systems; and tools and techniques for the co-design of safety and security critical interfaces.

Security-Awareness for Safety Engineers (SA4SE): This tutorial, chaired by Robert Stroud, was held on September 2013, in Toulouse, in conjunction with the SafeComp conference. Its aim was to raise awareness of cyber-security issues and concerns so as to help safety engineers to: (i) understand the risks that security threats pose to safety systems; (ii) appreciate whether safety systems are adequately secure as well as adequately safe; (iii) know when to seek specialised advice.

Practical Software and Systems Measurement (PSM⁶⁷) **Safety & Security Technical Working Group (TWG):** This TWG was run during Feb-March 2004, and produced two white-papers called *Safety Measurement* and *Security Measurement*. These white-papers were updated in 2006.

Integration of Safety and Security Engineering (ISSE): This workshop was 1st co-organised by the MERgE and SeSaMo projects as a satellite workshop of the SAFECOMP conference in Florence, on Sept. 8th, 2014. A 2nd edition was held in Delft on Sept. 22nd, 2015. Its purpose was to share ideas, experiences and solutions to concretely combine or integrate safety and security engineering activities.

Safety & Security in Cyber-Physical Systems: This workshop was organised by Fraunhofer IESE, in Kaiserslautern, on Sept. 15th, 2014. It focused on: (i) how to reuse security assurance artefacts for safety assurance, and vice versa; (ii) the crucial differences between security and safety; (iii) how to account for these differences in risk assessment and quality assurance strategies; how safety & security interact with each other in cyber-physical systems. The workshop was concluded by a comprehensive debriefing (Schwarz, et al., 2014) addressing:

- exploitable similarities: regarding safety/security properties, both relate to freedom from unreasonable risk; regarding safety/security assurance methods, both encourage multiple layers of defence; regarding safety/security assurance artefacts and metrics, both rely on separation kernels;
- critical differences: regarding safety/security properties, it is possible to oppose systematic / random faults vs. malicious faults, usage-domain constraints vs. new (mis)uses, fault probabilities vs. attacker motivation / capabilities; regarding safety/security assurance methods, it is possible to oppose “no dead code” vs. security trap, “never change a proven system” vs. security patching, safety certification vs. runtime cyber-security supervision;
- integration pros and cons: the integration optimists put forward the similarities of assurance activities, the reuse of existing assurance artefacts, the avoidance of effort duplication, the pressing need to cope with future cyber-physical systems; the integration pessimists put forward the plethora of safety and security standards involved and their recent tendency for a separation of concerns, the semantic gaps, subtle differences in assumptions, practices, and terminology, the impact on certification paradigms, the large and disjoint communities;
- scalability: typical issues relate to incremental design (i.e. safety and security invariance under composition, refinement or modularisation), impact of exceptional scenarios (e.g. security certificate revocation) in very large systems, use of components-off-the-shelf (COTS), efficiency of separation kernels in separating criticality aspects from functionality considerations (on the engineering plane) and containing faults (on the runtime impact plane);


⁶⁷ PSM served as the base document for the development of ISO/IEC 15939, Software Engineering - Software Measurement Process.


6th ISO 26262 International Annual Conference: This conference, held in Stuttgart between Sept. 29th and Oct. 1st, dedicated one afternoon to safety and security, addressing three main topics: (i) cyber-security guide-book for cyber-physical vehicle systems overview; (ii) an approach to safety and security analysis for automotive systems; and (iii) challenges in the joint integration of automotive safety and security.

Technical Meeting (TM) on Safety, Security and Safeguards: Interfaces and Synergies for the Development of a Nuclear Power Programme: This technical meeting, held at the IAEA Headquarters in Vienna, from 26 to 29 November 2012, was attended by 40 participants from 24 Member States (MS), the European Commission and the World Institute for Nuclear Security (WINS). Most participants expressed interest in identifying the interfaces and synergies between the three areas of nuclear safety, security and safeguards in order to identify good practices for improved regulations and operations of nuclear power plants (NPP). Several good practices were identified during the meeting such as: implementation of an Integrated Management System (IMS) as an effective tool for operationalizing core processes in organizations; Human Resource Development (HRD), career management, and common training across disciplines for safety, security, and safeguards; and ensuring that there is inter-organizational coordination during an emergency for an effective response and to provide correct and timely information to the public. Most of the participants agreed that it would be useful to develop a series of case studies and good practices on this topic and to share these with MS.

Ref: <https://www.iaea.org/NuclearPower/Meetings/2012/2012-11-26-11-29-TM.html>

At the time of writing this report, the following conference and seminar are only scheduled, but really focused on the topic.

 **Safety meets Security – Challenges and solutions.** This conference is scheduled to be held on March 2nd, 2016 in Kaiserslautern, Germany. It aims at providing an overview of the current status of regulations and standardization, allowing to find out more about the challenges and requirements of the combination of Safety and Security issues, to learn more about best practices of different industries, and to discuss with international experts and peers.

 **ISA-France Safety and cyber-security: how to reconcile two essential objectives of industrial security** seminar, in partnership with INSA-Lyon. The seminar aims to analyse the problematic of the two approaches in order to understand what unites and what differentiates them. Academic works on the subject will be presented as well as the normative work currently underway, in particular within ISA (ISA99, ISA 84) and IEC. Use cases and return of experience from real situations where safety and cyber-security have to coexist will be presented, with ultimately the aim to highlight best practices for optimal management of industrial risks. The seminar is scheduled to be held in October 2016 in Villeurbanne, France.

7 References

- 14 CFR** Title 14 - Aeronautics and Space [Online] // Electronic Code of Federal Regulations. - U.S. Government Printing Office (GPO), 25 09 2014. - 28 09 2014. - http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title14/14tab_02.tpl.
- 21 CFR 820** Title 21—Food and Drugs - Chapter I—Food and Drug Administration, Department of Health and Human Services, Subchapter H—Medical Devices, Part 820 - Quality System Regulation [Online] // Electronic Code of Federal Regulations. - U.S. Government Printing Office (GPO), 03 10 2014. - 06 10 2014. - http://www.ecfr.gov/cgi-bin/text-idx?SID=5c083a95bf6abac27db221f085f6f315&tpl=/ecfrbrowse/Title21/21cfr820_main_02.tpl;bcsi-ac-95bb4efa6a1646c8=23393A6F00000503uWtbz9kbY8DzCwcjFONdRtd73qZKAQAAAwUAAPXiEwAIBwAAAtwAAAO/fCQA=.
- 21 CFR 860** Title 21—Food and Drugs - Chapter I—Food and Drug Administration, Department of Health and Human Services, Subchapter H—Medical Devices, Part 860—Medical Device Classification Procedures [Online] // Electronic Code of Federal Regulations. - U.S. Government Printing Office (GPO), 03 10 2014. - 06 10 2014. - http://www.ecfr.gov/cgi-bin/text-idx?SID=5c083a95bf6abac27db221f085f6f315&tpl=/ecfrbrowse/Title21/21cfr860_main_02.tpl;bcsi-ac-b5f45ffb1099c547=234B714800000503+IDInhgSwuubFwJrver8BZm6fssSAAAAAwUAAPM/EwAIBwAABwAAA L6MAAA=.
- 25-356-SC** Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Isolation or Protection From Unauthorized Passenger Domain Systems Access [Online] // Federal Register. - Federal Aviation Administration, 01 02 2008. - 12 11 2014. - <https://federalregister.gov/a/E7-25467>. - 73 FR 27.
- 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 [Online] // Federal Register. - Federal Aviation Administration, 28 12 2007. - 10 10 2014. - <https://federalregister.gov/a/E7-25075>. - E7-25075.
- 49 CFR XII-C** Title 49 - Transportation, Chapter XII, Sub-chapter C, Civil Aviation Security [Online] // Electronic Code of Federal Regulations. - U.S. Government Printing Office (GPO), 30 10 2014. - 04 11 2014. - http://www.ecfr.gov/cgi-bin/text-idx?SID=31ff4b515b8904f5fe381a11f3d33562&tpl=/ecfrbrowse/Title49/49cfrv9_02.tpl#1500.
- 79 FR 60574** Request for Comment on Automotive Request for Comment on Automotive Security [Book Section] // Federal Register Volume 79, Issue 194 (October 7, 2014). - [s.l.] : Office of the Federal Register, National Archives and Records Administration, 2014. - 194 : Vol. 79. - FR Doc. 2014–23805.
- Abousahl Said [et al.]** Scientific and Technical Challenges to the effective implementation of the 3S - Safety, Security and Safeguards – approach with some practical experiences [Book Section] // International Cooperation for Enhancing Nuclear Safety, Security, Safeguards and Non-proliferation / ed. Maiani Luciano, Abousahl Said and Plastino Wolfango. - Rome : Springer International Publishing, 2015. - Vol. 172. - 10.1007/978-3-319-24322-1_6.
- Åkerberg Johan** On Safe and Secure Communication in Process Automation [Report] : PhD. Thesis / School of Innovation, Design and Engineering. - Västerås (Sweden) : Mälardalen University Press Dissertations, 2011. - p. 57. - ISBN: 978-91-7485-039-0.
- Altran Praxis** SafSec Methodology, Issue 3.1 [Report] : Standard. - 2006. - S.P1199.50.2.
- Alves-Foss Jim, Rinker Bob and Taylor Carol** Towards Common Criteria Certification for DO-178B Compliant Airborne Software Systems, Comparing Evaluation Assurance Level 5 (EAL5) to DO178 [Online] // University of Idaho, Department of Computer Science, Jim Alves-Foss, Recent Publications and Presentations. - Center for Secure and Dependable Systems, 01 2002. - Draft. - 10 07 2014. - <http://www2.cs.uidaho.edu/~jimaf/papers/compare02b.pdf>. - Not releasable to the Defense Technical Information Center per DOD directive 3200.12..
- Aoyama T. [et al.]** A unified framework for safety and security assessment in critical infrastructures [Book Section] // Safety and security engineering V / ed. Garzia F., Brebbia C. A. and Guarascio M.. - [s.l.] : WIT Press, 2013. - Vol. 134. - DOI: 10.2495/SAFE130071.
- Aprville Ludovic and de Saqui-Sannes Pierre** AVATAR: Un profil SysML temps réel outillé [Conference] // SysML France. - Paris : [s.n.], 2010a. - p. 28. - In French.
- Aprville Ludovic and Roudier Yves** Towards the Model-Driven Engineering of Secure yet Safe Embedded Systems [Conference] // Proceedings of 1st International Workshop on Graphical Models for Security

- (GraMSec) / ed. Kordy B., Mauw S. and Pieters W.. - Grenoble : Electronic Proceedings in Theoretical Computer Science, 2014. - Vol. 148. - pp. 15-30. - DOI: 10.4204/EPTCS.148.2.
- ARINC 653P0** Avionics Application Standard Software Interface, Part 0, Overview of ARINC 653 [Report] : Standard / Airlines Electronic Engineering Committee (AEEC). - Annapolis : Aeronautical Radio Incorporated (ARINC), 2013.
- ARINC 653P1-3** Avionics Application Software Standard Interface, Part 1, Required Services [Report] : Standard / Airlines Electronic Engineering Committee (AEEC). - Annapolis : Aeronautical Radio Incorporated (ARINC), 2010.
- ARINC 653P2-2** Avionics Application Software Standard Interface, Part 2, Extended Services [Report] : Standard / Airlines Electronic Engineering Committee (AEEC). - Annapolis : Aeronautical Radio Incorporated (ARINC), 2012.
- ARINC 653P3A** Avionics Application Software Standard Interface, Part 3A, Conformity Test Specification for ARINC 653 Required Services [Report] : Standard / Airlines Electronic Engineering Committee (AEEC). - Annapolis : Aeronautical Radio Incorporated (ARINC), 2014.
- ARINC 653P4** Avionics Application Software Standard Interface, Part 4, Subset Services [Report] : Standard / Airlines Electronic Engineering Committee (AEEC). - Annapolis : Aeronautical Radio Incorporated (ARINC), 2012.
- ARINC 811** Commercial Aircraft Information Security Concepts of Operation and Process [Report] : Standard / Airlines Electronic Engineering Committee (AEEC). - Annapolis : Aeronautical Radio Incorporated (ARINC), 2005.
- ARTEMIS EMC2** [Online] // Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments. - 2014. - 30 09 2014. - <http://www.artemis-emc2.eu/>.
- AS/NZS 4360** Risk Management [Report] : Standard / Joint Technical Committee OB/7 – Risk Management. - [s.l.] : Standards Australia, 1999. - Superseded by AS/NZS 4360:2004. - ISBN: 0 7337 2647 X.
- AVATAR** Automated Verification of reAl Time softwARe (AVATAR) [Online] // TTOOL. - Institut Télécom, Télécom Paris Tech, 2015. - 26 02 2015. - <http://ttool.telecom-paristech.fr/avatar.html>.
- Aven Terje** A unified framework for risk and vulnerability analysis covering both safety and security [Book Section] // Proceedings of Reliability Engineering & System Safety. - 2007.
- Aven Terje** A unified framework for risk and vulnerability analysis covering both safety and security [Book Section]. - [s.l.] : IEEE, 2011. - 4th : Vol. 39. - DOI: 10.1109/EMR.2011.6093894.
- Aven Terje** Identification of safety and security critical systems and activities [Book Section] // Reliability Engineering & System Safety. - 2009. - DOI: 10.1016/j.ress.2008.04.001.
- Avizienis Algirdas [et al.]** Basic concepts and taxonomy of dependable and secure computing [Book Section] // IEEE Trans. Dependable Secur. Comput.. - 2004.
- Axelrod C. Warren** Applying Lessons from Safety-Critical Systems to Security-Critical Software [Conference] // IEEE Systems, Applications and Technology Conference (LISAT). - Farmingdale, NY, USA : [s.n.], 2011. - DOI: 10.1109/LISAT.2011.5784222.
- Axelrod C. Warren** Bridging the safety-security software gap [Book Section] // Safety and Security Engineering V / ed. Garzia F., Brebbia C. A. and Guarascio M.. - Rome : WITpress, 2013a. - Vol. 134. - ISBN: 978-1-84564-744-5.
- Axelrod C. Warren** Engineering Safe and Secure Software Systems [Book]. - [s.l.] : Artech House Publishers, 2012. - ISBN: 978-1-60807-473-0.
- Axelrod C. Warren** Managing the risks of cyber-physical systems [Book Section] // IEEE Systems, Applications and Technology Conference (LISAT). - Farmingdale : IEEE, 2013c. - DOI: 10.1109/LISAT.2013.6578215.
- Axelrod C. Warren** Securing Cyber-Physical Software [Online] // APPSEC USA. - 18-21 Nov. 2013b. - 05 May 2014. - <http://2013.appsecusa.org/2013/wp-content/uploads/2013/12/APPSEC2013-Presentation-Final.ppt>.
- Babeshko E., Kharchenko V. and Gorbenko A.** Applying F(I)MEA-technique for SCADA-Based Industrial Control Systems Dependability Assessment and Ensuring [Conference] // Third International Conference on Dependability of Computer Systems (DepCos-RELCOMEX). - Szklarska Poreba : IEEE, 2008. - pp. 309 - 315. - DOI: 10.1109/DepCoS-RELCOMEX.2008.23.
- Banerjee Ayan [et al.]** Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber-Physical Systems [Journal] // Proceedings of the IEEE. - [s.l.] : IEEE, 2012. - 1 : Vol. 100. - pp. 283-299. - 10.1109/JPROC.2011.2165689.
- Bezzateev Sergey, Voloshina Natalia and Sankin Petr** Joint Safety and Security Analysis for Complex Systems [Conference] // 13th Conference of Open Innovations Association FRUCT. - Petrozavodsk, Russia : [s.n.], 2013.

- Bieber Pierre [et al.]** Security and Safety Assurance for Aerospace Embedded Systems [Book Section] // Embedded Real-Time Software and Systems (ERTS). - Toulouse : [s.n.], 2012.
- Bieber Pierre and Brunel Julien** From Safety Models to Security Models: Preliminary Lessons Learnt [Conference] // 1st International Workshop on the Integration of Safety and Security Engineering (ISSE), 33rd International Conference on Computer Safety, Reliability and Security (SafeComp) / ed. Bondavalli Andrea, Ceccarelli Andrea and Ortmeier Frank. - Florence : Springer, 2014. - pp. 269-281. - LNCS 8696. - DOI: 10.1007/978-3-319-10557-4.
- Blanquart Jean-Paul [et al.]** Similarities and dissimilarities between safety levels and security levels [Online] // ERTS'2012. - 03 02 2012. - 16 05 2014. - <http://www.erts2012.org/Default.aspx?Id=1050&Idd=1129>. - 8A.2.
- Blasum Holger** Partitioning in Safety and Security: Mapping to MILS Core Partitioning Mechanisms [Conference] // International Workshop on MILS: Architecture and Assurance for Secure Systems. - Amsterdam : [s.n.], 2015.
- Bloomfield Richard [et al.]** How secure is ERTMS? [Conference] // Workshop on Dependable and Secure Computing for Large-scale Complex Critical Infrastructures (DESEC4LCCI) / ed. Ortmeier Frank and Daniel Peter. - Herrenkrug : Springer, 2012. - Vol. 7613. - pp. 247-258. - <http://openaccess.city.ac.uk/1522/1/How%20secure%20is%20ERTMS.pdf>. - DOI: 10.1007/978-3-642-33675-1_22.
- Bock Hans-Hermann [et al.]** Towards an IT Security Protection Profile for Safety-Related Communication in Railway Automation [Conference] // 31st International Conference on Computer Safety, Reliability and Security (SafeComp) / ed. Ortmeier Frank and Daniel Peter. - Magdeburg : Springer Berlin Heidelberg, 2012. - Vol. 7612. - pp. 137-148. - DOI: 10.1007/978-3-642-33678-2_12.
- Boeing Cybersecurity Framework** Developing a Framework to Improve Critical Infrastructure Cybersecurity [Report] : RFI Response. - [s.l.] : Boeing, 2013. - p. 113.
- Boettcher Carolyn [et al.]** The MILS Component Integration Approach to Secure Information Sharing [Conference] // Proceedings of the 27th IEEE/AIAA Digital Avionics Systems Conference (DASC). - St. Paul, MN : IEEE, 2008. - DOI: 10.1109/DASC.2008.4702758.
- Braband Jens** IT security for functional safety in railway automation [Conference] // 1st Workshop on Safety and Security. - Kaiserslautern : [s.n.], 2014b. - Slides only.
- Braband Jens** Safety and Security Requirements for an Advanced Train Control System [Conference] // 16th International Conference on Computer Safety, Reliability and Security (SafeComp) / ed. Daniel Peter. - [s.l.] : Springer London, 1997. - pp. 111-122. - DOI: 10.1007/978-1-4471-0997-6_9.
- Braband Jens** Towards an IT security protection profile for safety-related communication in railway automation [Conference] // Embedded Real-Time Software and Systems (ERTS2). - Toulouse : [s.n.], 2014a.
- Braband Jens** What's Security Level got to do with Safety Integrity Level? [Conference] // 8th European Congress on Embedded Real Time Software and Systems (ERTS). - Toulouse, France : [s.n.], 2016. - To be published..
- Braber F. den [et al.]** Model-based risk assessment in a component-based software engineering process: the CORAS approach to identify security risks [Book Section] // Business Component-Based Software Engineering / book auth. Barbier Franck. - 2003.
- Brewer David F. C.** Applying Security Techniques to Achieving Safety [Book Section] // Directions in Safety-Critical Systems, Proceedings of the First Safety-critical Systems Symposium, Bristol 9–11 February 1993 / book auth. Redmill Felix and Anderson Tom. - London : Springer, 1993. - DOI: 10.1007/978-1-4471-2037-7_16.
- Brewer David F. C.** Ten Years On: Doesn't the World of Security have anything to offer the World of Safety? [Book Section] // Lessons in System Safety, Proceedings of the Eighth Safety-Critical Systems Symposium. - Southampton : Springer Verlag, 2000. - ISBN: 9781852332495 | 1852332492.
- Brooke Phillip J. and Paige Richard F.** Fault trees for security system design and analysis [Journal] // Computers & Security. - 2003. - 3 : Vol. 22. - pp. 256-264. - DOI: 10.1016/S0167-4048(03)00313-4.
- Brostoff Sacha and Sasse M. Angela** Safe and sound: a safety-critical approach to security [Book Section] // NSPW'01 Proceedings of the 2001 workshop on new security paradigms / ed. ACM. - New York : [s.n.], 2001. - DOI: 10.1145/508171.508178.
- Brunel Julien [et al.]** A Viewpoint-Based Approach for Formal Safety & Security Assessment of System Architectures [Conference] // 11th Workshop on Model Driven Engineering, Verification and Validation (MoDeV'Va) / ed. Boulanger Frédéric, Famelis Michalis and Ratiu Daniel. - Valencia : [s.n.], 2014b. - pp. 39-48.
- Brunel Julien [et al.]** Formal Safety and Security Assessment of an Avionic Architecture with Alloy [Book Section] // 3rd International Workshop on Engineering Safety and Security Systems (ESSS). - Singapore : EPTCS, 2014a. - Vol. 150. - DOI: 10.4204/EPTCS.150.2.
- Brunel Julien and Chemouil David** Safety and Security Assessment of Behavioral Properties Using Alloy [Conference] // 2nd International workshop on the Integration of Safety and Security Engineering / ed.

