Information and Software Technology 56 (2014) 689–717

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof

An extended systematic literature review on provision of evidence for safety certification

Sunil Nair [a,*], Jose Luis de la Vara [a], Mehrdad Sabetzadeh [b], Lionel Briand [b]

[a] Certus Centre for Software V&V, Simula Research Laboratory, P.O. Box 134, 1325 Lysaker, Norway
[b] SnT Centre for Security, Reliability and Trust, 4 rue Alphonse Weicker, L-2721, Luxembourg

ARTICLE INFO

Article history:
Received 27 August 2013
Received in revised form 6 March 2014
Accepted 9 March 2014
Available online 15 March 2014

Keywords:
Safety–critical systems
Safety standards
Safety compliance
Safety certification
Safety evidence
Systematic literature review

ABSTRACT

Context: Critical systems in domains such as aviation, railway, and automotive are often subject to a formal process of safety certification. The goal of this process is to ensure that these systems will operate safely without posing undue risks to the user, the public, or the environment. Safety is typically ensured via complying with safety standards. Demonstrating compliance to these standards involves providing evidence to show that the safety criteria of the standards are met.

Objective: In order to cope with the complexity of large critical systems and subsequently the plethora of evidence information required for achieving compliance, safety professionals need in-depth knowledge to assist them in classifying different types of evidence, and in structuring and assessing the evidence. This paper is a step towards developing such a body of knowledge that is derived from a large-scale empirically rigorous literature review.

Method: We use a Systematic Literature Review (SLR) as the basis for our work. The SLR builds on 218 peer-reviewed studies, selected through a multi-stage process, from 4963 studies published between 1990 and 2012.

Results: We develop a taxonomy that classifies the information and artefacts considered as evidence for safety. We review the existing techniques for safety evidence structuring and assessment, and further study the relevant challenges that have been the target of investigation in the academic literature. We analyse commonalities in the results among different application domains and discuss implications of the results for both research and practice.

Conclusion: The paper is, to our knowledge, the largest existing study on the topic of safety evidence. The results are particularly relevant to practitioners seeking a better grasp on evidence requirements as well as to researchers in the area of system safety. As a major finding of the review, the results strongly suggest the need for more practitioner-oriented and industry-driven empirical studies in the area of safety certification.

Abbreviations: AADL, Architecture Analysis & Design Language; ACRuDA, Assessment and Certification Rules for Digital Architectures; ASA, Automated and Structured Analysis; ASCAD, Adelard Safety Case Development; BBN, Bayesian Belief Networks; CAE, Claims, Arguments and Evidence; CCS, Calculus of Communicating Systems; CDL, Configuration Deviation List; CENELEC, Comité Européen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardization) ; CMA, Common Mode Analysis; COTS, Commercial Off-The-Shelf; CSP, Communicating Sequential Processes; DECOS, Dependable Embedded COmponents and Systems; DOVE, Design Oriented Verification and Evaluation; ECHA, Environmental Condition Hazard Assessment; EMFI, Electromagnetic Fault Injection; ETA, Event Tree Analysis; EVA, Evidence Volume Approach; FFA, Functional Failure Analysis; FFPA, Functional Failure Patch Analysis; FHA, Functional Hazard Analysis; FMEA, Failure Mode, Effects Analysis; FMECA, Failure Mode, Effects and Criticality Analysis; FMEDA, Failure Modes, Effects and Diagnostic Coverage Analysis; FMES, Failure Mode and Effect Summary; FPGA, Field-programmable gate array; FPTC, Fault Propagation and Transformation Calculus; FPTN, Failure Propagation and Transformation Notation; FSM, Functional Safety Management; FTA, Fault Tree Analysis; GQM, Goal Question Metric; GSN, Goal Structuring Notation; HAZID, Hazard Identification Study; HAZOP, HAZard and Operability; HEP, Human Error Prediction; HHA, Human Hazard Analysis; HOL, Higher Order Logic; HRA, Human Reliability Analysis; IEC, International Electro-technical Commission; IET, Institution of Engineering and Technology; IHA, Intrinsic Hazard Analysis; ISO, International Organization for Standardization; MDE, Model-Driven Engineering; MC/DC, Modified Condition/Decision Coverage; MMEL, Master Minimum Equipment List; MTBF, Mean Time Between Failures; MTTF, Mean Time To Failure; OCL, Object Constraint Language; OS, Operating System; PHA, Preliminary Hazard Analysis; PRA, Particular Risk Analysis; PS, Primary Study; PSAC, Plan for Software Aspects of Certification; QA, Quality Assurance; RASP, Risk Assessment of Structural Part; RTCA, Radio Technical Commission for Aeronautics; RTOS, Real-Time OS; SACM, Structured Assurance Case Metamodel; SAL, Safety Assurance Level; SAS, Software Accomplishment Summary; SCMP, Software Configuration Management Plan; SDP, Software Development Plan; SEAL, Safety Evidence Assurance Level; SHARD, Software Hazard Analysis and Resolution in Design; SIL, Safety Integrity Level; SLR, Systematic Literature Review; SQA, Software QA; SRS, Software Requirements Specification; SSG, Safety Specification Graph; SVP, Software Verification Plan; SWIFI, Software Implemented Fault Injection; TPTP, Thousands of Problems for Theorem Provers; UAS, Unmanned Autonomous Systems; V&V, Verification and Validation.

