Simula Research Laboratory, Technical Report 2012-13 July 2012

SLR on Evidence Classification, Structuring and Assessment for Safety.

Extracted Data, Technical Report

Sunil Nair[1], Jose Luis de la Vara[1], Mehrdad Sabetzadeh[2], and Lionel Briand[2]
[1]Certus Centre for Software V&V, Simula Research Laboratory, P.O. Box 134, 1325 Lysaker, Norway
[2]SnT Centre for Security, Reliability and Trust, 4 rue Alphonse Weicker, L-2721 Luxembourg

Abstract—

Context: Critical systems in domains such as avionics, 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 large 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.

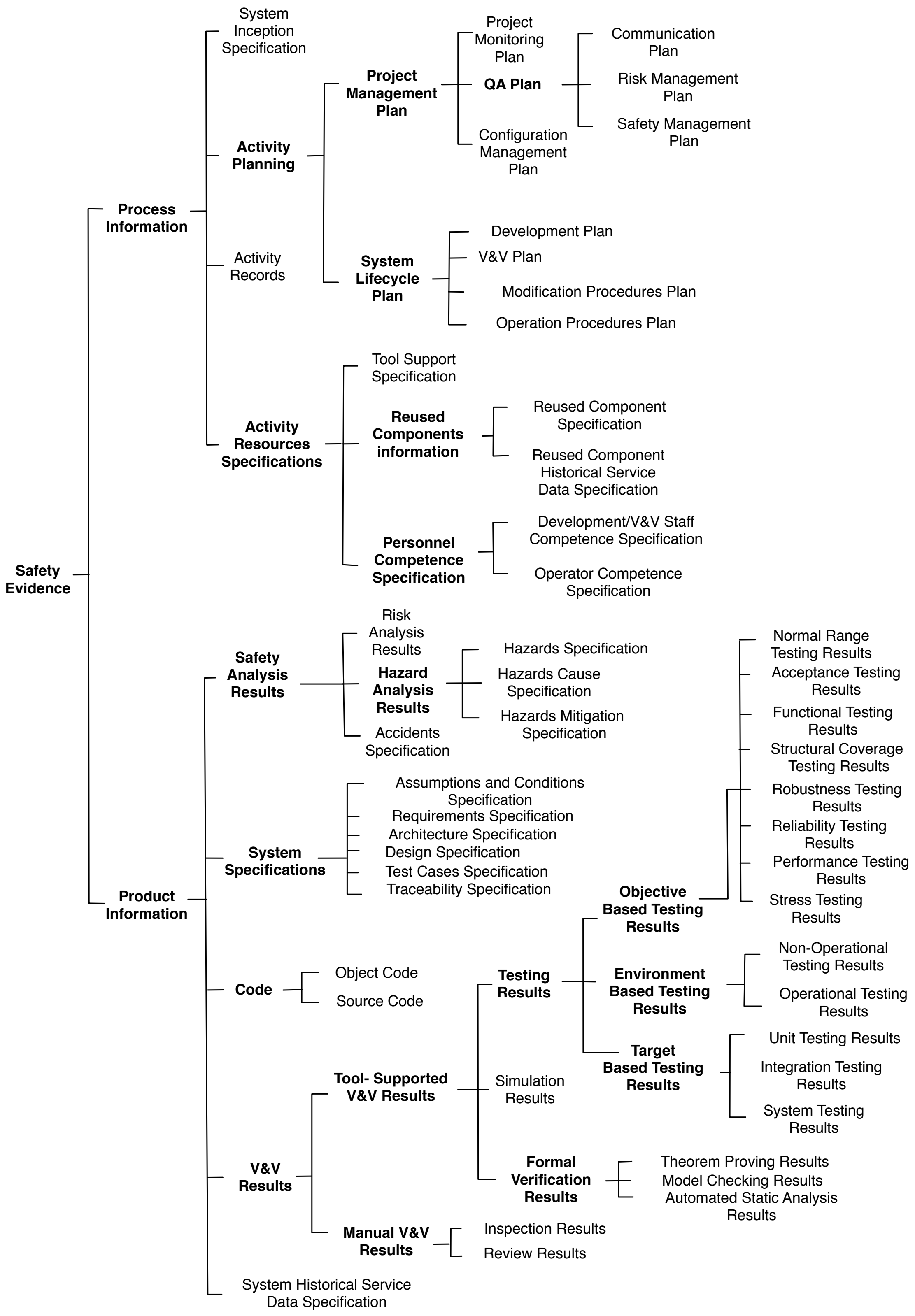
Method: We use a Systematic Literature Review (SLR) as the basis for our work. The SLR builds on 217 peer-reviewed studies, selected through a multi-stage process, from 4,963 studies published between 1990 and 2012.

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.

Keywords: safety-critical systems; safety standards; safety compliance; safety certification; safety evidence; systematic literature review.