Koornneef F. and Gulijk C. van. - Delft : Springer International Publishing Switzerland, 2015. - Vol. LNCS 9338. - pp. 251–263. - DOI: 10.1007/978-3-319-24249-1 22.

BS EN 61508-1 Functional safety of electrical/ electronic/ programmable electronic safety-related systems - General requirements [Book]. - [s.l.] : British Standards Institution (BSI), 2002. - p. 68. - Withdrawn - replaced by BS EN 61508-1:2010. - ISBN: 0 580 32719 1.

Burns A., McDermid J. and Dobson J. On the meaning of safety and security [Book Section] // The Computer Journal - Special issue on safety and security parallel. - Oxford : Oxford University Press, 1992. - 1st : Vol. 35. - DOI: 10.1093/comjnl/35.1.3.

Carter Adele-Louise Safety-Critical versus Security-Critical Software [Conference] // 5th IET International Conference on System Safety. - Manchester, United Kingdom : [s.n.], 2010. - DOI: 10.1049/cp.2010.0814.

CASA CAAP 232A Civil Aviation Advisory Publication [Online] // Administration of Aircraft & Related Ground Support Network Security Programs. - Civil Aviation Safety Authority, 02 2013. - 12 11 2014. - http://www.casa.gov.au/wcmswr/_assets/main/newrules/ops/download/draft-caap-232a-1.pdf.

Casals Silvia Gil, Owezarski Philippe and Descargues Gilles Risk Assessment for Airworthiness Security [Book Section] // Computer Safety, Reliability, and Security, Lecture Notes in Computer Science. - 2012. - Vol. 7612. - DOI: 10.1007/978-3-642-33678-2_3.

CENELEC EN 20159 Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems [Report] : Standard. - [s.l.] : European Committee for Electro-technical Standardization, 2010. - Supersedes EN 50159-1:2001 and EN 50159-2:2001..

CENELEC EN 50126-1 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) -- Part 1: Basic requirements and generic process [Report] : Standard. - Brussels : European Committee for Electro-technical Standardization, 2010. - p. 82. - EN 50126-1:1999. Corrigendum, July 2010..

CENELEC EN 50128 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems [Report] : Standard. - [s.l.] : European Committee for Electro-technical Standardization, 2014.

CENELEC EN 50128 Railway Applications: Software for Railway Control and Protection [Report] : Standard. - [s.l.] : European Committee for Electrotechnical Standardization, 1997.

CENELEC EN 50129 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling [Report] : Standard. - [s.l.] : European Committee for Electro-technical Standardization, 2010. - Revises CENELEC EN 50129:2003.

CENELEC EN 50129 Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling [Report] : Standard. - [s.l.] : European Committee for Standardization, 2003. - Superseded by CENELEC EN 50129:2010.

CENELEC EN 50155 Railway applications - Electronic equipment used on rolling stock [Report] : Standard. - [s.l.] : European Committee for Electro-technical Standardization, 2012.

CESAR D_SP1_R5.2_M1 Safety-Diagnosability requirements specification V1 [Report] : Technical Report. - [s.l.] : Cost-Efficient methods and processes for Safety Relevant embedded systems (CESAR) ARTEMIS project, 2009. - p. 69.

Chapon Nicolas and Piètre-Cambacédès Ludovic Towards system engineering integrating safety and security / Vers une ingénierie système intégrant sûreté et sécurité (in French) [Book Section] // Génie Logiciel. - 2012. - 100th.

Chen Binbin [et al.] Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective [Conference] // 2nd International Workshop on the Integration of Safety and Security Engineering / ed. Koornneef Floor and Gulijk Coen van. - Delft, The Netherlands : Springer, 2015. - Vol. LNCS 9338. - pp. 277–290. - DOI: 10.1007/978-3-319-24249-1 24.

Chevrel Cédric Avionics System (AVS) safety, trends & key R&T [Conference] // Journée de Palaiseau on Safety Engineering. - Palaiseau : Thales, 2014. - p. 21. - Thales Group Internal.

Chorus 2.0 DDQS Design, Develop and Qualify the Solution // Chorus 2.0 Thales Reference System. - [s.l.] : Thales Group, 2013. - Thales Group Internal. - 87202127-DDQ-GRP-EN-007-TCS-002.

Chorus 2.0 ECC Evaluer les Critères Communs // Chorus 2.0 Thales Reference System. - [s.l.] : Thales Group, 2011. - Thales Group Internal. - 83050954-DDQTCS-FR.

Chorus 2.0 SSDV Software Specification, Design and Verification Standard (DO178) // Chorus 2.0 Thales Reference System. - [s.l.] : Thales Group, 2011. - Thales Group Restricted. - 83090018-DDQ-TAV-EN.

Cimatti Alessandro [et al.] Combining MILS with Contract-Based Design for Safety and Security Requirements [Conference] // 2nd International workshop on the Integration of Safety and Security Engineering / ed. Koornneef F. and Gulijk C. van. - Delft : Springer International Publishing Switzerland, 2015. - Vol. LNCS 9338. - pp. 264–276. - DOI: 10.1007/978-3-319-24249-1 23.

- CLUSIF** Portail des Formations Universitaires SSI [Online] // Club de la Sécurité de l'Information Français (CLUSIF). - 28 11 2014. - <http://www.clusif.asso.fr/fr/production/formations/>. - In French.
- Cockram Trevor J. and Lautieri Samantha R.** Combining security and safety principles in practice [Conference] // 2nd Institution of Engineering and Technology International Conference on System Safety. - London : IET, 2007. - pp. 159 - 164. - ISBN: 978-0-86341-863-1.
- Contini S., Cojazzi G.G.M. and Renda G.** On the use of non-coherent fault trees in safety and security studies [Book Section] // Safety and Reliability for Managing Risk / book auth. Soares Guedes and Zio. - London : Taylor & Francis Group, 2006. - http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDkQFjAC&url=http%3A%2F%2Fwww.dimat.unina2.it%2Fmarrone%2Fdwld%2FProceedings%2FESREL%2F2006%2FPdf%2FS-341.pdf&ei=5QmUVOfGM8y9adyJgbgE&usq=AFQjCNHRv52Uh0W06G1Bbt_U-IG60lyScg&bvm=bv.8200133. - ISBN: 0-415-41620-5.
- Corneillie Pierre [et al.]** SQUALE Dependability Assessment Criteria [Report]. - [s.l.] : LAAS-CNRS, 1999. - 4th Edition. - ACTS95/AC097.
- Cusimano John and Byres Eric** Safety and Security: Two Sides of the Same Coin [Online]. - April 2010. - March 2014. - <http://www.controlglobal.com/articles/2010/safetysecurity1004>.
- Czerny Barbara J.** System Security and System Safety Engineering: Differences and Similarities and a System Security Engineering Process Based on the ISO 26262 Process Framework [Journal] // Journal of Passenger Cars – Electronic and Electrical Systems. - [s.l.] : SAE International, 2013. - 1 : Vol. 6. - DOI: 10.4271/2013-01-1419.
- Daniel Hans** Security in Safety Systems: the Need to Step beyond Traditional Engineering [Conference] // The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop. - 2008.
- DARPA I2O HACMS** High-Assurance Cyber Military Systems (HACMS) [Online] // Open Catalog / prod. Fisher Kathleen. - DARPA, 06 11 2014. - 21 11 2014. - <http://www.darpa.mil/opencatalog/HACMS.html>.
- Daruwala Burzin [et al.]** Threat Analysis for Hardware and Software Products Using HazOp [Book Section] // International Conference on Computational and Information Science (CIS'09). - Stevens Point : World Scientific and Engineering Academy and Society (WSEAS), 2009.
- De Saqui-Sannes Pierre and Aprville Ludovic** AVATAR/TTTool : un environnement en mode libre pour SysML temps réel [Conference] // Génie Logiciel. - [s.l.] : HAL, archives-ouvertes, 2011. - Vol. 98. - pp. 22-26. - In French. - hal-00667856.
- DEF STAN 00-56** Safety Management Requirements for Defence Systems - Part 1: Requirements [Report]. - [s.l.] : UK Ministry of Defence, 1996. - Withdrawn.
- DEF STAN 00-56** Safety Management Requirements for Defence Systems - Part 1: Requirements [Report] : Military Standard. - [s.l.] : UK Ministry of Defence, 2014. - Issue 5.
- Delange Julien** Security and dependability integration for the construction of critical middleware (in French: Intégration de la sécurité et de la sûreté de fonctionnement dans la construction d'intergiciels critiques) [Report] : PhD Thesis / Laboratoire Traitement et Communication de l'Information, UMR 5141 ; Département informatique et réseau. - Paris : Ecole Nationale Supérieure des Télécommunications (TELECOM ParisTech), 2010. - p. 276. - pastel-00006301.
- Deleuze Gilles [et al.]** Are safety and security in industrial systems antagonistic or complementary issues? [Book Section] // 17th European safety and reliability conference (ESREL) / book auth. Martorell Sebastián, Guedes Soares Carlos and Barnett Julie. - Valencia : CRC Press, 2008. - <http://hal-ineris.ccsd.cnrs.fr/ineris-00970394>.
- Derock A., Hebrard P. and Vallée F.** Convergence of the latest standards addressing safety and security for information technology [Book Section] // On-line proceedings of Embedded Real Time Software and Systems (ERTS2 2010). - Toulouse, France : [s.n.], 2010.
- Dewar Robert B. K.** Safety and security: two sides of the same coin? [Conference] // The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop. - 2008.
- Directive 2008/57/EC** Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (Recast) [Report] : Directive. - [s.l.] : Official Journal of the European Union, 2008. - p. 45. - Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0057&from=EN>.
- Directive 95/46/EC** Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Online] // EUR-Lex. - European Parliament, Council of the European Union, 24 10 1995. - 18 09 2015. - <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046>.
- D-MILS** Distributed MILS for Dependable Information and Communication Infrastructures [Online]. - Scott Hansen, 2007. - 12 06 2015. - www.d-mils.org/.

- Dolev Danny and Yao Andrew C.** On the security of public key protocols [Journal] // IEEE Transactions on Information Theory / ed. IEEE. - 1983. - 2 : Vol. 29. - pp. 198-208. - DOI: 10.1109/TIT.1983.1056650.
- Eames David Peter and Moffett Jonathan** The Integration of Safety and Security Requirements [Book Section] // SAFECOMP '99 Proceedings of the 18th International Conference on Computer Computer Safety, Reliability and Security. - London : Springer-Verlag, 1999. - ISBN:3-540-66488-2 .
- EASA CS-25** Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes / Amendment 15 [Report] : Standard. - Cologne : European Aviation Safety Agency, 2014. - p. 921. - Available at <http://easa.europa.eu/system/files/dfu/00%20Annex%20to%20ED%20Decision%202014-026-R.pdf>.
- EASA** Regulations [Online]. - European Aviation Safety Agency , 2014. - 27 09 2014. - <http://easa.europa.eu/regulations>.
- EC DG Health & Consumers** Medical devices - Reference documents [Online] // Public Health. - European Commission - DG Health & Consumers, 2014. - 06 10 2014. - http://ec.europa.eu/health/medical-devices/documents/index_en.htm.
- EC M/483 EN** Mandate for programming and standardisation addressed to the European standardisation bodies under Directive 2008/57/EC in the field of the interoperability of the rail system within the European Union [Report] : Mandate / Directorate-General for Mobility and Transport. - Brussels : European Commission, 2011. - p. 4. - Mandate for programming and standardisation addressed to the European standardisation bodies under Directive 2008/57/EC in the field of the interoperability of the rail system within the European Union.
- ECSS Web page** Home [Online] // European Cooperation on Space Standardization (ECSS). - European Space Agency, 2014. - 02 10 2014. - <http://www.ecss.nl/>.
- ECSS-Q-ST-30C** Space product assurance - Dependability [Report] : Standard / ESA Requirements and Standards Division. - Noordwijk : European Cooperation on Space Standardization (ECSS), 2009. - p. 54.
- ECSS-Q-ST-40C** Space product assurance - Safety [Report] : Standard / ESA Requirements and Standards Division. - Noordwijk : European Cooperation on Space Standardization (ECSS), 2009. - p. 75.
- ECSS-Q-ST-80C** Space product assurance - Software product assurance [Report] : Standard / ESA Requirements and Standards Division. - Noordwijk : European Cooperation on Space Standardization (ECSS), 2009. - p. 113.
- Elliott John, Lovering Andy and Gerrard Chris** Enhancing Safety Assurance Using Security Concepts [Conference] // Proceedings of the 3rd Safety-critical Systems Symposium / ed. Redmill Felix and Anderson Tom. - Brighton : Springer London, 1995. - pp. 90-116. - DOI: 10.1007/978-1-4471-3003-1_7.
- ETR 367** Telecommunications Security; Guidelines on the relevance of security evaluation to ETSI standards [Report] : ETSI Technical Report (ETR) 367. - Sophia Antipolis - Valbonne : European Telecommunications Standards Institute, 1997. - p. 21. - DTR/SEC-002701.
- EU COM(2012) 11 final** Reform of the data protection legal framework in the EU [Online] // European Commission - Justice - Data protection. - 01 2012. - 18 09 2015. - http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
- EUROCAE ED-109A** Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems - Software Integrity Assurance [Rapport] : Standard. - [s.l.] : European Organisation for Civil Aviation Equipment, 2012.
- EUROCAE ED-12B** Software Considerations in Airborne Systems and Equipment Certification [Report] : Standard. - [s.l.] : European Organisation for Civil Aviation Equipment, 1992. - Superseded by EUROCAE ED-12C:2012. - WG-12.
- EUROCAE ED-12C** Software Considerations in Airborne Systems and Equipment Certification [Report] : Standard. - [s.l.] : European Organisation for Civil Aviation Equipment, 2012. - WG-12.
- EUROCAE ED-14G** Environmental Conditions and Test Procedures for Airborne Equipment [Report] : Standard. - [s.l.] : European Organisation for Civil Aviation Equipment, 2011.
- EUROCAE ED-153** Guidelines for ANS Software Safety Assurance [Report] : Standard. - [s.l.] : European Organisation for Civil Aviation Equipment, 2009.
- EUROCAE ED-202** Airworthiness security process specification [Report]. - [s.l.] : European Organization for Civil Aviation Equipment (EUROCAE), 2010. - Superseded by EUROCAE ED-202A:2014. - WG-72.
- EUROCAE ED-202A** Airworthiness Security Process Specification [Report] : Standard. - [s.l.] : European Organization for Civil Aviation Equipment (EUROCAE), 2014.
- EUROCAE ED-203** Airworthiness security methods and considerations [Report] : Standard. - [s.l.] : European Organization for Civil Aviation Equipment, 2012. - Working draft version rev 0.9.9. - WG-72.
- EUROCAE ED-204** Information Security Guidance for Continuing Airworthiness [Report] : Standard. - [s.l.] : EUROCAE, 2014.

- EUROCAE ED-215** Software Tool Qualification Considerations [Report]: Standard. - [s.l.]: European Organisation for Civil Aviation Equipment, 2012.
- EUROCAE ED-216** Formal Methods supplement to ED-12C and ED-109A [Report]: Standard. - [s.l.]: European Organisation for Civil Aviation Equipment, 2012.
- EUROCAE ED-217** Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A [Report]: Standard. - [s.l.]: European Organisation for Civil Aviation Equipment, 2012.
- EUROCAE ED-218** Model-Based development and verification supplement to ED-12C and ED-109A [Report]: Standard. - [s.l.]: European Organisation for Civil Aviation Equipment, 2012.
- EUROCAE ED-79A** Guidelines for Development of Civil Aircraft and Systems [Rapport]: Standard. - [s.l.]: European Organisation for Civil Aviation Equipment, 2010.
- EUROCAE ED-80** Design Assurance Guidance for Airborne Electronic Hardware [Report]: Standard. - [s.l.]: European Organisation for Civil Aviation Equipment, 2000. - WG-46.
- EURO-MILS EC FP7 Project EURO-MILS** [Online]. - 01 10 2012. - 16 09 2014. - <http://www.euomils.eu/>.
- EVITA** E-safety vehicle intrusion protected applications (EVITA) [Online] // Evita-project / prod. Henniger Olaf. - FP7 EVITA Project, 1 12 2011. - 07 11 2014. - <http://www.evita-project.org/index.html>.
- exida** Certification [Online]. - 2015. - 2015 05 28. - <http://www.exida.com/Certification/>.
- Faucogney Anthony and al.** Report on open-issues in security and safety concern integration [Report] / ITEA2 – Project #11011. - [s.l.]: Multi-Concerns Interactions System Engineering (MERgE), 2014. - D3.4.1.
- Favaro John and Stroud Robert** ARTEMIS SESAMO Project: Work Achieved and Perspectives [Conference] // 1st International Workshop on the Integration of Safety and Security Engineering (ISSE), 33rd International Conference on Computer Safety, Reliability and Security (SafeComp). - Florence: [s.n.], 2014. - Introductory talk - Slides only.
- Feyt Nathalie [et al.]** Security Engineering Guide [Report]: Guide / Thales. - [s.l.]: Chorus 2.0, 2016. - p. 44. - 87210647-DDQ-GRP-EN.
- Firesmith Donald G.** Common concepts underlying safety, security, and survivability engineering [Report] / Software Engineering Institute; Carnegie Mellon University. - 2003. - CMU/SEI-2003-TN-033.
- Firesmith Donald G.** Tutorial: Engineering safety- and security-related requirements for software-intensive systems [Conference] // 6th International Workshop on Software Engineering for Secure Systems (SESS'10) Workshop at the 32nd ICSE Conference. - Cape Town, South Africa: [s.n.], 2010.
- Fisher Kathleen** High Assurance Cyber Military Systems (HACMS): Making sure you are in control of your vehicle [Conference]. - [s.l.]: DARPA, 2013. - p. 33.
- Förster Marc, Schwarz Reinhard and Steiner Max** Integration of modular safety and security models for the analysis of the impact of security on safety [Report]. - [s.l.]: Fraunhofer IESE, 2010. - IESE-078.10/E.
- Foster Nathalie Louise** The application of software and safety engineering techniques to security protocol development [Report]: Thesis. - [s.l.]: University of York, 2002.
- Fovino Igor Nai, Masera Marcelo and De Cian Alessio** Integrating Cyber Attacks within Fault Trees [Journal] // Reliability Engineering and System Safety / ed. LTD ELSEVIER SCI. - 2009. - 9: Vol. 94. - pp. 1394-1402. - 10.1016/j.ress.2009.02.020.
- FR-78-151-47712** Federal Register / Vol. 78, No. 151, p 47712 [Online]. - 06 08 2013. - 06 10 2014. - <http://www.gpo.gov/fdsys/pkg/FR-2013-08-06/pdf/2013-19020.pdf>.
- Freie Universität Berlin, Institut für Informatik** Research Forum on Public Safety and Security [Online] // Forschungsforum Öffentliche Sicherheit. - 10 2009. - 03 06 2014. - <http://www.sicherheit-forschung.de/en/forschungsforum/index.html>.
- Fruth Jana and Nett Edgar** Uniform Approach of Risk Communication in Distributed IT Environments Combining Safety and Security Aspects [Conference] // 1st International Workshop on the Integration of Safety and Security Engineering (ISSE), 33rd International Conference on Computer Safety, Reliability and Security (SafeComp) / ed. Bondavalli Andrea, Ceccarelli Andrea and Ortmeier Frank. - Florence: Springer, 2014. - pp. 289-300. - DOI: 10.1007/978-3-319-10557-4_32.
- Furtwangen University** Security & Safety Engineering (Bachelor) [Online] // Furtwangen University. - 19 05 2014. - <http://en.hs-furtwangen.de/study-programmes/area-of-interest/engineering-sciences/security-safety-engineering-bachelor.html>.
- Garavel Hubert and Graf Susanne** Formal Methods for Safe and Secure Computers Systems [Report]: Survey. - [s.l.]: Federal Office for Information Security, 2013. - p. 326. - BSI Study 875.
- Gebauer Carsten** Safety and security as drivers for future system development [Conference] // 1st Workshop on Safety and Security. - Kaiserslautern: [s.n.], 2014. - Slides only.
- Gerhold Lars** The Future of Research on Safety and Security in Germany - Results from an Explorative Delphi Study [Book Section] // Security in Futures – Security in Change, Proceedings of the Conference “Security in