* Corresponding author. Tel.: +47 40 64 40 46; fax: +47 67 82 82 01.
E-mail addresses: sunil@simula.no (S. Nair), jdelavara@simula.no (J.L. de la Vara), mehrdad.sabetzadeh@uni.lu (M. Sabetzadeh), lionel.briand@uni.lu (L. Briand).

http://dx.doi.org/10.1016/j.infsof.2014.03.001
0950-5849/© 2014 Elsevier B.V. All rights reserved.

Contents

1. Introduction

A safety–critical system is one whose failure may cause death or injury to people, harm to the environment, or substantial economic loss [5]. In domains such as aviation, railway, and automotive, such systems are typically subject to a rigorous safety assessment process. A common type of assessment, usually conducted by a licensing or regulatory body, is *safety certification*. The goal of safety certification is to provide a formal assurance that a system will function safely in the presence of known hazards [PS93]. Safety certification can be associated with the assessment of *products, processes, or personnel*. For software-intensive safety–critical systems, certification of products and processes are regarded as being the most challenging [PS93].

Assessing and assuring safety of a system relies on building sufficient confidence in the safe operation of the system in its operating context. This confidence is often developed by satisfying safety objectives that mitigate the potential safety risks that a system can pose during its lifecycle. The safety objectives are usually established by a set of industry-accepted criteria, typically available as standards. Examples of safety standards include IEC61508 [11] for a broad class of programmable electronic systems, DO-178C [7] for aviation, the CENELEC standards (e.g., [33]) for railway, and ISO26262 [8] for the automotive sector.

Demonstrating compliance with safety standards involves collecting evidence that shows that the relevant safety criteria in the standards are met [16]. Although, safety standards prescribe the procedures for compliance, it often proves to be a very challenging task to the system suppliers due to the fact that these standards are presented in very large textual documents that are subject to interpretation. In general, evidence can be defined as *"The available body of facts or information indicating whether a belief or proposition is true or valid"* [30]. For realistically large systems, however, one can seldom argue that evidence serves as a definitive proof of the truth or validity of safety claims, but only whether the evidence is sufficient for building (adequate) confidence in the claims. Hence, we define evidence for safety certification as *"information or artefacts that contribute to developing confidence in the safe operation of a system and to showing the fulfilment of the requirements of one or more safety standards"*. Some generic examples of safety evidence are test results, system specifications, and personnel competence.

The lack of consistent interpretation of a standard can lead to misunderstanding the evidence needs. Failing to clearly understand the evidence needs for assessing a system can result in two main problems [34,PS145]. First, the supplier may fail to record critical details during system development that the certifier will require later on. Building the missing evidence after-the-fact can be both expensive and laborious. Second, not knowing ahead of time what the certifiers will receive as evidence may affect the planning and organisation of the certification activities. In particular, the certifier may find it hard to develop sufficient confidence in the system undergoing certification if the evidence requirements have not been negotiated and agreed with the supplier a priori [PS54,15].

Apart from understanding and precisely defining the evidence requirements, attention needs to be paid to how this evidence is organised and assessed for adequacy. If the evidence is not structured properly, its sheer volume and complexity can jeopardize the clarity of the safety arguments [PS124]. Furthermore, it is important to be able to determine how definitive and credible the evidence is. Though safety standards mandate adequate evidence to show compliance, they are vague on what adequate means in a particular context, often intentionally and for the sake of being general.

The main objective of this paper is to synthesise the existing knowledge in the academic literature about safety evidence, concentrating on the three facets outlined above: the information that constitutes evidence; structuring of evidence; and evidence assessment. The term *evidence provision* is used hereafter to collectively