- Futures – Security in Change”, 3-4 June 2010, Turku, Finland / book auth. Auffermann Burkhard and Kaskinen Juha / ed. Auffermann Burkhard and Kaskinen Juha. - 2011. - FFRC eBook 5/2011.
- Goertzel Karen Mercedes, Winograd Theodore and Hamilton Booz Allen** Safety and Security Considerations for Component-Based Engineering of Software-Intensive Systems [Report]. - [s.l.]: Navy Software Process Improvement Initiative (SPII) and Department of Homeland Security, 2011.
- Goertzel, Mercedes Karen and Feldman Larry** Software Survivability: Where Safety and Security Converge [Book Section] // Proceedings of the American Institute of Aeronautics and Astronautics (AIAA) Infotech@Aerospace Conference. - Seattle : [s.n.], 2009.
- Gorbenko Anatoliy [et al.]** F(I)MEA-technique of Web Services Analysis and Dependability Ensuring [Book Section] // Rigorous Development of Complex Fault-Tolerant Systems, Lecture Notes in Computer Science / ed. Butler Michael [et al.]. - Berlin Heidelberg : Springer, 2006. - Vol. 4157. - DOI: 10.1007/11916246_8.
- Green Hills Software** Integrity Real-Time Operating System [Online]. - 2014. - 16 12 2014. - <http://www.ghs.com/products/rtos/integrity.html>.
- Greve David, Wilding Matthew and Vaneet W. Mark** A Separation Kernel Formal Security Policy [Conference] // 4th International Workshop on the ACL2 Theorem Prover and its Applications (ACL2). - Boulder, Colorado, USA : [s.n.], 2003. - <http://www.cs.utexas.edu/users/moore/acl2/workshop-2003/>.
- Grøtan Tor Olav [et al.]** The SeSa Method for Assessing Secure. Remote Access to Safety Instrumented [Report]. - Trondheim : Sintef, 2007. - p. 44. - <https://www.sintef.no/globalassets/project/pds/reports/sintef-a1626-the-sesa-method-for-assessing-secure-remote-access-to-safety-instrumented-systems.pdf>. - SINTEF A1626.
- Gutgarts Peter B. and Temin Aaron** Security-Critical versus Safety-Critical Software [Book Section] // Proceedings of IEEE International Conference on Technologies for Homeland Security (HST). - 2010. - DOI: 10.1109/THS.2010.5654973.
- Hansen Kai** Security attack analysis of safety systems [Book Section] // Proceedings of IEEE Conference on Emerging Technologies & Factory Automation (ETFA). - Mallorca : [s.n.], 2009. - DOI: 10.1109/ETFA.2009.5347258.
- Helmer Guy [et al.]** A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System [Journal] // Requirements Engineering. - London : Springer-Verlag, 2002. - 4 : Vol. 7. - pp. 207-220. - DOI: 10.1007/s007660200016.
- Hessami Ali G.** A systems framework for safety and security: The holistic paradigm [Section] // Systems Engineering. - [s.l.]: Wiley Periodicals, 2004. - 2nd : Vol. 7. - DOI: 10.1002/sys.10060.
- Hessami Ali G.** Surety: Atkins Integrated Safety, Security and Environmental Assurance, Product Sheet [Online] // Atkins. - 2014. - <http://www.atkinsglobal.com/>.
- Honeywell** Integrating Control and Safety with Secure System [Report] : White Paper / Automation & Control Solutions. - Phoenix : [s.n.], 2008. - p. 11.
- Horn Marianne** Developing safety-security critical systems: A prototype LEGO Mindstorm Detection System [Report] : Technical Report / Department of Computer and Information Science (IDI). - Trondheim : Norwegian University of Science and Technology (NTNU), 2005. - p. 82. - URL: <http://www.idi.ntnu.no/grupper/su/fordypningsprosjekt-2005/horn-fordyp05.pdf>.
- HSEQ AP** HSEQ assessment [Online] // Inspecta. - 2012. - 18 05 2015. - <http://www.inspecta.com/en/Our-Services/Certification/Management-Systems/HSEQ-assessment/>.
- Hunter Bruce** Integrating Safety and Security into the System Lifecycle [Conference] // Improving Systems and Software Engineering Conference (ISSEC) / ed. (ISSEC) Improving Systems and Software Engineering Conference. - Canberra : Eventcorp Pty Ltd, 2009. - pp. 147-158. - ISBN: 978-0-9807680-0-8.
- IAEA DSSR** Safety of Nuclear Power Plants: Design Specific Safety Requirements [Report] : Standard. - Vienna : International Atomic Energy Agency (IAEA), 2012.
- IAEA NS-G-1.1** Software for computer based systems important to safety in nuclear power plants - safety guide [Report] : Standard. - Vienna : International Atomic Energy Agency (IAEA), 2000. - p. 97. - ISSN: 1020-525X.
- IAEA NS-G-1.3** Instrumentation and Control Systems Important to Safety in Nuclear Power Plants - Safety Guide [Report] : Standard. - Vienna : International Atomic Energy Agency (IAEA), 2002. - p. 99.
- IAEA NS-R-1** Safety of nuclear power plants : design : safety requirements [Report] : Standard. - Vienna : International Atomic Energy Agency (IAEA), 2000. - p. 73. - Superseded by IAEA SSR-2/1:2012.
- IAEA SSR-2/1** Safety of nuclear power plants : design : specific safety requirements [Report] : Standard. - Vienna : International Atomic Energy Agency (IAEA), 2012. - p. 91. - ISSN: 1020-525X.
- Ibrahim Linda [et al.]** Safety and Security Extensions for Integrated Capability Maturity Models [Report] / United States Federal Aviation Administration. - 2004.

- ICAO** ICAO Secretariat Study on the Safety and Security Aspects of Economic Liberalization [Report]. - [s.l.] : International Civil Aviation Organization, 2005.
- IEC 31010** Risk management -- Risk assessment techniques [Report]. - [s.l.] : International Electrotechnical Commission, 2009. - p. 176. - ISO/TMBG.
- IEC 60601-1-SER** Medical electrical equipment - All parts [Report] : Standard. - [s.l.] : International Electrotechnical Commission (IEC), 2014. - p. 1368. - TC/SC 62A.
- IEC 60880** Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions [Report]. - [s.l.] : International Electrotechnical Commission (IEC), 2006. - p. 217. - TC/SC 45A.
- IEC 60880** Software for computers in the safety systems of nuclear power stations [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 1986. - p. 133. - Superseded by IEC 60880 ed2.0 (2006-05).
- IEC 61226** Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions [Report] : Standard. - [s.l.] : International Electrotechnical Commission (IEC), 2009. - p. 64. - TC/SC 45A.
- IEC 61508-1** Functional safety of electrical / electronic / programmable electronic safety-related systems - Part 1: General requirements [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 1998. - p. 115. - (withdrawn). - Ed1.0.
- IEC 61508-2** Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2000. - p. 143. - (withdrawn).
- IEC 61508-3** Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 1998. - p. 95. - (withdrawn).
- IEC 61508-4** Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 1998. - p. 53. - (withdrawn).
- IEC 61508-5** Functional safety of electrical/electronic/programmable electronic safety related systems - Part 5: Examples of methods for the determination of safety integrity levels [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 1998. - p. 57. - (withdrawn).
- IEC 61508-6** Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2000. - p. 145. - (withdrawn).
- IEC 61508-7** Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2000. - p. 229. - (withdrawn). - ISBN: 2-8318-5151-3.
- IEC 61511-SER** Functional safety – Safety instrumented systems for the process industry sector – All Parts [Report] : Standard. - Geneva : International Electrotechnical Commission, 2004. - p. 449. - TC/SC 65A.
- IEC 61513** Nuclear power plants - Instrumentation and control important to safety - General requirements for systems [Report] : Standard. - [s.l.] : International Electrotechnical Commission (IEC), 2011. - p. 205. - TC/SC 45A.
- IEC 62138** Nuclear power plants - Instrumentation and control important to safety - Software aspects for computer-based systems performing category B or C functions [Report]. - [s.l.] : International Electrotechnical Commission (IEC), 2004. - p. 95. - TC/SC 45A.
- IEC 62278** Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS) [Report] : Standard. - Geneva : International Electrotechnical Commission, 2002. - p. 159. - TC/SC 9.
- IEC 62304** Medical device software - Software life cycle processes [Report] : Standard. - [s.l.] : International Electrotechnical Commission (IEC), 2006. - p. 155. - ISBN: 2-8318-8637-6.
- IEC 62443-2-1** Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2010. - TC/SC 65.
- IEC 62443-3-3** Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2013.
- IEC 62645** Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2014. - p. 93.

- IEC 62859** Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2015. - Ed. 1.0.
- IEC 80001-1** Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities [Report]. - [s.l.] : International Electrotechnical Commission, 2010. - p. 70. - ISO/TC 215.
- IEC/TR 62443-3-1** Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2009.
- IEC/TS 62443-1-1** Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2009. - TC/SC 65.
- INCOSÉ** What is a standard? [Online]. - International Council on System Engineering , 23 11 2004. - 28 09 2014. - www.incose.org/practice/standards/standards.aspx.
- ISO 14971** Medical devices -- Application of risk management to medical devices [Report]. - [s.l.] : International Organization for Standardization, 2007. - p. 82. - Revises ISO 14971:2000. - ISO/TC 210.
- ISO 15998** Earth-moving machinery -- Machine-control systems (MCS) using electronic components -- Performance criteria and tests for functional safety [Report] : Standard. - [s.l.] : International Organization for Standardization, 2008. - p. 33. - ISO/TC 127/SC 3.
- ISO 23273** Fuel cell road vehicles -- Safety specifications -- Protection against hydrogen hazards for vehicles fuelled with compressed hydrogen [Report] : Standard. - [s.l.] : International Organization for Standardization, 2013. - p. 6. - ISO/TC 22/SC 21.
- ISO 25119-1** Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems -- Part 1: General principles for design and development [Report] : Standard. - [s.l.] : International Organization for Standardization, 2010. - p. 24. - ISO/TC 23/SC 19.
- ISO 25119-2** Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems -- Part 2: Concept phase [Report]. - [s.l.] : International Organization for Standardization, 2010. - p. 37. - ISO/TC 23/SC 19.
- ISO 25119-3** Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems -- Part 3: Series development, hardware and software [Report]. - [s.l.] : International Organization for Standardization, 2010. - p. 57. - ISO/TC 23/SC 19.
- ISO 25119-4** Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems -- Part 4: Production, operation, modification and supporting processes [Report] : Standard. - [s.l.] : International Organization for Standardization, 2010. - p. 22. - ISO/TC 23/SC 19.
- ISO 26262-1** Road vehicles -- Functional safety -- Part 1: Vocabulary [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 23. - ISO/TC 22/SC 3.
- ISO 26262-10** Road vehicles -- Functional safety -- Part 10: Guideline on ISO 26262 [Report] : Standard. - [s.l.] : International Organization for Standardization, 2012. - p. 89. - ISO/TC 22/SC 3.
- ISO 26262-2** Road vehicles -- Functional safety -- Part 2: Management of functional safety [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 26. - ISO/TC 22/SC 3.
- ISO 26262-3** Road vehicles -- Functional safety -- Part 3: Concept phase [Report]. - [s.l.] : International Organization for Standardization, 2011. - p. 25. - ISO/TC 22/SC 3.
- ISO 26262-4** Road vehicles -- Functional safety -- Part 4: Product development at the system level [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 36. - ISO/TC 22/SC 3.
- ISO 26262-5** Road vehicles -- Functional safety -- Part 5: Product development at the hardware level [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 76. - ISO/TC 22/SC 3.
- ISO 26262-6** Road vehicles -- Functional safety -- Part 6: Product development at the software level [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 40. - ISO/TC 22/SC 3.
- ISO 26262-7** Road vehicles -- Functional safety -- Part 7: Production and operation [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 11. - ISO/TC 22/SC 3.
- ISO 26262-8** Road vehicles -- Functional safety -- Part 8: Supporting processes [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 48. - ISO/TC 22/SC 3.
- ISO 26262-9** Road vehicles -- Functional safety -- Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 16. - ISO/TC 22/SC 3.
- ISO 31000** Risk management – Principles and guidelines [Report] : Standard. - [s.l.] : International Organization for Standardization, 2009. - p. 24. - ISO/TC 262.

ISO 6469-1 Electrically propelled road vehicles -- Safety specifications -- Part 1: On-board rechargeable energy storage system (RESS) [Report] : Standard. - [s.l.] : International Organization for Standardization, 2009. - p. 9. - ISO/TC 22/SC 21.

ISO 6469-2 Electrically propelled road vehicles -- Safety specifications -- Part 2: Vehicle operational safety means and protection against failures [Report] : Standard. - [s.l.] : International Organization for Standardization, 2009. - p. 6. - ISO/TC 22/SC 21.

ISO 6469-3 Electrically propelled road vehicles -- Safety specifications -- Part 3: Protection of persons against electric shock [Report] : Standard. - [s.l.] : International Organization for Standardization, 2011. - p. 14. - ISO/TC 22/SC 21.

ISO/IEC 15026 Information technology -- System and software integrity levels [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 1998. - Withdrawn. - ISO/IEC JTC 1/SC 7.

ISO/IEC 15026-1 Systems and software engineering -- Systems and software assurance -- Part 1: Concepts and vocabulary [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2013. - p. 24. - Revises: ISO/IEC TR 15026-1:2010. - ISO/IEC JTC 1/SC 7.

ISO/IEC 15026-2 Systems and software engineering -- Systems and software assurance -- Part 2: Assurance case [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2011. - p. 10. - ISO/IEC JTC 1/SC 7.

ISO/IEC 15026-3 Systems and software engineering -- Systems and software assurance -- Part 3: System integrity levels [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2011. - p. 32. - Revises: ISO/IEC 15026:1998.

ISO/IEC 15408-1 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2009. - p. 64. - ISO/IEC JTC 1/SC 27.

ISO/IEC 15408-1 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2005. - Withdrawn.

ISO/IEC 15408-1 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 1999. - Withdrawn.

ISO/IEC 15408-2 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2008. - p. 218. - ISO/IEC JTC 1/SC 27.

ISO/IEC 15408-2 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 1999. - p. 27. - Revised by: ISO/IEC 15408-2:2005.

ISO/IEC 15408-3 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components [Report]. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2008. - p. 174. - ISO/IEC JTC 1/SC 27.

ISO/IEC 15408-3 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 1999. - Withdrawn.

ISO/IEC 17799 Information technology -- Code of practice for information security management [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2000. - Revised by: ISO/IEC 17799:2005. - ISO/IEC JTC 1/SC 27.

ISO/IEC 17799 Information technology -- Security techniques -- Code of practice for information security management [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2005. - Revised by: ISO/IEC 27002:2005. - ISO/IEC JTC 1/SC 27.

ISO/IEC 18045 Information technology -- Security techniques -- Methodology for IT security evaluation [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission (ISO/IEC), 2008. - p. 290. - ISO/IEC JTC 1/SC 27.

ISO/IEC 21827 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® [Report] = SSE-CMM®. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2008. - p. 144. - ISO/IEC JTC 1/SC 27.

ISO/IEC 21827 Information technology -- Systems Security Engineering -- Capability Maturity Model [Report] = SSE-CMM®. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2002. - Withdrawn.

ISO/IEC 27000 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2014. - p. 31. - ISO/IEC JTC 1/SC 27.

ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2013. - p. 23. - ISO/IEC JTC 1/SC 27.

ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security controls [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2013. - p. 80. - ISO/IEC JTC 1/SC 27.

ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2011. - p. 68. - ISO/IEC JTC 1/SC 27.

ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management [Report] : Standard. - [s.l.] : International Standards Organization / International Electrotechnical Commission, 2008. - Withdrawn. - ISO/IEC JTC 1/SC 27.

ITSEC Information Technology Security Evaluation Criteria (ITSEC) - Harmonized Criteria of France, Germany, the Netherlands, the United Kingdom [Report] / Department of Trade and Industry. - London : Commission of the European Communities, 1991. - p. 164. - Withdrawn - Available: https://www.bsi.bund.de/cae/servlet/contentblob/471346/publicationFile/30220/itsec-en_pdf.pdf.

Jackson Daniel Alloy: a language & tool for relational models [Online] // MIT. - 2012. - 12 05 2015. - <http://alloy.mit.edu/alloy/>.

Jackson Dave and Dobbing Brian Changing Regulation in Safety and Security – Implications and Opportunities [Conference] // The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop. - 2008.

Jacquet Jean-René, Thuiller Elie and Tyrode Jean-Francois Security Risk Assessment Guide [Report] : Guide / Thales. - [s.l.] : Chorus 2.0, 2016. - p. 39. - 87210648-DDQ-GRP-EN.

Jalouneix Jean, Cousinou Patrick and Jean Couturier Denis Winter Approche comparative entre sûreté et sécurité nucléaires [Report] : Technical Report. - [s.l.] : Institut de Radioprotection et the Sûreté Nucléaire (IRSN), 2009. - p. 26. - [inFrench]. - IRSN 2009/117.

Johnson Chris W. Using Assurance Cases and Boolean Logic Driven Markov Processes to Formalise Cyber Security Concerns for Safety-Critical Interaction with Global Navigation Satellite Systems [Journal] // Electronic Communications of the EASST. - 2011. - Vol. 45. - pp. 1-18. - DOI: <http://dx.doi.org/10.14279/tuj.eceasst.45.679>.

Johnson Christopher W. CyberSafety: On the Interactions Between CyberSecurity and the Software Engineering of Safety-Critical Systems [Book Section] // Achieving System Safety / book auth. Dale C. and Anderson T.. - London : Springer Verlag, 2012. - Paper to accompany a keynote address, 20th Annual Conference of the UK Safety-Critical Systems Club. - ISBN: 978-1-4471-2493-1.

Johnson Roger G. Adversarial safety analysis: borrowing the methods of security vulnerability assessments [Journal] // Journal of Safety Research. - Amsterdam : Elsevier Science B.V., 2004. - 3 : Vol. 35. - pp. 245-248. - DOI: 10.1016/j.jsr.2004.03.013.

Jonsson Erland and Olovsson Tomas On the Integration of Security and Dependability in Computer Systems [Conference] // International Conference on Reliability, Quality Control and Risk Assessment (IASTED). - Washington DC : [s.n.], 1992. - pp. 93-97. - http://publications.lib.chalmers.se/records/fulltext/167782/local_167782.pdf. - ISBN: 0-88986-171-4.

Jonsson Erland Towards an integrated conceptual model of security and dependability [Conference] // First International Conference on Availability, Reliability and Security (ARES). - [s.l.] : IEEE, 2006. - pp. 646-653. - DOI: 10.1109/ARES.2006.138.

Joyce Jeff and Fabre Laurent Integration of security & airworthiness in the context of certification and standardization [Conference] // 1st workshop on the Integration of Safety and Security Engineering (ISSE). - Florence : [s.n.], 2014. - p. 18. - Invited talk - Slides only.

Katta Vikash and Stålhane Tor Traceability of Safety Systems: Approach, Meta-Model and Tool Support [Report] : Technical Report / OECD Halden Reactor Project. - Trondheim : Institute for Energy Technology (IET), 2013b. - Available upon request. - HWR-1053.

Katta Vikash, Raspotnig Christian and Stålhane Tor Requirements management in a combined process for safety and security assessments [Conference] // 8th International Conference on Availability, Reliability and Security (ARES). - Regensburg, Germany : [s.n.], 2013a.

Kleidermacher Mike and Kleidermacher David Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development [Book]. - [s.l.] : Elsevier, 2012. - p. 396. - ISBN: 978-0-12-386886-2.

Knorre Daniel and Apvrille Ludovic TEPE: A SysML Language for Time-Constrained Property Modeling and Formal Verification [Conference] // Third IEEE International workshop UML and Formal Methods (UML&FM). - Shanghai : IEEE, 2010. - DOI:10.1145/1921532.1921556.

Kornecki Andrew J. and Liu Mingye Fault Tree Analysis for Safety/Security Verification in Aviation Software [Journal]. - [s.l.] : Electronics, 2013a. - 1 : Vol. 2. - pp. 41-56. - DOI:10.3390/electronics2010041.

Kornecki Andrew J., Subramanian Nary and Zalewski Janusz Studying Interrelationships of Safety and Security for Software Assurance in Cyber-Physical Systems: Approach Based on Bayesian Belief Networks [Conference] // Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS). - Kraków : IEEE, 2013b. - pp. 1381–1387.

Koscher Karl [et al.] Experimental Security Analysis of a Modern Automobile [Conference] // Symposium on Security and Privacy (SP). - Oakland, CA, USA : IEEE, 2010. - pp. 447 - 462. - ISBN: 978-1-4244-6894-2.

Kriaa Siwar [et al.] A survey of approaches combining safety and security for industrial control systems [Journal] // ScienceDirect Publication: Reliability Engineering & System Safety. - [s.l.] : Elsevier, 2015a. - Vol. 139. - pp. 156-178. - <http://freepaper.me/download/PDF/10.1016-J.RESS.2015.02.008.PDF?hash=MMMz7yMUAtol5XReLMQNGw>. - DOI: 10.1016/j.res.2015.02.008 .

Kriaa Siwar [et al.] Comparing two approaches to safety and security modelling: BDMP technique and CHASSIS method [Conference] // OECD Halden Reactor Project, 37th Enlarged Halden Programme Group (EHPG) meeting. - Storefjell : [s.n.], 2013. - number C4.14.

Kriaa Siwar [et al.] Safety and Security Interactions Modeling Using the BDMP Formalism: Case Study of a Pipeline [Book Section] // Computer Safety, Reliability, and Security (Lecture Notes in Computer Science), Proceedings of the 33rd International Conference, SAFECOMP 2014, Florence, Italy, September 10-12, 2014 / book auth. Bondavalli Andrea and Giandomenico Felicita Di. - Florence : Springer International Publishing, 2014. - Vol. 8666. - 10.1007/978-3-319-10506-2_22.

Kriaa Siwar, Bouissou Marc and Laarouchi Youssef A Model Based Approach For SCADA Safety and Security Joint Modelling: S-cube [Conference] // IET Safety and Cyber-Security Conference. - Bristol : [s.n.], 2015b.

Ksinant Vladimir [et al.] Cyber-security for Architects Guide [Report] : Guide / Thales. - [s.l.] : Chorus 2.0, 2016. - p. 84. - 87210649-DDQ-GRP-EN.

Lano Kevin, Clark David and Androutopoulos Kelly Safety and Security Analysis of Object-Oriented Models [Book Section] // Computer Safety, Reliability and Security - Proceedings of 21st International SAFECOMP Conference, Catania, Italy, September 10–13, 2002 / ed. Heidelberg Springer Berlin. - 2002. - Vol. 2434. - DOI: 10.1007/3-540-45732-1_10.

Laprie Jean-Claude Dependability: Basic Concepts and Terminology [Book]. - Vienna : Springer, 1992. - Vol. 5 : pp. 3-245. - DOI: 10.1007/978-3-7091-9170-5.

Lee Shou-Yu, Wong W. Eric and Gao Ruizhi Software Safety Standards: Evolution and Lessons Learned [Conference] // First International Conference on Trustworthy Systems and Their Applications (TSA). - Taiwan : [s.n.], 2014.

Line Maria B. [et al.] Safety vs. Security? [Conference] // International Conference on Probabilistic Safety Assessment and Management (PSAM 8). - New Orleans, USA : [s.n.], 2006.

Lynch J. A. Applying Safety Critical Systems Engineering Techniques to Secure Systems [Report]. - 2002. - p. 82. -

http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCMQFjAA&url=http%3A%2F%2Fwww-users.cs.york.ac.uk%2F~jac%2FPublishedPapers%2FJimLynch.doc&ei=DPSTVMXxH9OUav6dgl&usq=AFQjCNFHqroMkJZN_waDdyfIWwzHkHS5rQ&bvm=bv.82001339,d.d2

Lynx Software Technologies [Online]. - 2015. - 06 03 2015. - <http://www.lynx.com/>.

Macher Georg [et al.] A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive System [Conference] // 2nd International workshop on the Integration of Safety and Security Engineering / ed. Koornneef Floor and Gulijk Coen van. - Delft : Springer International Publishing Switzerland, 2015b. - Vol. LNCS 9338. - pp. 237–250. - DOI: 10.1007/978-3-319-24249-1_21.

Macher Georg [et al.] SAHARA: A Security-Aware Hazard and Risk Analysis Method [Conference] // Design, Automation & Test in Europe Conference & Exhibition (DATE). - Grenoble : IEEE, 2015a. - pp. 621-624. - ISBN: 978-3-9815-3704-8.

MAFTIA Malicious-and Accidental-Fault Tolerance for Internet Applications [Online] // LAAS. - IST MAFTIA Project n°11583, 01 01 2000. - 25 09 2014. - <http://webhost.laas.fr/TSF/cabernet/maftia/>.

- Mattila Minna** Different Views on Defining Safety, Security and Social Responsibility [Journal] // Interdisciplinary Studies Journal - Special Issue on Security, Safety and Social Responsibility / ed. Laakkonen Tarja, Paasonen Jyri and Mattila Minna. - Helsinki : Prima Oy, 2013. - 1 : Vol. 3. - pp. 7-20. - ISSN: 1799-2710.
- Mazzini Silvia [et al.]** Security and Safety Modelling in Embedded Systems [Conference] // Embedded Real Time Software and Systems (ERTS). - Toulouse : [s.n.], 2014.
- Mc Guire Nicholas** Utilizing security methods of FLOSS GPOS for safety [Conference] // Embedded World Exhibition & Conference. - Nürnberg : [s.n.], 2011.
- MIL-STD-882C** System Safety Program Requirements [Report] : Military Standard. - [s.l.] : US Department of Defense, 1993. - p. 115. - Superseded by MIL-STD-882D:2000.
- MIL-STD-882D** Standard Practice for System Safety [Report] : Military Standard. - [s.l.] : US Department of Defense, 2000. - p. 31. - Superseded by MIL-STD-882E:2012.
- MIL-STD-882E** Standard Practice for System Safety [Report] : Military Standard. - [s.l.] : Department of Defense (DoD), 2012. - p. 104. - Supersedes MIL-STD-882:2000.
- MODSafe** Modular Urban Transport Safety and Security Analysis [Online]. - EU FP7, 01 09 2008. - 21 05 2014. - <http://www.modsafe.eu/>.
- Monakova Ganna, Brucker Achim D. and Schaad Andreas** Security and safety of assets in business processes [Conference] // 27th Annual ACM Symposium on Applied Computing. - New York, NY, USA : Association for Computing Machinery, 2012. - pp. 1667-1673. - DOI: 10.1145/2245276.2232045.
- Müller Kevin [et al.]** MILS-Based Information Flow Control in the Avionic Domain: a Case Study on Compositional Architecture and Verification [Conference] // 31st Digital Avionics Systems Conference (DASC). - Williamsburg : IEEE, 2012a. - pp. 1-13. - DOI: 10.1109/DASC.2012.6382411.
- Müller Kevin [et al.]** MILS-related information flow control in the avionic domain: A view on security-enhancing software architectures [Conference] // 42nd International Conference on Dependable Systems and Networks Workshops (DSN-W). - Boston, MA : IEEE, 2012b. - pp. 1-6. - 10.1109/DSNW.2012.6264665.
- Müller Kevin [et al.]** On MILS I/O Sharing Targeting Avionic Systems [Conference] // 10th European Dependable Computing Conference (EDCC). - Newcastle : IEEE, 2014. - pp. 182-193. - 10.1109/EDCC.2014.35.
- Murdoch John [et al.]** Security Measurement [Report] : White-Paper / Safety & Security Technical Working Group (TWG). - [s.l.] : Practical Software and Systems Measurement (PSM), 2006. - p. 67. - v3.0.
- Netkachova Kateryna [et al.]** Security-Informed Safety Case Approach to Analysing MILS Systems [Conference] // 1st International Workshop on MILS: Architecture and Assurance for Secure Systems. - Amsterdam, The Netherlands : [s.n.], 2015. - <http://mils-workshop-2015.euromils.eu/>.
- Nicol David M., Sanders William H. and Trivedi Kishor S.** Model-based evaluation: from dependability to security [Journal] // IEEE Transactions on Dependable and Secure Computing. - [s.l.] : IEEE, 2004. - 1 : Vol. 1. - pp. 48-65. - DOI: 10.1109/TDSC.2004.11.
- Nielson Hanne Riis and Nielson Flemming** Safety versus Security in the Quality Calculus [Book Section] // Theories of Programming and Formal Methods, Lecture Notes in Computer Science / book auth. Liu Zhiming, Woodcock Jim and Zhu Huibiao. - Berlin Heidelberg : Springer, 2013. - Vol. 8051. - DOI: 10.1007/978-3-642-39698-4_18.
- NIST Cybersecurity Framework** Framework for Improving Critical Infrastructure Cybersecurity [Report] : Standard. - [s.l.] : National Institute of Standards and Technology, 2014. - p. 39. - Accessible at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.
- NIST SP 800-30** Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1 [Report] : Standard / Information Technology Laboratory ; Computer Security Division. - Gaithersburg : National Institute of Standards and Technology, 2012. - p. 95.
- NIST SP 800-30** Risk Management Guide for Information Technology Systems, Special Publication 800-30 [Report] : Standard / Information Technology Laboratory ; Computer Security Division. - Gaithersburg : National Institute of Standards and Technology, 2002. - p. 56. - Withdrawn.
- NIST SP 800-82** Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, Revision 1 [Report] : Standard / Computer Security Division ; Information Technology Laboratory. - Gaithersburg : National Institute of Standards and Technology, 2013. - p. 170. - <http://dx.doi.org/10.6028/NIST.SP.800-82r1>.
- Nordland Odd** Some Security Aspects in Safety-Related Systems [Conference] // The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop. - 2008.
- Novak Thomas, Treytl Albert and Palensky Peter** Common Approach to Functional Safety and System Security in Building Automation and Control Systems [Book Section] // Proceedings of Conference on Emerging Technologies and Factory Automation (ETFA). - [s.l.] : IEEE, 2007.

- NST036 IAEA** Computer Security of Instrumentation and Control Systems at Nuclear Facilities (Draft) [Report] : Standard. - Vienna : International Atomic Energy Agency (IAEA), 2014. - <http://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst036.pdf>.
- Obama Barack** Improving Critical Infrastructure Cybersecurity // Executive Orders. - Washington : The White House, Office of the Press Secretary, 2013. - Available at: <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>. - EO 13636.
- Olive Michael L., Oishi Roy T. and Arentz Stephen** Commercial Aircraft Information Security — An Overview of ARINC Report 811 [Conference] // 25th Digital Avionics Systems Conference (DASC). - Portland : IEEE, 2006. - pp. 1-12. - DOI: 10.1109/DASC.2006.313761.
- OMG SACM** Structured Assurance Case Meta-model [Online] // Object Management Group. - 2 2013. - 23 05 2014. - <http://www.omg.org/spec/SACM>.
- Pan Dong-bo and Huang Wei** Operation of Functional Safety and Security [Conference] // 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA). - [s.l.] : IEEE, 2007b. - pp. 1318 - 1322 . - DOI: 10.1109/ICIEA.2007.4318619.
- Pan Dong-bo and Liu Feng** Influence between Functional Safety and Security [Conference] // 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA). - [s.l.] : IEEE, 2007a. - pp. 1323 - 1325. - DOI: 10.1109/ICIEA.2007.4318620.
- PARSEC** Systematic Paris Region [Online] // Production d'Applications Réparties Sûres pour l'Embarqué Critique (PARSEC). - FUI 8 PARSEC, 10 2009. - 26 09 2014. - <http://www.systematic-paris-region.org/fr/projets/parsec>. - See also: <http://www.parsec-project.fr/>.
- Paul Stéphane and Rioux Laurent** Over 20 Years of Research in Cybersecurity and Safety Engineering: a short Bibliography [Conference] // 6th International Conference on Safety and Security Engineering (SAFE). - Opatija : [s.n.], 2015. - p. 15.
- Paul Stéphane** On the Meaning of Security for Safety (S4S) [Conference] // 6th International Conference on Safety and Security Engineering (SAFE). - Opatija : [s.n.], 2015.
- Paulitsch Michael [et al.]** Evidence-Based Security in Aerospace: From Safety to Security and Back Again [Conférence] // IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW). - [s.l.] : IEEE, 2012. - pp. 21-22. - DOI: 10.1109/ISSREW.2012.37.
- Pauly Bernard** Safety in Thales LAS –ATM [Conference] // Journée de Palaiseau on Safety Engineering. - Palaiseau : Thales, 2014. - p. 24. - Thales Group Internal.
- Pedroza Gabriel, Apvrille Ludovic and Knorreck Daniel** AVATAR: A SysML environment for the formal verification of safety and security properties [Conference] // 11th International Conference on New Technologies of Distributed Systems (NOTERE). - Paris : IEEE, 2011. - pp. 1-10. - DOI: 10.1109/NOTERE.2011.5957992.
- Pfitzmann Andreas** Why Safety and Security Should and Will Merge, Volume [Book Section] // Computer Safety, Reliability, and Security, Lecture Notes in Computer Science. - 2004. - Vol. 3219. - DOI: 10.1007/978-3-540-30138-7_1.
- Piètre-Cambacèdes Ludovic and Bouissou Marc** Cross-fertilizations between safety and security engineering [Journal] // Reliability Engineering & System Safety. - [s.l.] : Elsevier B.V., 2013. - Vol. 110. - pp. 110–126. - DOI: 10.1016/j.ress.2012.09.011.
- Piètre-Cambacèdes Ludovic and Bouissou Marc** Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes), IEEE International Conference Systems Man and Cybernetics (SMC) [Book Section]. - Istanbul : [s.n.], 2010. - DOI: 10.1109/ICSMC.2010.5641922.
- Piètre-Cambacèdes Ludovic and Chaudet Claude** Disentangling the relations between safety and security [Book Section] // AIC'09 Proceedings of the 9th WSEAS international conference on Applied informatics and communications. - Stevens Point : [s.n.], 2009. - ISBN: 978-960-474-107-6.
- Piètre-Cambacèdes Ludovic and Chaudet Claude** The SEMA referential framework: avoiding ambiguities when dealing with security and safety issues [Conference] // Fourth Annual IFIP Working Group 11.10, International Conference on Critical Infrastructure Protection (CIP). - Washington , DC, USA : [s.n.], 2010c.
- Piètre-Cambacèdes Ludovic and Quinn Ted** IEC 62859: Towards an international standard on the coordination between safety and cybersecurity for nuclear I&C systems [Conference] // 9th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC-HMIT). - Charlotte, USA : [s.n.], 2015.
- Piètre-Cambacèdes Ludovic** On the relations between safety and security (in French – “Des relations entre sûreté et sécurité”) [Report] : PhD Thesis / Informatique et Réseaux. - Paris : Telecom ParisTech, 2010f. - pastel-00570432.
- Piètre-Cambacèdes Ludovic** On the relations between safety and security (in French – “Des relations entre sûreté et sécurité”) [Report] : PhD Thesis / Informatique et Réseaux. - Paris : Telecom ParisTech, 2010f. - pastel-00570432.

- Pietre-Cambacedes Ludovic, Quinn Edward L. and Hardin Leroy** Cyber Security of Nuclear Instrumentation & Control Systems: Overview of the IEC Standardization Activities [Conference] // 7th International Federation of Automatic Control (IFAC) Conference on Manufacturing Modelling, Management and Control. - Saint Petersburg, Russia : [s.n.], 2013b.
- POK Community** Home page [Online] // A Partitioned Operating System (POK). - 31 01 2011. - 04 07 2014. - <http://pok.tuxfamily.org/>.
- Prentice Stephen P.** Safety Vs. Security: can we afford both? [Online] // AviationPros. - 01 04 2002. - 12 05 2015. - <http://www.aviationpros.com/article/10387597/safety-vs-security-can-we-afford-both>.
- QNX** QNX Hypervisor [Online]. - 2015. - 06 03 2015. - <http://www.qnx.com/products/hypervisor/index.html>.
- Ramirez Adrian Garcia [et al.]** On Two Models of Noninterference: Rushby and Greve, Wilding, and Vanfleet [Conference] // 33rd International Conference (SAFECOMP) / ed. Bondavalli Andrea and Giandomenico Felicita Di. - Florence : Springer International Publishing, 2014. - Vol. 8666. - pp. 246-261. - DOI: 10.1007/978-3-319-10506-2_17.
- Raspotnig Christian [et al.]** Enhancing CHASSIS: A Method for Combined Safety and Security Assessments [Conference] // 8th International Conference on Availability, Reliability and Security (ARES). - Regensburg, Germany : [s.n.], 2013b. - DOI: 10.1109/ARES.2013.102.
- Raspotnig Christian and Opdahl Andreas L.** Comparing risk identification techniques for safety and security requirements [Journal] // Journal of Systems and Software. - 2013a. - 4 : Vol. 86. - pp. 1124 – 1151. - DOI: 10.1016/j.jss.2012.12.002.
- Raspotnig Christian and Opdahl Andreas L.** Improving security and safety modelling with failure sequence diagrams [Book Section] // International Journal of Secure Software Engineering (IJSSE). - 2012a. - DOI: 10.4018/jsse.2012010102.
- Raspotnig Christian** Requirements for safe and secure information systems [Rapport] : Thesis / University of Bergen. - 2014.
- Raspotnig Christian, Karpati Peter and Katta Vikash** A Combined Process for Elicitation and Analysis of Safety and Security Requirements [Book Section] // Enterprise, Business- Process and Information Systems Modeling (EMMSAD), Lecture Notes in Business Information Processing / book auth. Bider I. [et al.]. - [s.l.] : Springer Berlin Heidelberg, 2012b. - Vol. 113. - DOI: 10.1007/978-3-642-31072-0_24.
- Regulation (EC) No 1108** Official Journal of the European Union [Online] // EUR-Lex. - European Parliament and Council, 21 10 2009. - 22 11 2014. - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:309:0051:0070:EN:PDF>.
- Reichenbach Frank [et al.]** A pragmatic approach on combined safety and security risk analysis [Book Section] // IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW). - Dallas : IEEE, 2012. - DOI: 10.1109/ISSREW.2012.98.
- Ridgway John** Achieving Safety through Security Management [Book Section] // The Safety of Systems / ed. Redmill Felix and Anderson Tom. - London : Springer, 2007. - DOI: 10.1007/978-1-84628-806-7_1.
- Roth Michael et Liggesmeyer Peter** Modeling and Analysis of Safety-Critical Cyber Physical Systems using State/Event Fault Trees [Conférence] // Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP) / éd. Roy Matthieu. - Toulouse, France : HAL, 2013. - HAL Id: hal-00848640.
- Rowe Jayson** Software Security & Design Assurance [Conference] // Design & Manufacture Seminar. - [s.l.] : Civil Aviation Safety Authority, Australian Government, 2013. - p. 35. - Slides only. - http://www.casa.gov.au/wcmswr/_assets/main/lib100210/d1t05.pdf.
- RTCA DO-160G** Environmental Conditions and Test Procedures for Airborne Equipment [Report] : Standard. - [s.l.] : Radio Technical Commission for Aeronautics, 2010. - SC-135.
- RTCA DO-178B** Software Considerations in Airborne Systems and Equipment [Report] : Standard. - Washington : Radio Technical Commission for Aeronautics, 1992. - Not superseded by RTCA DO-178C:2011. - SC-167.
- RTCA DO-178C** Software Considerations in Airborne Systems and Equipment [Report] : Standard. - Washington : Radio Technical Commission for Aeronautics, 2011. - p. 144. - RTCA DO-178C does not supersede RTCA DO-178B:1992. - SC-205.
- RTCA DO-254** Design Assurance Guidance for Airborne Electronic Hardware [Report] : Standard. - [s.l.] : Radio Technical Commission for Aeronautics, 2000. - SC-180.
- RTCA DO-278A** Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance [Report] : Standard. - Washington : Radio Technical Commission for Aeronautics, 2011. - SC-205.
- RTCA DO-326** Airworthiness Security Process Specification [Report] : Standard. - [s.l.] : Radio Technical Commission for Aeronautics, 2010. - Superseded by RTCA DO-326A. - SC-216.

- RTCA DO-326A** Airworthiness Security Process Specification [Report] : Standard. - Washington : Radio Technical Commission for Aeronautics (RTCA), 2014. - p. 88. - SC-216.
- RTCA DO-330** Software Tool Qualification Considerations [Report] : Standard. - [s.l.] : Radio Technical Commission for Aeronautics, 2011.
- RTCA DO-331** Model-Based Development and Verification Supplement to DO-178C and DO-278A [Report] : Standard. - [s.l.] : Radio Technical Commission for Aeronautics, 2011. - SC-205.
- RTCA DO-332** Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A [Report] : Standard. - [s.l.] : Radio Technical Commission for Aeronautics, 2011.
- RTCA DO-333** Formal Methods Supplement to DO-178C and DO-278A [Report] : Standard. - Washington : Radio Technical Commission for Aeronautics, 2011. - p. 118. - SC-205.
- RTCA DO-355** Information Security Guidance for Continuing Airworthiness [Report] : Standard. - Washington : Radio Technical Commission for Aeronautics (RTCA), 2014. - p. 78. - SC-216.
- RTCA DO-356** Airworthiness Security Methods and Considerations [Report] : Standard. - Washington : Radio Technical Commission for Aeronautics (RTCA), 2014. - SC-216.
- Rudolph Manuel and Schwarz Reinhard** A Critical Survey of Security Indicator Approaches [Conference] // 7th International Conference on Availability, Reliability and Security (ARES). - Prague : IEEE, 2012. - pp. 291-300. - DOI: 10.1109/ARES.2012.10.
- Rushby John** Critical properties: survey and taxonomy [Report] / Computer Science Laboratory; SRI International. - Menlo Park : [s.n.], 1994. - CSL-93-01.
- Rushby John** Kernels for Safety? [Book Section] // Safe and Secure Computing Systems / book auth. Anderson T.. - [s.l.] : Blackwell Scientific Publications, 1989.
- Rushby John** Noninterference, transitivity and channel-control security policies [Report] : Technical Report. - [s.l.] : Computer Science Laboratory, SRI International, 1992.
- Rushdi Ali Muhammad and Ba-Rukab Omar M.** A doubly-stochastic fault-tree assessment of the probabilities of security breaches in computer systems [Book Section] // Proceedings of the 2nd Saudi Science Conference. - 2004. - Vol. 4.
- Rushdi Ali Muhammad and Ba-Rukab Omar M.** Fault-tree modelling of computer system security [Journal] // International Journal of Computer Mathematics. - 2005. - Vol. 82. - pp. 805-819. - DOI: 10.1080/00207160412331336017.
- S + IEC 61508** Functional safety of electrical / electronic / programmable electronic safety-related systems [Report] : Standard. - [s.l.] : International Electrotechnical Commission, 2010. - p. 1000. - Ed2.0.
- Sadvandi Sara, Chapon Nicolas and Piètre-Cambacédès Ludovic** Safety and Security Interdependencies in Complex Systems and SoS: Challenges and Perspectives [Book Section] // Complex Systems Design and Management (CSDM) / book auth. Hammami O., Krob D. and Voirin J.-L.. - [s.l.] : Springer Berlin Heidelberg, 2012. - DOI: 10.1007/978-3-642-25203-7_16.
- SAE ARP 4754A** Guidelines for Development of Civil Aircraft and Systems [Report] : Standard / Aerospace Recommended Practice (ARP). - [s.l.] : Society of Automotive Engineers (SAE) International, 2010.
- SAE ARP 4761A** Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment [Report] / Aerospace Recommended Practice (ARP). - [s.l.] : Society of Automotive Engineers (SAE) International, 2004. - p. 170.
- Saglietti Francesca** Common Analysis and Verification Techniques for Safety- and Security- Critical Software Systems [Conference] // The Relationship between Safety and Security in Software-Based Systems, SafeComp Workshop. - 2008.
- Sallhammar Karin, Helvik Bjarne E. and Knapskog Svein J.** Towards a Stochastic Model for Integrated Security and Dependability Evaluation [Conference] // First International Conference on Availability, Reliability and Security. - Washington : IEEE, 2006. - pp. 156-165. - DOI: 10.1109/ARES.2006.137.
- Schaefer Robert M.** Technology—safety and security [Book Section] // Addressing Contemporary Campus Safety Issues. New Directions for Student Services. - [s.l.] : Wiley Periodicals, 2002. - Vol. 2002. - DOI: 10.1002/ss.63.
- Schmittner Christoph [et al.]** A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems [Conference] // 1st ACM Workshop on Cyber-Physical System Security (CPSS). - New York : ACM, 2015a. - pp. 69-80. - DOI: 10.1145/2732198.2732204.
- Schmittner Christoph [et al.]** Security Application of Failure Mode and Effect Analysis (FMEA) [Conference] // 33rd International Conference on Computer Safety, Reliability and Security (SafeComp) / ed. Bondavalli Andrea and Giandomenico Felicita Di. - Florence : Springer, 2014b. - DOI: 10.1007/978-3-319-10506-2_21.
- Schmittner Christoph and Ma Zhendong** Towards a Framework for Alignment Between Automotive Safety and Security Standards [Conference] // EWICS/ERCIM/ARTEMIS Dependable Cyber-physical Systems and

Systems-of-Systems Workshop (DECSoS) / ed. Koornneef Floor and Gulijk Coen van. - Delft : Springer International Publishing Switzerland, 2015b. - Vol. LNCS 9338. - pp. 133–143. - DOI: 10.1007/978-3-319-24249-1_12.

Schmittner Christoph, Ma Zhendong and Gruber Thomas Standardization Challenges for Safety and Security of Connected, Automated and Intelligent Vehicles [Conference] // 3rd International Conference on Connected Vehicles & Expo (ICCVE). - Vienna : [s.n.], 2014c.

Schmittner Christoph, Ma Zhendong and Smith Paul FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles [Conference] // 1st International Workshop on the Integration of Safety and Security Engineering (ISSE), 33rd International Conference on Computer Safety, Reliability and Security (SafeComp) / ed. Bondavalli Andrea, Ceccarelli Andrea and Ortmeier Frank. - Florence : Springer, 2014a. - pp. 282–288. - LNCS 8696. - DOI: 10.1007/978-3-319-10557-4_31.

Schneider Daniel Runtime certification of safety and security in cyber-physical system [Conference] // 1st Workshop on Safety & Security. - Kaiserslautern : [s.n.], 2014. - Slides only..

Schoitsch Erwin Design for safety and security of complex embedded systems: a unified approach [Book Section] // Cyberspace Security and Defense: Research Issues, NATO Science Series II: Mathematics, Physics and Chemistry / book auth. Kowalik J., Gorski J. and Sachenko A.. - [s.l.] : Springer Netherlands, 2005. - Vol. 196. - DOI: 10.1007/1-4020-3381-8_9.

Schoitsch Erwin Safety and security – what about a joint process? [Conference] // 1st Workshop on Safety & Security. - Kaiserslautern : [s.n.], 2014. - p. 37. - Slides only.

Schwarz Reinhard and Schneider Daniel Workshop Debriefing [Conference] // 1st IESE Workshop on Safety and Security. - Kaiserslautern : [s.n.], 2014. - p. 10. - Slides only.

Schwarz Reinhard My thoughts on safety and security metrics [Conference] // 1st IESE Workshop on Safety and Security. - Kaiserslautern : [s.n.], 2014. - Slides only.

SEISES Cooperative Projects [Online] // Aerospace Valley. - FUI, 2008. - 21 05 2014. - <http://www.aerospace-valley.com/les-projets?keywords=seises>. - In French.

SeSaMo D2.1 Specification of Safety and Security Mechanisms [Report]. - [s.l.] : Security and Safety Modelling, Artemis JU Project Grant Agreement no.: 295354, 2013.

SeSaMo D3.1 Specification of Safety and Security Analysis and Assessment Techniques [Report]. - [s.l.] : Security and Safety Modelling, Artemis JU Project Grant Agreement no.: 295354, 2013.

SeSaMo D4.1 Integrated Design and Evaluation Methodology [Report]. - [s.l.] : Security and Safety Modelling, Artemis JU Project Grant Agreement no.: 29535, 2014.

SeSaMo Security and Safety Modelling [Online]. - 2012. - 20 05 2014. - <http://sesamo-project.eu/>.

Simpson Andrew, Woodcock Jim and Davies Jim Safety through Security [Book Section] // IWSSD'98 Proceedings of the 9th international workshop on Software specification and design / ed. Society IEEE Computer. - Washington : [s.n.], 1998. - ISBN:0-8186-8439-9.

Sindre Guttorm A look at misuse cases for safety concerns [Book Section] // Situational Method Engineering: Fundamentals and Experiences / book auth. Ralyt'e9 J., Brinkkemper S. and Henderson-Sellers B. / ed. Boston Springer. - [s.l.] : IFIP International Federation for Information Processing, 2007. - Vol. 244. - DOI: 10.1007/978-0-387-73947-2_20.

Smith J., Russell S. and Looi M. Security as a Safety Issue in Rail Communications [Book Section] // Proceedings of SCS'03, 8th Australian Workshop on Safety Critical Systems and Software, Canberra, October 9-10, 2003 / ed. Australian Computer Society Inc.. - Darlinghurst : ACM, 2003. - Vol. 33. - ISBN:1-920-68215-5.

Sommerville Ian An Integrated Approach to Dependability Requirements Engineering [Book Section] // Current Issues in Safety-Critical Systems / book auth. Redmill Felix and Anderson Tom / ed. Springer. - London : [s.n.], 2003. - DOI: 10.1007/978-1-4471-0653-1_1.

Sørby Karine Relationship between security and safety in a security-safety critical system: Safety consequences of security threats [Report] : Master Thesis. - Trondheim, Norway : Norwegian University of Science and Technology (NTNU), 2003. - p. 185.

Srivatanakul Thitima Security Analysis with Deviational Techniques [Report] : PhD. Thesis. - York : University of York, Department of Computer Science, 2005. - p. 279.

Srivatanakul Thitima, Clark John A. and Polack Fiona Effective Security Requirements Analysis: HazOp and Use Cases [Book Section] // Information Security, Lecture Notes in Computer Science / book auth. Zhang K. and Zheng Y.. - Berlin / Heidelberg : Springer, 2004. - Vol. 3225.

Stålthane Tor and Sindre Guttorm Safety Hazard Identification by Misuse Cases: Experimental Comparison of Text and Diagrams [Book Section] // Model Driven Engineering Languages and Systems, Lecture Notes in Computer Science / book auth. Czarnecki K. [et al.]. - [s.l.] : Springer Berlin Heidelberg, 2008. - Vol. 5301.

Stavridou V. and Dutertre B. From Security to Safety and Back [Book Section] // Computer Security, Dependability and Assurance: From needs to Solutions. Proceedings / ed. IEEE. - York : [s.n.], 1998. - DOI: 10.1109/CSDA.1998.798365.

Steiner Max and Liggesmeyer Peter Combination of Safety and Security Analysis - Finding Security Problems that Threaten the Safety of a System [Conference] // ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems (DECS), 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP). - 2013.

Stephenson Peter Information security in 2014: Another year of big events [Online] // Reviews. - SC Magazine, 8 12 2014. - 12 12 2014. - <http://www.scmagazine.com/information-security-in-2014-another-year-of-big-events/article/384497/>.

Stoneburner G. Toward a Unified Security-Safety Model [Book Section]. - [s.l.] : IEEE Computer, 2006. - Vol. 39.

Subramanian Nary and Zalewski Janusz Assessment of Safety and Security of System Architectures for Cyberphysical Systems [Conference] // International Systems Conference (SysCon). - Orlando, FL : IEEE, 2013. - pp. 634 - 641. - DOI: 10.1109/SysCon.2013.6549949.

Subramanian Nary and Zalewski Janusz Quantitative Assessment of Safety and Security of System Architectures for Cyberphysical Systems Using the NFR Approach [Journal] // IEEE Systems Journal / ed. IEEE. - 09 01 2014. - 99 : Vol. PP. - pp. 1-13. - DOI: 10.1109/JSYST.2013.2294628.

Sun Mu [et al.] Addressing Safety and Security Contradictions in Cyber-Physical Systems [Conference] // 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW). - Newark : US Department of Homeland Security, 2009. - http://cimic.rutgers.edu/positionPapers/cpssecurity09_MuSun.pdf.

Sysgo PikeOS Hypervisor [Online]. - 2014. - 16 12 2014. - <http://www.sysgo.com/products/pikeos-rtos-and-virtualization-concept/>.

Taguchi Kenji, Souma Daisuke and Nishihara Hideaki Safe & Sec Case Patterns [Conference] // 3rd International Workshop on Assurance Cases for Software-Intensive Systems (ASSURE) / ed. Koorneef Floor and Gulijk Coen van. - Delft : Springer International Publishing Switzerland, 2015. - Vol. LNCS 9338. - pp. 27–37. - DOI: 10.1007/978-3-319-24249-1_3.

Taylor Carol, Alves-Foss Jim and Rinker Bob Merging Safety and Assurance: the Process of Dual Certification of Software [Conference] // Software Technology Conference. - 2002b.

Taylor Carol, Alves-Foss Jim and Rinker Bob Towards Common Criteria Certification for DO-178B: Executive Summary [Online] // University of Idaho, Department of Computer Science, Jim Alves-Foss, Recent Publications and Presentations. - Center for Secure and Dependable Systems, 03 2002a. - 10 07 2014. - <http://www2.cs.uidaho.edu/~jimaf/papers/compare02a.pdf>.

TCSEC Trusted Computer System Evaluation Criteria [Report] : Standard. - [s.l.] : Department of Defense, 1985. - p. 116. - Available: <http://csrc.nist.gov/publications/history/dod85.pdf>. - DoD 5200.28-STD.

Tiwari Ashish [et al.] Safety Envelope for Security [Conference] // 3rd international conference on High Confidence Networked Systems (HiCoNS). - Berlin : ACM Digital Library, 2014. - pp. 85-94. - <http://www.csl.sri.com/users/tiwari/papers/hicons14.pdf>. - DOI: 10.1145/2566468.2566483.

TÜV Rheinland Home page [Online]. - 2015. - 28 05 2015. - <http://www.tuv.com/en/corporate/home.jsp>.

Tverdyshev Sergey MILS – Architecture for Safety and Security [Conference] // 1st workshop on safety and security. - Kaiserslautern : [s.n.], 2014. - Slides only.

ViERforES Safely into the Future with Reliable Technology [Online] // Fraunhofer Institute for Factory Operation and Automation (IFF). - 2008. - 04 07 2014. - <http://www.iff.fraunhofer.de/en/research-network/vierfores.html>.

Viswanathan Shekar Master of Science in Homeland Security and Emergency Management [Online] // National University. - <http://www.nu.edu/OurPrograms/SchoolOfEngineeringAndTechnology/AppliedEngineering/Programs/720-818.html>.

Vogt Roland Safety / security conflicts in large system architectures [Conference] // 1st Workshop on Safety and Security. - Kaiserslautern : [s.n.], 2014. - Slides only.

Vouk Mladen A. Differences and Similarities between Software Reliability and Software Security Engineering [Conference] // Software Reliability in 2013: Theory & Practice. - Levallois-Perret : IEEE-RS, 2013.

Ward David, Ibarra Ileri and Ruddle Alastair Threat Analysis and Risk Assessment in Automotive Cyber Security [Conference] // SAE World Congress & Exhibition. - [s.l.] : SAE Int., 2013. - DOI:10.4271/2013-01-1415.

Weiss Joseph Protecting Industrial Control Systems from Electronic Threats [Book]. - New York : Momentum Press, 2010. - ISBN: 978-1-60650-197-9.

Wiander Timo Positive and Negative Findings of the ISO/IEC 17799 Framework [Conference] // Proceedings of the 18th Australasian Conference on Information Systems (ACIS). - Toowoomba : AIS Electronic Library (AISeL), 2007. - Paper 75..

Wikipedia Medical Device Medical device [Online]// Wikipedia. - 01 09 2014. - 06 10 2014. - http://en.wikipedia.org/wiki/Medical_device#cite_note-4.

Wind River VxWorks [Online]. - 2015. - 06 03 2015. - <http://www.windriver.com/products/vxworks/>.

Winther Rune Qualitative and Quantitative Analysis of Security in Safety and Reliability Critical Systems [Book Section] // Probabilistic Safety Assessment and Management / ed. Schmocker Cornelia Spitzer . Ulrich and Dang Vinh N.. - London : Springer, 2004. - Vol. 6. - DOI: 10.1007/978-0-85729-410-4_377.

Winther Rune, Johnsen Ole-Arnt and Gran Bjørn Axel Security assessments of safety critical systems using HAZOPs [Book Section] // SafeComp'01 Proceedings of the 20th International Conference on Computer Safety, Reliability and Security / ed. Springer-Verlag. - London : [s.n.], 2001. - ISBN:3-540-42607-8.

Woskowski Christoph A Pragmatic Approach towards Safe and Secure Medical Device Integration [Conference] // 33rd International Conference on Computer Safety, Reliability, and Security (SAFECOMP) / ed. Bondavalli Andrea and Giandomenico Felicita Di. - Florence : Springer International Publishing, 2014. - Vol. LNCS 8666. - pp. 342-353. - DOI: 10.1007/978-3-319-10506-2_23.

Yang Lili and Yang S. H. A Framework of Security and Safety Checking for Internet-Based Control Systems [Journal] // Int. J. Information and Computer Security. - 2007. - 1/2 : Vol. 1. - pp. 185-200.

Young William and Leveson Nancy G. Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory [Article]// Communications of the ACM. - 2014. - 2 : Vol. 57. - pp. 31-35. - DOI: 10.1145/2556938.

YVL A.11 Security of a nuclear facility [Report] : Standard. - Helsinki : Radiation and Nuclear Safety Authority (STUK), 2013. - p. 32. - http://www.finlex.fi/data/normit/41951-YVL_A.11e.pdf. - ISBN: 978-952-309-065-1.

YVL A.12 Information security management of a nuclear facility [Report] : Standard. - Helsinki : Radiation and Nuclear Safety Authority (STUK), 2013. - p. 12. - http://www.finlex.fi/data/normit/41822-YVL_A.12e.pdf. - ISBN: 978-952-309-068-2.

Zhenhai Zhang, Xiaoming Wang and Yanpeng Zhang Study of Service-Oriented Framework of Information Integration of Safety and Security for High-speed Railway [Conference]// International Conference on Information Networking and Automation (ICINA). - Kunming : IEEE, 2010. - pp. V2-307 - V2-311 . - 10.1109/ICINA.2010.5636504.

8 Acronyms

Term/ abbreviation	Explanation
A	Action
AADL	Architecture Analysis and Design Language
ADO	Delivery and Operation
AFRL	Air Force Research Laboratory
AGD	Guidance Documents
ALARP	As Low As Reasonably Practicable
AMC	Acceptable Means of Compliance
ANS	Air Navigation Service
ARE	Admiralty Research Establishment
ARM	ARgument Meta-model
AT	Attack Tree
AVA	Vulnerability Assessment
AVATAR	Automated Verification of reAl Time softwARe
BACS	Building Automation and Control System
BBN	Bayesian Belief Network
BDMP	Boolean logic Driven Markov Process
BEV	Battery-Electric Vehicles
CAA	Civil Aviation Authority
CAE	Claims-Argument-Evidence
CC	Common Criteria
CENELEC	Committee for Electro-technical Standardization
CFT	Component Fault Tree
CHASSIS	Combined Harm Assessment for Safety and Security of Information Systems
CHAZOP	Control HAZard and OPerability
CIA	Confidentiality, Integrity and Availability
CLM	Component Logic Model
CLUSIF	French Cyber-Security Club (In French: Club de la Sécurité de l'Information Français)
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and related Technology
CoP	Chain of Protection
CPS	Cyber-Physical System
CR	Critical Resource
CS	Computer System

CS	Certification Specifications
CWE	Common Weakness Enumeration
D	Defence
DAH	Design Approval Holder
DAL	Development Assurance Level
DAR	Decision, Analysis and Resolution
DARPA	Defense Advanced Research Project Agency
DDQS	Design, Develop and Qualify the Solution
D-MUC	Diagrammatical Misuse Case
DoD	Department of Defence
DoS	Denial of Service
DRA	Defence Research Agency
E/E/PE	Electrical / Electronic / Programmable Electronic
EAL	Evaluation Assurance Level
EASA	European Aviation Safety Agency
EFT	Extended Fault Tree
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EWICS	European Workshop on Industrial Computer Systems Reliability, Safety and Security
F	Failure
FA	Free Agent
FAA	Federal Aviation Authority
FAR	Federal Aviation Regulation
FCV	Fuel-Cell Vehicle
FDA	Food and Drug Administration
FHA	Functional Hazard Analysis
FMEA	Failure Mode and Effect Analysis
FPTC	Failure Propagation and Transformation Calculus
FSD	Failure Sequence Diagram
FT	Fault Tree
GEMS	Generic Error-Modelling System
GM	Guidance Material
GPP	General Purpose Processor
GSN	Goal Structuring Notation
GWV	Greve, Wilding, and Vanfleet
H	Harm
HACMS	High-Assurance Cyber Military Systems

HazOp	HAZard and OPerability
HEV	Hybrid Electric Vehicles
HLR	High-Level Requirement
I&C	Instrumentation and Control
IACS	Industrial Automation and Control System
IAEA	International Atomic Energy Agency
iCMM	integrated Capability Maturity Model
ICAO	International Civil Aviation Organisation
ICS	Industrial Control System
IDS	Intrusion Detection System
IMA	Integrated Modular Avionics
INCOSE	International Council on System Engineering
IoT	Internet of Things
ISR	Instruction Set Randomization
KUL	Katholieke Universiteit Leuven
LLR	Low-Level Requirement
LOPA	Layer-Of-Protection Analysis
LSP	Liskov Substitutability Principle
MAFTIA	Malicious-and Accidental-Fault Tolerance for Internet Applications
MCS	Machine-Control Systems
MCS	Minimal Cut Set
MILS	Multiple Independent Levels of Security (obsolete)
MLS	Multiple Levels of Security
MOD	Ministry of Defence (UK)
MSC	Minimal Sufficient Condition
MUSD	Misuse Sequence Diagram
NFR	Non-Functional Requirement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
O	Operator
OE	Operational Environment
OMG	Object Management Group
ONERA	Office National d'Études et de Recherches Aérospatiales (The French Aerospace Lab)
OS	Operating System
OSI	Open Systems Interconnection
P	Probability
PP	Protection Profile
PSM	Practical Software and Systems Measurement

PSSA	Preliminary System Security Assessment
R	Rating
RAE	Requirements Analysis and Elicitation
RESS	Rechargeable Energy Storage System
RFT	Request For Tender
RTCA	Radio Technical Commission for Aeronautics
S	Secret
SACM	Structured Assurance Case Meta-model
SAEM	Software Assurance Evidence Meta-model
SAM	Safety Assessment Methodology
SAT	Satisfiability
SaTrAp	Safety Traceability Approach
SCA	Software Communication Architecture
SCIS	Software-intensive Critical Information Systems
SDR	Software Defined Radio
SeCM	Security Conceptual Model
SEISES	Secured and Safe IT Embedded Systems
SEMA	System vs. Environment & Malicious vs. Accidental
SIL	Safety Integrity Level
SIS	Safety Interlock System
SL	Security Level
SL	Single Level (of Security)
SMT	Satisfiability Modulo Theory
SoS	System of Systems
SQUALE	Security, Safety and Quality Evaluation for Dependable Systems
STAMP	System-Theoretic Accident Model and Processes
STUK	Radiation and Nuclear Safety Authority (of Finland)
TCS	Thales Communications & Security
TEPE	TEmporal Property Expression
T-MUC	Textual Misuse Cases
ToE	Target of Evaluation
TRT	Thales Research & Technology
TS	Top Secret
TSF	Target of Evaluation Security Function
TSFI	TSF Interface
TVRA	Threat, Vulnerability and Risk Assessment
TTOOL	TURTLE Tool
VIA	Vulnerability Identification and Analysis

9 Appendixes

These appendixes provide extended descriptions of some of the key referenced documents, as discussed in the state of the art.

9.1 Airworthiness Security Process Specification

The Airworthiness Security Process Specification (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014) is a resource for Airworthiness Authorities (AA) and the aviation industry for certification when the development or modification of aircraft systems and the effects of intentional unauthorized electronic interaction can affect aircraft safety. It deals with the activities that need to be performed in support of the airworthiness process when it comes to the threat of intentional unauthorized electronic interaction (the “What”).

The Airworthiness Security Risk Management Framework (cf. Figure 136) is composed of three major parts. First the dedicated Certification Activities (steps 1 and 7) to manage the certification process itself. Second, the Security Risk Assessment related activities (steps 2, 3 and decision gate 4) to evaluate risk based upon identified threat scenarios to determine acceptability and to assess the implemented security. Finally the acceptability of the risk (decision gate 4) will determine the role of third part, the Security Development related activities (steps 5 and 6) to implement the require security measures.

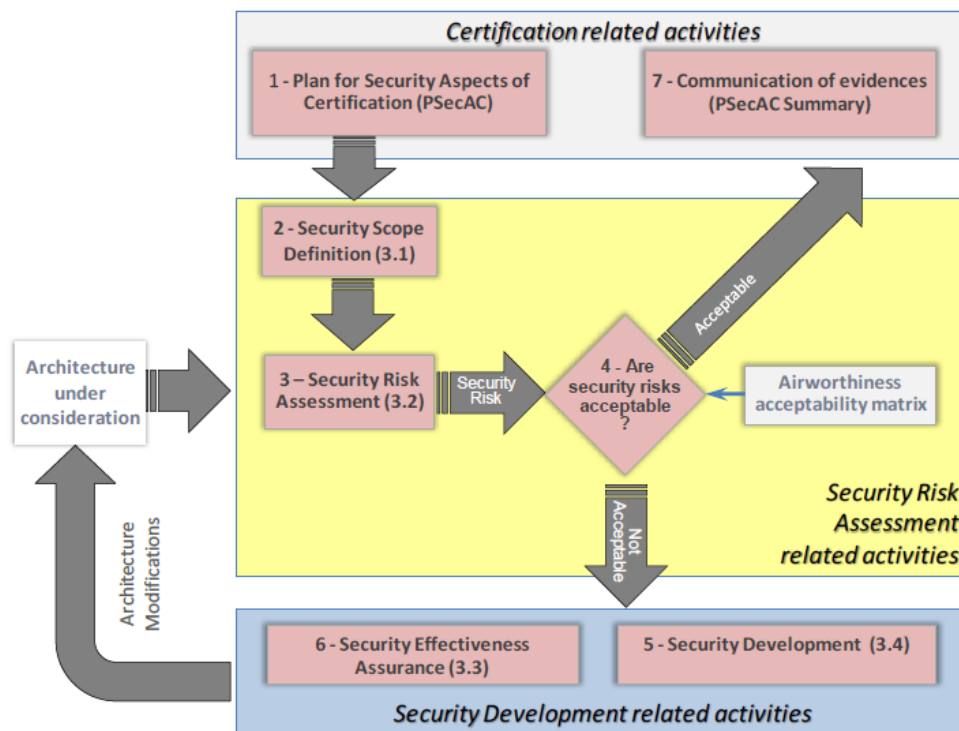


Figure 136: Airworthiness Security Risk Management Framework (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)

We find here some communality with the (ISO/IEC 27005, 2011). Thus Step 2, Security Scope Definition, is equivalent to (ISO/IEC 27005, 2011) Context Establishment. Step 3, Security Risk Assessment, is equivalent to (ISO/IEC 27005, 2011) Risk Assessment, and Steps 5 and 6 are equivalent to (ISO/IEC 27005, 2011) Risk Treatment).

In the Airworthiness Security Process Framework, the Security Risk Assessment related activities may be performed at two levels of development: aircraft and system. They are organized according to the following breakdown:

- at aircraft level:

- Aircraft Security Scope Definition (ASSD),
- Preliminary Aircraft Security Risk Assessment (PASRA),
- Aircraft Security Risk Assessment (ASRA);
- at system level:
 - System Security Scope Definition (SSSD),
 - Preliminary System Security Risk Assessment (PSSRA),
 - System Security Risk Assessment (SSRA).

The Security Development related activities support the implementation of the security measures to mitigate the risks identified by Security Risk Assessment. They are organized according to the following breakdown (cf. Figure 137) and are described in details (i.e. purpose, details, input, output, compliance of objectives) in Appendix A of the standard:

- at aircraft level:
 - Aircraft Security Architecture and Measures (ASAM),
 - Aircraft Security Operator Guidance (ASOG),
 - Aircraft Security Verification (ASV);
- at system level:
 - System Security Architecture and Measures (SSAM),
 - System Security Integrator Guidance (SSIG),
 - System Security Verification (SSV).

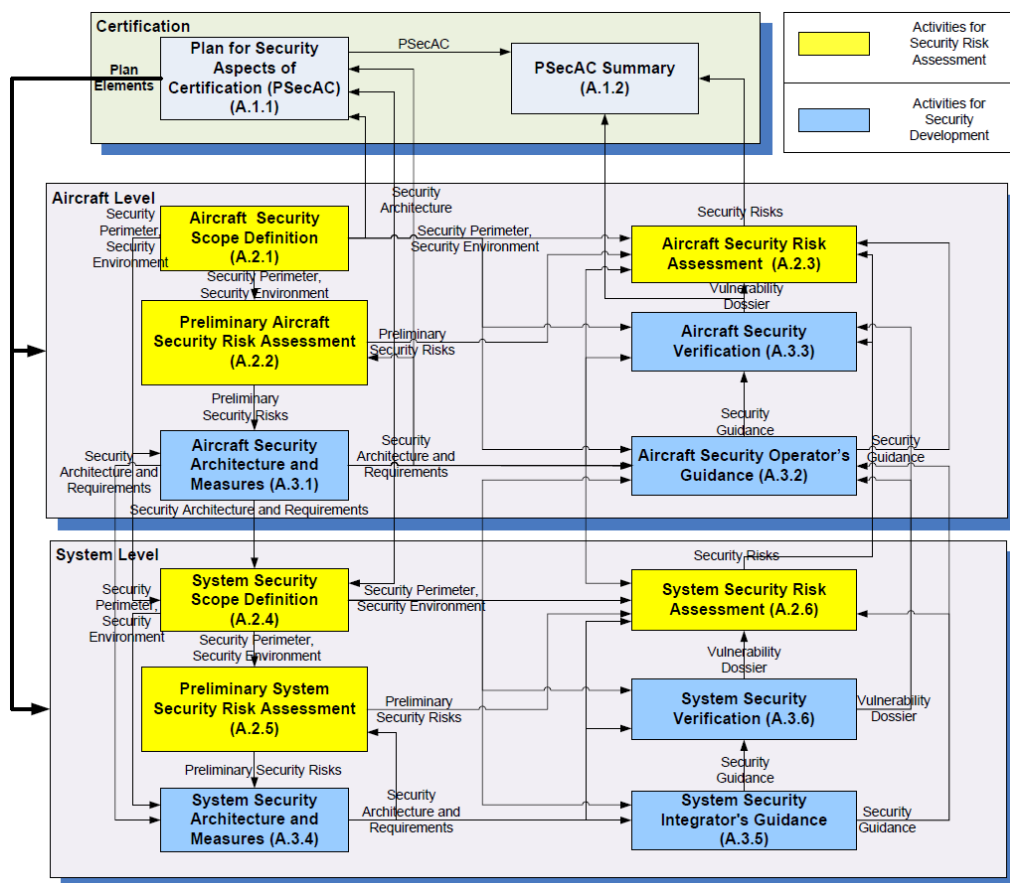


Figure 137: Airworthiness Security Process Activities (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)

The Airworthiness Security Process Activities as proposed in (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014) and pictured above represent a significant update, cf. Figure 138, with the previous release of the standards, i.e. (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010). The changes are extensively discussed in (Joyce, et al., 2014).

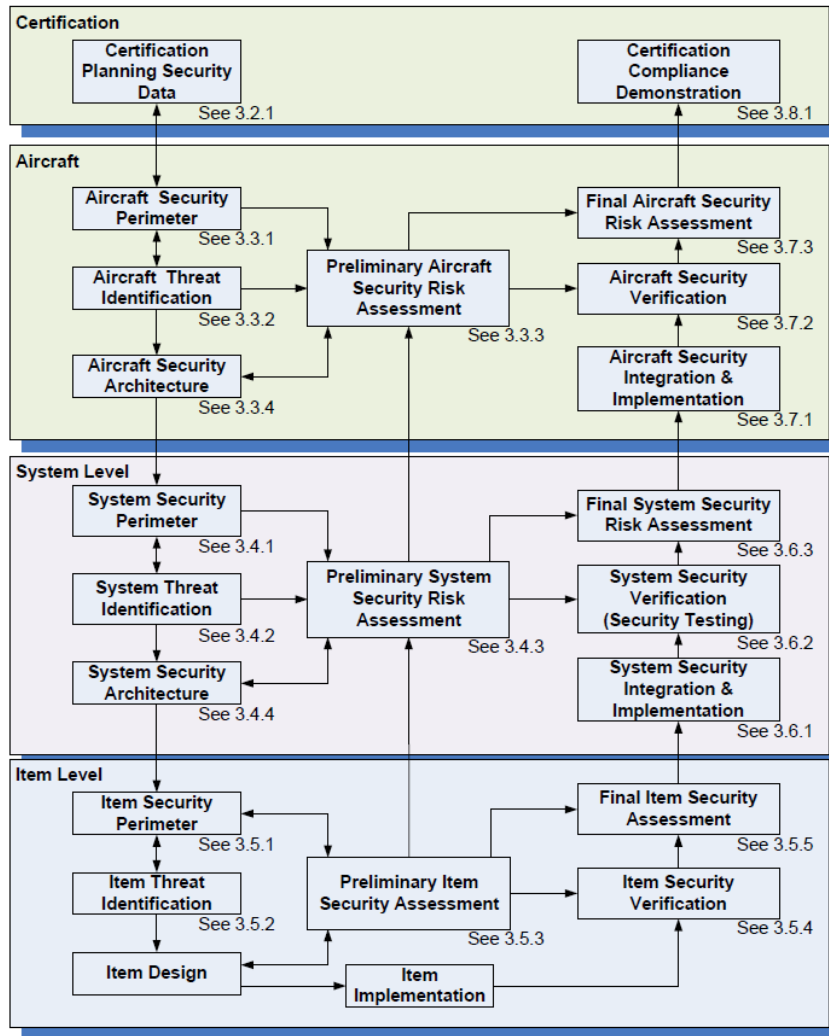


Figure 138: Obsolete generic airworthiness security activities as per (EUROCAE ED-202, 2010) / (RTCA DO-326, 2010)

The Security Risk Assessment related activities interact with the Safety Assessment process to manage the added environment risk to aircraft when it is exposed to the threat of unauthorized interaction (cf. Figure 139).

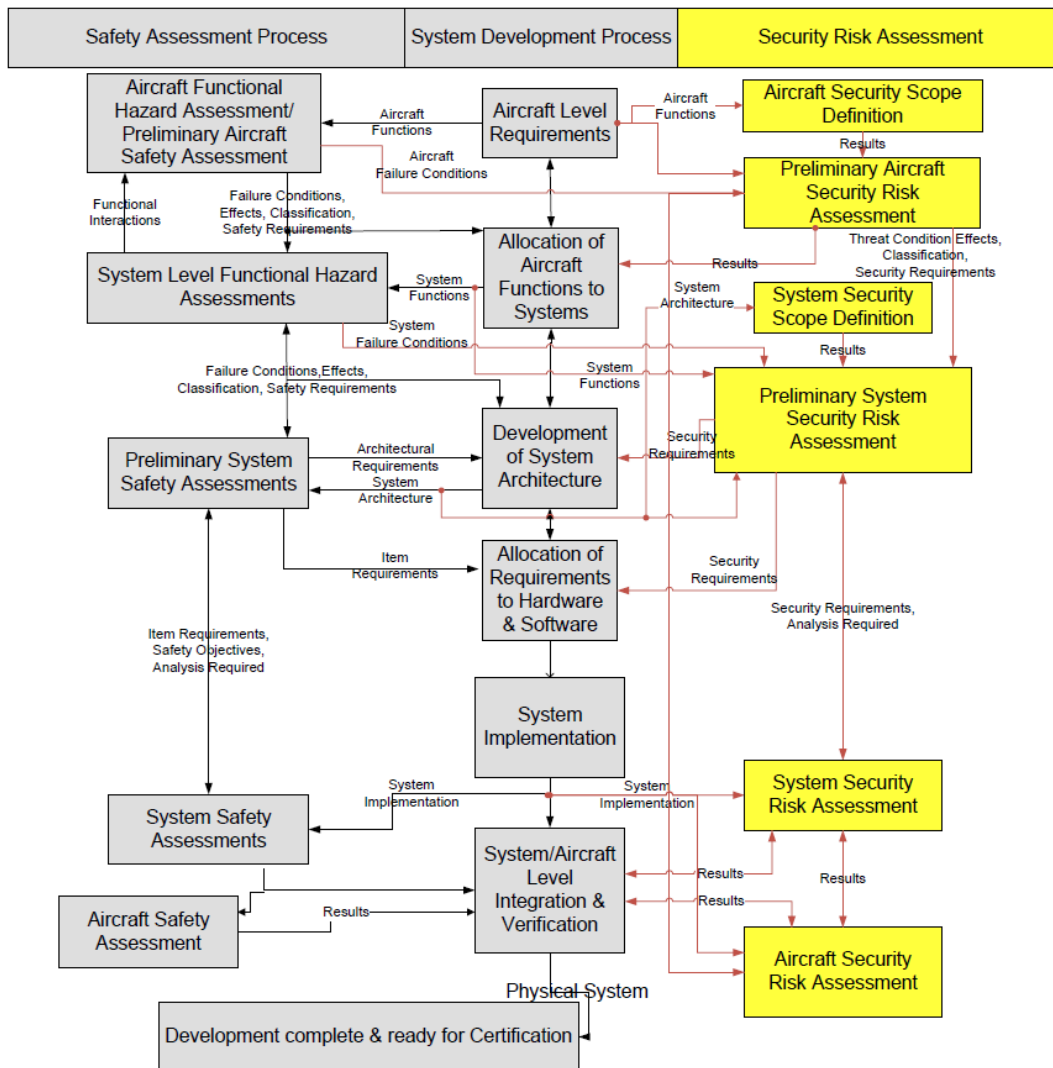


Figure 139: Airworthiness Security Process as Part of Aircraft Certification Process (RTCA DO-326, 2010) / (SAE ARP 4754A, 2010) / (EUROCAE ED-79A, 2010)

The (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014) standards specify in details three fundamental concepts which are related to establishing the security scope: security risk assessment, security effectiveness and security development activities. Figure 140 gives more information about the approach recommended to assess the security risk of a threat scenario.

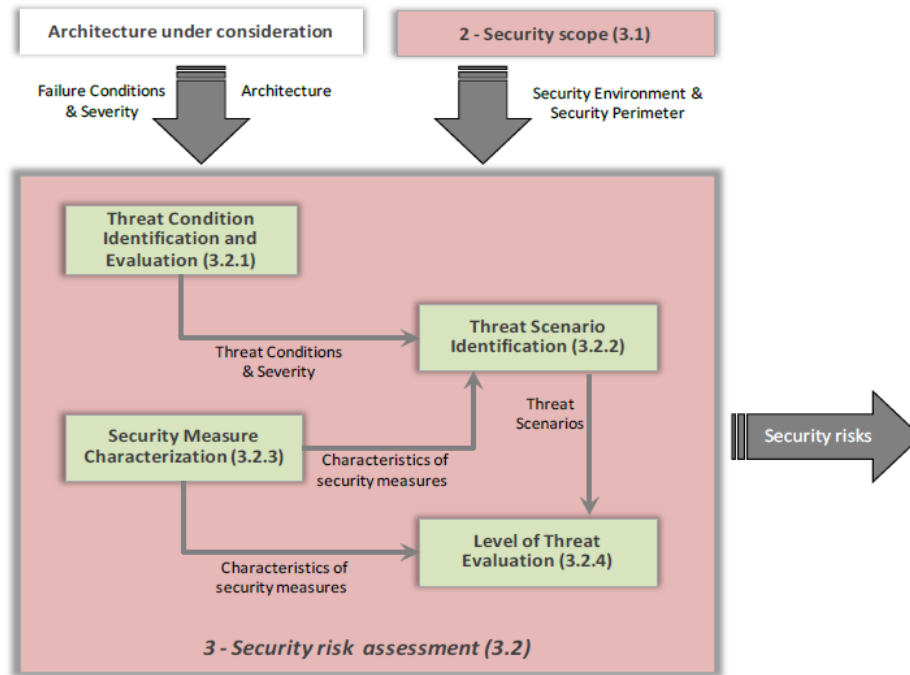


Figure 140: Security Risk Assessment (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)

Threat conditions are evaluated by the loss of security attributes of an asset as described in Figure 141.

Asset Security Attribute	Threat Conditions of the System due to the loss of the Asset's Security Attribute (non-exhaustive)
Integrity	Conditions representing misuse or interference with the Function
Availability	Conditions representing denial of access to the Function, including intermittent failures in the continuity of data over a required service interval.
Confidentiality	Conditions resulting from exposure of data to an unauthorized entity.

Figure 141: Asset Security Attributes and Threat Conditions (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)

The security effectiveness is supported by a subset of activities inside each part of the Airworthiness Security Process, as shown in Figure 142.

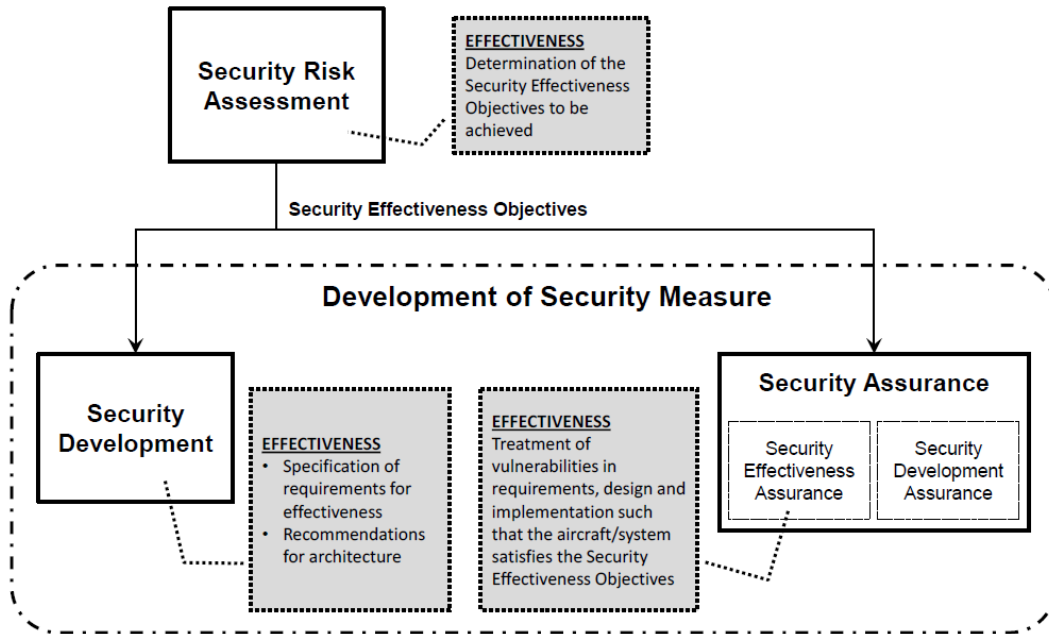


Figure 142: Asset Security Effectiveness for the Airworthiness Security Process (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)

The security development activities should highlight the following topics:

- security architecture,
- security measures,
- security guidance,
- security verification.

As shown in Figure 143 the types of measures include, but are not limited to: deterrent, preventive, detective, corrective, restorative/recovery measures.

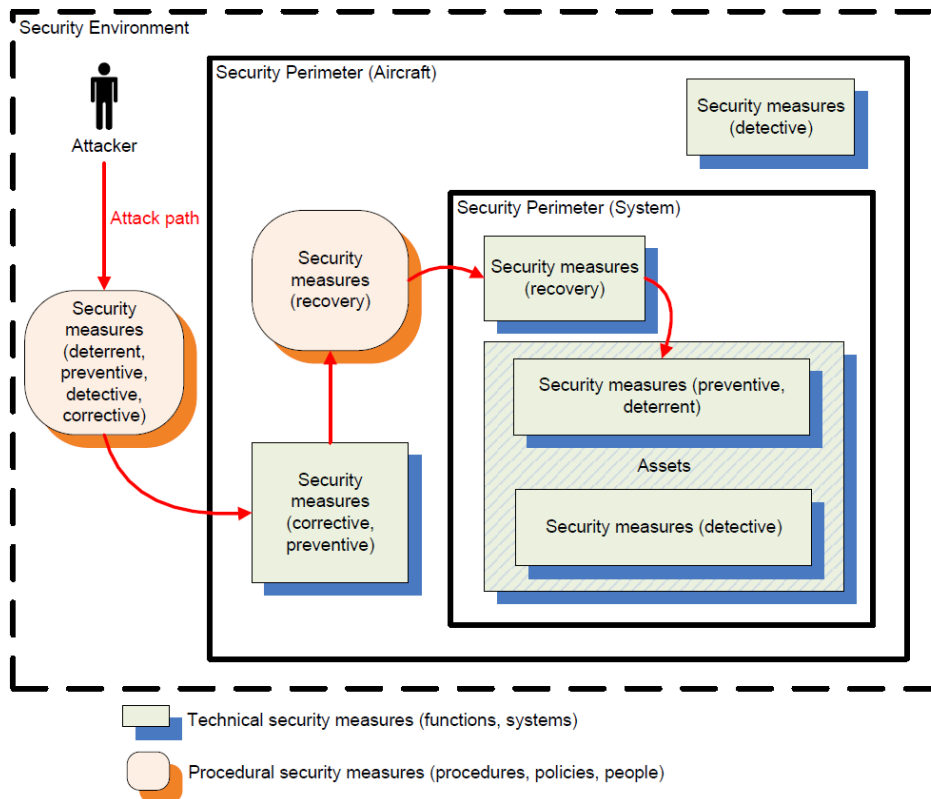


Figure 143: Simplified example of a security architecture with different types of technical and procedural security measures (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)

Security verification includes analysis and three kinds of testing: security requirements tests, security robustness tests and vulnerability tests. Figure 144 illustrates the security testing organization with its inputs and how it contributes to the required outputs.

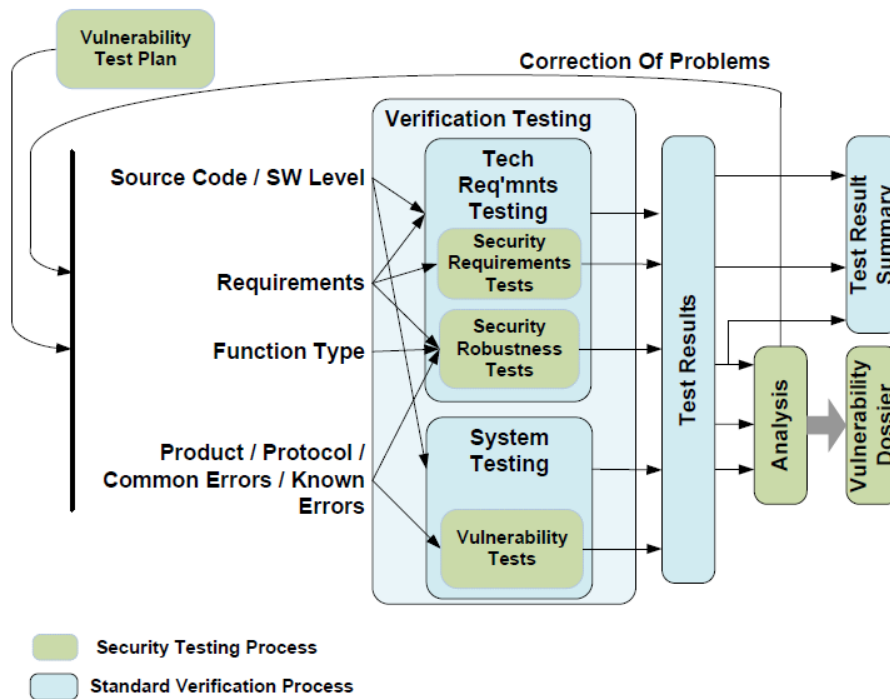


Figure 144: Security Testing Activities (EUROCAE ED-202A, 2014) / (RTCA DO-326A, 2014)

In chapter 4, the Airworthiness Security Process Specification also introduces modifications to aircraft and systems and provides guidance to determine when aircraft level / system level Security Risk Assessment is required.

9.2 Airworthiness Security Methods and Considerations

The Airworthiness Security Methods and Considerations standard (RTCA DO-356, 2014) gives guidelines to be compliant with the security process of the (RTCA DO-326A, 2014) / (EUROCAE ED-202A, 2014) and introduces specific methods for analysing the security risk through threat trees, and for defining security network domains.

An overview of the topics covered by the (RTCA DO-356, 2014) is given in the Figure 145 hereafter.

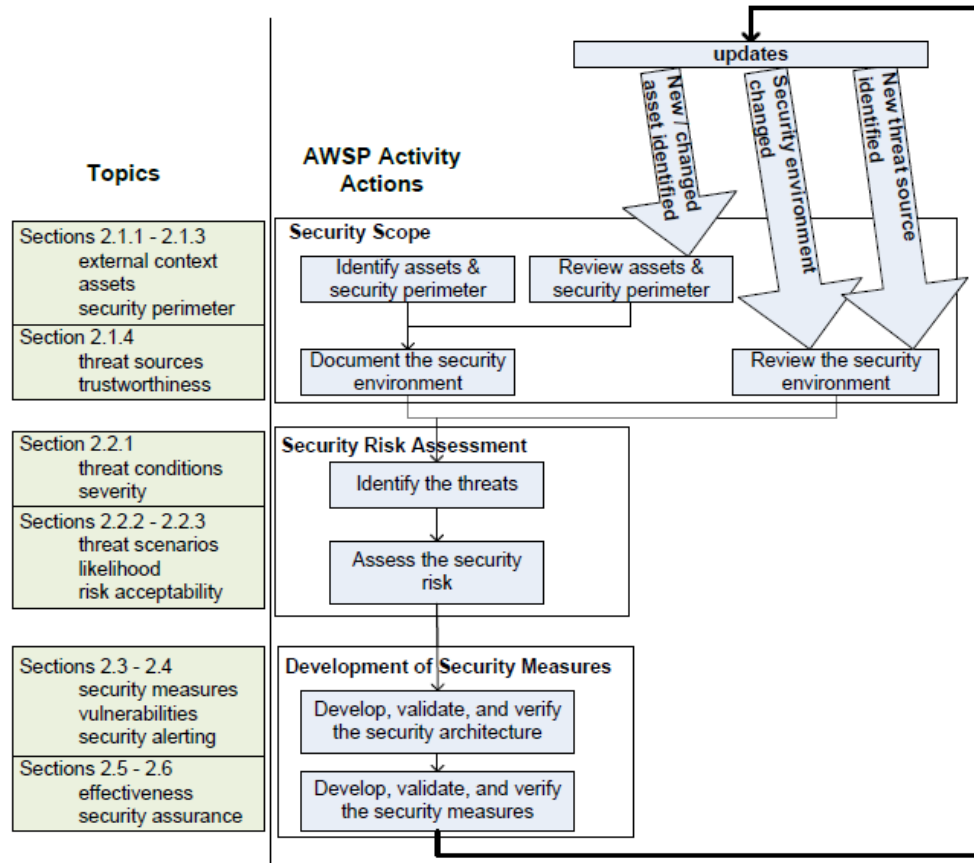


Figure 145: Overview of Airworthiness Security Process Topics (RTCA DO-356, 2014)

More specifically, for describing the system security scope the following activities must be performed:

- identify assets and specify their security perimeters;
- describe all physically accessible open system ports, slots, and wireless on the aircraft, including: connections within the aircraft for use by: passenger devices, cabin and flight crew devices, and maintenance and product support devices;
- describe all digital connections and digital data communications with ground systems;
- summarize physical digital connections to other aircraft systems (in case a threat from another aircraft system is identified in the security risk assessment);
- classify the connections by the populations that have an access to the connections and by the form of attack supported by the connections;
- describe and classify the significant information assets for the system; this includes: data characterized by external / internal digital data connections from / to / through system ; data kept by the system as part of its operation, including system logs and fault data; data used by the system to define its function and configuration, generally considered as part of the system's installation and administration data (including: software parts, databases, such as navigation databases, and configuration information, such as subscriber information, firewall rules, security keys, digital certificates, personality modules);
- describe the security controls for each connection, including: access limits and controls for the connection, and what limits there may be to exploit; physical assess controls for the connection.

The security environment must be monitored and updated to capture the changing security context of an aircraft / system. During development, it is updated as part of the development activities. During operation, it is updated as part of the continuing airworthiness activities (RTCA DO-355, 2014). Security environment updates could be

triggered by new attack techniques, new technologies introduced into the environment, new services, capacity increase, etc. The security environment must be a trigger for “cyclic” update activities of the airworthiness security process.

The security perimeter must catalogue the parts of the aircraft or system that contact external systems or populations. It includes the portions that support physical links (e.g., Ethernet ports, wireless transceivers), logical links (e.g., IP stack), network protocols (e.g., DNS, ICMP, gateways, packet filters), network services and clients (e.g., HTML server, FTP client/server, IPSEC server), and remote applications (e.g. file transfer services, remote monitoring, and web applications).

Threat identification consists of the analysis of potential threat sources upon the system and the potential threat conditions that can be created by those threat sources. Threat conditions are then analysed for the severity of their impact upon system safety and threat scenarios are developed. The threat scenarios are then analysed with the characterization of security measures to determine the level of threat.

The complement to the level of threat of a source is the trustworthiness of the source – the level of assurance that the source will use its access in the manner intended by the developer. Trustworthiness is a qualitative judgment about the threat sources relative to the asset under assessment. An example using five levels of consistency with the severity levels is presented in Figure 146, but the number of levels could vary in other methods.

Level	Definition
twE	Not trustworthy to use or manage assets with any safety impact above No Effect
twD	Trustworthy to use and manage assets of Minor safety impact
twC	Trustworthy to use and manage assets of Major safety impact
twB	Trustworthy to use and manage assets of Severe/Hazardous safety impact
twA	Trustworthy to use and manage assets of Catastrophic safety impact

Figure 146: Trustworthiness Levels (RTCA DO-356, 2014)

The trustworthiness level of an external population is established when the population is compliant with standards and regulations appropriate for the level of trustworthiness (or is not compliant, and so is of level twE). These specific standards and regulations are numerous and can be complex (see Figure 147 for examples of trustworthiness standards).

Asset	Trustworthiness Standards
Flight deck access during flight and control of flight for 14CFR Part 25 Aircraft	Pilots and flight crew trained and certified by operators operating under 14CFR Part 121, 14CFR Part 125, 14CFR Part 129, 14CFR Part 135
Maintenance of 14CFR Part 25 Aircraft	Maintenance crew trained, certified, and operating under 14CFR Part 43, 14CFR Part 65, 14CFR Part 121, 14CFR Part 129, 14CFR Part 125, 14CFR Part 135, 14CFR Part 145, maintenance guidance managed under MSG-3, compliance with security guidance under DO-355/ED-204
Support Organizations for Equipment subject to, 14CFR Part 25, (See DO-355/ED-204)	Maintenance crew trained under 14CFR Part 65 and Basic Maintenance performed under 14CFR Part 43
Flight Navigation Databases	Type 1 and Type 2 Vendors operating under DO-200A and DO-201A
Production of Software Parts and Hardware Parts	Aircraft Type Certification and Production Certification or Approval
Aircraft Navigation Service Providers	Varies by national agency

Figure 147: Examples of Trustworthiness Standards (RTCA DO-356, 2014)

Airworthiness Security Risk Assessment must be organized according to the threat scenarios, each of which must classify the pertinent information about potential successful attacks. A threat scenario must be organized in terms of:

- threat conditions that resulted from attack,
- vulnerabilities used in the attack,
- operational events or conditions that enable the attack,
- threat source profile of external population and attack vector,
- security measures (if present) that were intended to intervene to mitigate the attack.

The logic of the security architecture access points, assets, security measures, and interdependencies between security measures and their supporting assets must be captured by identifying the chains of protection. The internal attack paths of the threat scenarios can be organized according to the sequences of security measures (that the attacker must overcome), assets (that the attacker compromises), and threat conditions (that the attacker causes). Conceptually these sequences can be considered to traverse a graph showing the Chains of Protection (CoP) that link together various Security Measures (SM). Each stage of attack progresses from one security measure to another resulting in threat conditions at each stage. Figure 148 shows the basic ingredients for a simple threat scenario with the associated basic risk assessment measures.

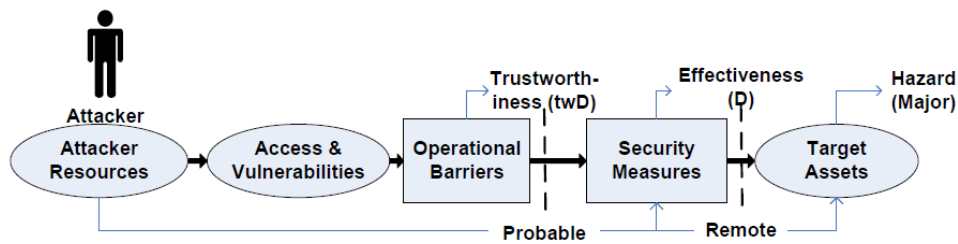


Figure 148: Single Stage Threat Scenario (RTCA DO-356, 2014)

In the case of multi-stage attacks on security architectures with layers and/or defence in depth, the initial attack will be to compromise supporting assets to obtain the necessary capabilities to launch additional attacks to reach the target assets, as in Figure 149. The effectiveness of the first layer is shown in the example figure to reduce “Frequent” to “Remote”, and the effectiveness of the second measure is to reduce “Remote” to “Extremely Remote”, as is necessary to show acceptable risk for a final condition severity in the figure of “Hazardous”.

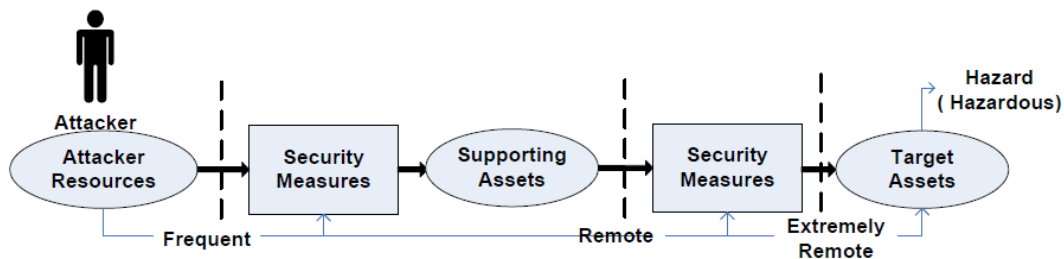


Figure 149: Two Stages Threat Scenario (RTCA DO-356, 2014)

One means of generating threat scenarios is through reference to an up-to-date threat catalogue which documents potential threat sources and methods of attacks.

The Chain of Protection is the sequence of security measures which are defeated in order for a particular attack scenario to succeed. Each stage of a Chain of Protection must be assessed. Figure 150 shows the associated data and data dependencies to assess the first stage, which generates the security environment for assessing the next stage. The severity of the Chain of Protection is the severity of the final consequence base on the impact on the primary asset. The likelihood of the Chain of Protection is based on the attack attempt likelihood, and the likelihood of attack success, based on the effectiveness of the security measures in the chain against the attacker.

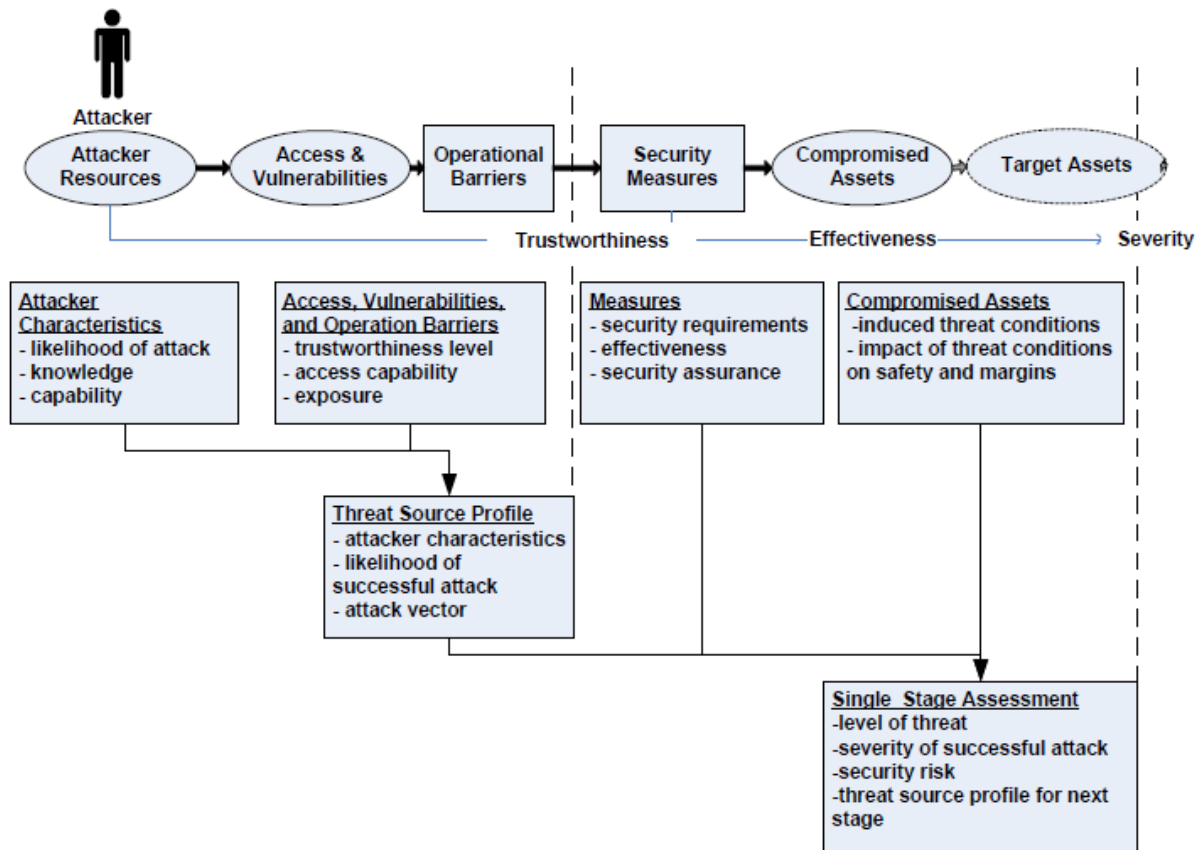


Figure 150: Security Risk Assessment for each stage in the Chain Protection (RTCA DO-356, 2014)

The standard emphasizes also the fact that the Chain of Protection should show both the direct attack on the security measure, and the indirect multi-stage attack on the supporting asset and their security measure.

The standard gives also detailed information on how to consider failure conditions during the security risk assessment. As part of establishing the attack paths and other means to bypass the security architecture, failure conditions for the security measures should be established and defined as threat conditions within the security risk assessment. Thus any list of threat conditions can start with a list of classes of failure conditions as stated in Figure 151.

Class of Failure Condition	Security Attribute	Asset	Definition
Loss of function or loss of continuity in function	Availability of interfaces and information that support the function	System supporting interface and function	Intended function is not performed, intended information is not provided, including intermittent failures in the continuity of data over a required service interval.
Malfunction	Integrity of interfaces and information that support the function	System supporting interface and function	Intended function is performed incorrectly or not provided when or where needed.

Figure 151: Assets and Failure Condition Classes (RTCA DO-356, 2014)

To this list must be added a list of classes of threat conditions as stated in Figure 154.

Class of Threat Condition	Security Attribute	Asset	Definition
Failure conditions (See Table 2-4)	(See Table 2-4)	(See Table 2-4)	(See Table 2-4)
Loss of Confidentiality	Confidentiality of the information and of interfaces that are the source of the information	System(s) supporting function(s) and interface(s) responsible for data representing the information	Exposure of information.
Unintended function	Integrity of the information provided by the unintended function and of interfaces and systems that provide the unintended function	System(s) supporting the unintended function and the interfaces used by the unintended function	Unintended function is performed. This includes the presence of malware.
Tampered information	Integrity of the information and of interfaces and systems that are the source of the information	System(s) supporting function(s) and interface(s) responsible for data representing the information	Intended function appears to be performed correctly but is incorrect or information is incorrect but satisfies safety integrity mechanisms. Includes coherent corruption.
Spoofed information	Integrity of the information and of interfaces and systems that provide the spoofed information	System(s) supporting function(s) and interface(s) responsible for data representing the information	Intended information appears to be correct and correctly sent, but either source or destination is incorrect.
Misuse	Integrity of information and interfaces and systems that are being misused	System(s) that support the functions and interfaces being misused	An intended function being invoked by an unauthorized entity.
Counterfeiting	Integrity of information	System(s) supporting function(s) and interface(s) responsible for persistent data representing the information	Tampering with persistent data. Includes but is not limited to coherent corruption of software part or user modifiable data.

Figure 152: Assets and Threat Condition Classes (RTCA DO-356, 2014)

The security risk assessment must also be based on judging the severity of attacks on the safety of the aircraft. The standard (RTCA DO-356, 2014) gives more information about the way to evaluate the level of threat and to conduct the risk assessment as follows. The level of threat of a threat condition is determined by its likelihood. The exposure time, as defined in the standard (SAE ARP 4761A, 2004), for security aspects includes those maintenance and operational phases during which the various stages of a multi-stages attack can be conducted. The rate of occurrence of a threat scenario across a given service life-span is classified according to the likelihood classifications given in Figure 153.

Symbol	Term	Definition
pV	Frequent	Anticipated to occur routinely in the life of each airplane
pIV	Probable	Unlikely to occur to each airplane during a routine flight but may occur one or more times in the life of each airplane
pIII	Remote	Unlikely to occur to each airplane during its total life but may occur several times in the total life of a number of airplanes of the type
pII	Extremely Remote	Not anticipated to occur to each airplane during its total life but which may occur a few times in the total life of all airplanes of the type
pI	Extremely Improbable	Not anticipated to occur during the entire operational life of all airplanes of the type

Figure 153: Likelihood Definitions (RTCA DO-356, 2014)

The combined effect on the likelihood of the threat scenario itself will depend on the joint distribution of these likelihoods and the events of the threat scenario. Applicable approaches include Bayesian or Boolean probability models such as Threat Tree method.

Once a threat scenario has been built, the factors involved in the likelihood of the associated threat condition are presented in Figure 154 hereafter.

Element	Metric	Is Determined By
Attacker Source Profile	Likelihood of Attack	Trustworthiness of Attacker Organization*
Vulnerabilities	Probability of Exploitation	Effectiveness of mitigation**
Operational Conditions	Probability of Exposure	Likelihood of Occurrence of Condition
Security Measures	Probability that Measure Will Fail	Effectiveness
Resulting in		
Threat Condition	Likelihood of Successful Attack	Combination of metrics over all Threat Scenarios for that Threat Condition

Figure 154: Threat Condition Components (RTCA DO-356, 2014)

Finally the risk for a given severity classification is assessed by aggregating all the threat scenarios with their threat conditions and its acceptability is examined through the risk matrix given in Figure 155.

Risk Level		Threat Scenario Impact				
		V	IV	III	II	I
	Threat Scenario Likelihood	No Effect	Minor	Major	Hazardous	Catastrophic
pV	Frequent	Acceptable	Unacceptable	Unacceptable	Unacceptable	Unacceptable
pIV	Probable	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
pIII	Remote	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
pII	Extremely Remote	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
pI	Extremely Improbable	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

* = Risk acceptability must include demonstrating the absence of a single point of vulnerability

Figure 155: Risk Matrix (RTCA DO-356, 2014)

If the risk is found to be unacceptable, risk mitigations may be defined to modify or augment the system. The risk acceptability should then be reviewed after updating the risk assessment to consider the modified system. This may be repeated until an acceptable risk is found.

Security measures are characterized by their effectiveness against unauthorized interactions. This is shown by:

- Establishing effectiveness of the security architecture through validation of the correctness of the security architecture, i.e. non-bypass, protection, independence, detection and restoration...
- Determining the vulnerability of the security measures and assessing their effects on effectiveness: assessment and test of system design vulnerabilities including well-known vulnerabilities. The Security Risk Assessment should provide the severity for various failures. Through the safety analysis, changes can be made to the proposed response and alerting plan, taking into account the severity of occurrence of the security related failures. Testing of the system should also address the ability of the alerting scheme to properly handle the failures and whether it is possible to compromise the normal alerting failures through a security fault. In all cases the safety of the aircraft should be designed into the system such that safety is never compromised by a response to a failure. Failures of security functions should not be allowed to impede the communication of important systems, such as navigation and flight controls. Pilots should not have to resolve security issues nor review audit logs. Likewise, any crew alerting message should follow the same design philosophy. The alerting messages should address the safety concern of the aircraft, not the security function. Alerting messages for failure of a firewall should not announce that the firewall no longer operates, instead, the effect on safety of the aircraft should be annunciated, such as "Loss of Radio Channel", which can no longer talk through the firewall.
- Establishing effectiveness of the security measures through validation of the correctness of the security requirements to perform with the security environment: effectiveness of the protocols and algorithms through the validation of their requirements, effectiveness of the technical implementation of a security measure through the application of assurance level (see), effectiveness of the policies and procedures of an operational or management security measure through the organizational trustworthiness.
- Establishing an appropriate assurance level for effectiveness: the assurance level for effectiveness is a qualitative evaluation of the level of performance required for the security measures. The security effectiveness objectives drive the required level of assurance. The security effectiveness is the ability of the security measure to protect an asset against the threats identified in the security scope and systematically established in the security risk assessment. The level is classified by the effectiveness as in Figure 156.

Assurance Level	Effectiveness Classification*
E	No Effect
D	Sufficient to protect against a Minor safety effect by intentional unauthorized electronic interactions with the system
C	Sufficient to protect against a Major safety effect by intentional unauthorized electronic interactions with the system
B	Sufficient to protect against a Hazardous safety effect by intentional unauthorized electronic interactions with the system
A**	Sufficient to protect against a Catastrophic safety effect by intentional unauthorized electronic interactions with the system

*: With an acceptable security risk as established by the Security Risk Assessment against the threat defined in the security scope.

** : Also requires that there cannot be the potential for a single vulnerability in the architecture that would compromise all the security measures.

Figure 156: Effectiveness Classification of Assurance Level (RTCA DO-356, 2014)

A defence-in-depth architecture organizes the security measures so the resulting layered protection is more effective than the individual measures by forcing an attacker to defeat multiple measures in order to reach an aircraft asset. Following the principles of assigned development assurance levels, this consideration results in the guidance shown in Figure 157 and Figure 158.

Assurance Level for Combined Elements and Layers	Level for Common Elements between Layers	Level for Primary Layer	Level for Secondary Layers
E	E	E	N/A
D	D	D	N/A
C	C	C D	N/A D
B	B	B C	N/A C
A*	A	A B	N/A B

*: Also requires that there cannot be the potential for a single vulnerability in the architecture that would compromise all the security measures.

Figure 157: Minimum Assurance Levels for Layered Defense-in-Depth Architectures (RTCA DO-356, 2014)

Assurance Level	Development Assurance Level If implemented as an onboard control	If implemented through organizational trustworthiness
E	DAL E	twE
D	DAL D	twD
C	DAL C	twC
B	DAL B	twB
A	DAL A*	twA

*: Also requires that there cannot be the potential for a single vulnerability in the architecture that would compromise all the security measures.

Figure 158: Allocating Assurance Levels to Development or Organizational Trustworthiness (RTCA DO-356, 2014)

In case of a system that can lead to catastrophic safety conditions (DAL A), specific requirements must be defined and only the resulting residual impact outside of the specific security requirements should be included in the assurance requirement.

For most external conditions, the security measures should also combine on-board and organizational controls as shown in because there is always an access population with authorized access.

Total Assurance Level	Assurance Level for Onboard Measures (Internal Layer)	Trustworthiness for Organizational Measures (External Layer)
E	E	N/A
D	D E	N/A twD
C	C D* E	N/A twD* twC
B	B C* E	N/A twC* twB
A	A** B* E	N/A twB* twA

*: Only applies if external access to onboard systems cannot bypass the organizational controls, and organizational access cannot bypass the onboard measures.

** : Also requires that there cannot be the potential for a single vulnerability in the architecture that would compromise all the security measures.

Figure 159: Layering On-board and Organizational Assurances (RTCA DO-356, 2014)

Regarding the qualification of security testing tools, the standard (RTCA DO-356, 2014) argues that in general security tools (i.e. scanning, attack, and robustness “fuzzing”) are used as verification tools. Therefore by the tool qualification criteria from the standard (RTCA DO-178B, 1992) use of TQL-5 is appropriate. Requirements corresponding to TQL-5 include the following:

- operational requirements are defined;
- operational requirements include requirements for content currency and integrity of tool delivery;
- tool and related material is under configuration control for identification, integrity, traceability, retrieval, retention, and protection from unauthorized change;
- tool is operated in accordance with operational requirements;
- tool is adequate for requirements.

The standard (RTCA DO-356, 2014) gives the possibility to choose an alternate compliance method for security. The following elements are to be defined:

- the Target of Evaluation consists of the system with its security scope (security perimeter, assets, security environment), and any associated life cycle data;
- the Protection Profile, if used, should satisfy the security requirements for the systems, including its security scope and threat identification.

When the alternate method is based on the Common Criteria (ISO/IEC 15408-1, 2009) standard, the applicable assurance requirements should be defined according to Figure 160.

Assurance Level	EAL
E	CC EAL 1
D	CC EAL 3
C	CC EAL 4
B	CC EAL 5
A	CC EAL 5

Figure 160: Alternate Common Criteria EAL Levels for System Level Assurance (RTCA DO-356, 2014)