Evidence Taxonomy:


Safety Evidence
Process Information
System Inception Specification
Activity Planning
Project Management Plan
Project Monitoring Plan
QA Plan
Communication Plan
Risk Management Plan
Safety Management Plan
Configuration Management Plan
System Lifecycle Plan
Development Plan
V&V Plan
Modification Procedures Plan
Operation Procedures Plan
Activity Records
Activity Resources Specifications
Tool Support Specification
Reused Components information
Reused Component Specification
Reused Component Historical Service Data Specification
Personnel Competence Specification
Development/V&V Staff Competence Specification
Operator Competence Specification
Product Information
Safety Analysis Results
Risk Analysis Results
Hazard Analysis Results
Hazards Specification
Hazards Cause Specification
Hazards Mitigation Specification
Accidents Specification
System Specifications
Assumptions and Conditions Specification
Requirements Specification
Architecture Specification
Design Specification
Test Cases Specification
Traceability Specification
Code
Object Code
Source Code
V&V Results
Tool- Supported V&V Results
Testing Results
Objective Based Testing Results
Normal Range Testing Results
Acceptance Testing Results
Functional Testing Results
Structural Coverage Testing Results
Robustness Testing Results
Reliability Testing Results
Performance Testing Results
Stress Testing Results
Environment Based Testing Results
Non-Operational Testing Results
Operational Testing Results
Target Based Testing Results
Unit Testing Results
Integration Testing Results
System Testing Results
Simulation Results
Formal Verification Results
Theorem Proving Results
Model Checking Results
Automated Static Analysis Results
Manual V&V Results
Inspection Results
Review Results
System Historical Service Data Specification

Definition of Evidence types (with Artifacts, tools and techniques extracted)

Acceptance Testing Results
Definition: Results from the validation of the behaviour of a critical system against the customers' requirements. The customers undertake, or specify, typical tasks to check that their requirements have been met.
Techniques: user evaluation in mock work environments.
Accidents Specification
Definition: Specification of the events that result in an outcome culminating in death, injury, damage, harm, and/or loss as a consequence of the occurrence of a hazard of a critical system.
Techniques: ETA; PHL; PHA; FMEA; FMECA; FMES; IHA; FMEDA.
Activity Records
Definition: Specification of the worked performed to execute the activity planning of a critical system.
Artifacts: QA audit results, maintenance log; change requests report; system changes report; review checklists; quality management report; safety management report; technical safety report; risk management file; safety and engineering meeting minutes; design checklists; V&V effort report; configuration control records; QA activities report; quality control documents; safety criteria report; safety compliance assessment report; failure checklist; customer feedback reports; feasibility analysis; implementation track; integration report; quality management report; project execution report; hazard checklist; report on monitoring operator performance and periodic review of skills; structural coverage analysis review checklist; SAS. **Information:** testing team independence.
Architecture Specification
Definition: Description of the fundamental organization of a critical system, embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution.
Artifacts: dependence diagram.
Assumptions and Conditions Specification
Definition: Description of the constraints on the working environment of a critical system for which it was designed.
Artifacts: assumptions about the environment where the code is executed; domain assumptions.
Automated Static Analysis Results
Definition: Results from an automatic process for evaluating a critical system based on its form, structure, content, or documentation.
Techniques: code static analysis; fault model static analysis; control flow analysis; worst case execution time analysis; integrity analysis; cyclomatic complexity analysis; data coupling analysis; control coupling analysis.
Communication Plan
Definition: Description of the activities targeted at creating project-wide awareness and involvement in the development of a critical system.
Configuration Management Plan
Definition: Description of how identification, change control, status accounting, audit, and interface of a critical system will be governed.
Artifacts: SCMP; version management; change control procedures. **Information:** target platform.
Design Specification
Definition: Specification of the components, interfaces, and other internal characteristics of a critical system or component.
Techniques: ADDL; UML; SysML; diagrams human factors guidelines and standards; SCADE. **Artifacts:** interface design; data structures; state machine. **Information:** safety assessment reliability prediction.
Development Plan
Definition: Description of how a critical system will be built. It includes information about the requirements, design and implementation (coding and/or integration) phases.
Artifacts: SDP; test generation procedure; verification process. **Information:** development methodology; coding standards; coding guidelines; design rules; pair-programming; use of industry-standard state machine notations; metrics for function-code size; FFPA

method; design technique; implementation technique.
Development and V&V Staff Competence Specification
Definition: Specification of the skills or knowledge that the parties involved in the development and V&V plans of a critical system need in order to perform the activities assigned to them.
Artifacts: developer qualification; engineers CV. **Information:** staff experience; authority and training; tool training; software architects experience; experience, authority and training of verification engineers; reviewer competence.
Functional Testing Results
Definition: Results from the validation of whether or not the observed behaviour of a system conforms to its specification.
Techniques: hazard directed testing.
Hazards Causes Specification
Definition: Specification of the factors that create the hazards of a critical system.
Techniques: FTA; FMEA; FMECA; anthropometric and workload assessment; Markov Analysis; HAZOP; causal analysis; SHARD; common failure analysis; common mode failure analysis; common mode analysis; root cause analysis; FMES; FPTC; FPTN; IHA; FFA; ECHA; HEP; HRA; FMEDA. **Information:** human error.
Hazards Specification
Definition: Specification of the conditions in a critical system that can become a unique, potential accident.
Techniques: FuHA; PHL; PHA; SHA; HHA; FMEA; FMECA; FaHA; Petri Nets; Markov Analysis; HAZOP; SHARD; HAZID; FMES; vulnerability analysis; IHA; ECHA; HEP; HRA FMEDA. **Artifacts:** hazard log.
Hazards Mitigation Specification
Definition: Specification of how to reduce hazard likelihood and hazard consequences when a hazard cannot be eliminated in a critical system.
Synonyms: hazard contingency, hazard barriers, and hazard protections.
Techniques: PHA; SHA; FMECA; IHA; ECHA; diversity analysis; FMEDA;
Inspection Results
Definition: Results from the visual examination of system lifecycle products of a critical system to detect errors, violations of development standards, and other problems.
Synonyms: audit (usually used to refer to inspections made by an independent party).
Technique: functional configuration audit; physical configuration audit; inspection of safety requirements; code inspection; independent analysis of requirements and architecture specification; safety audit; independent assessment of tests. **Artifacts:** independent safety audit report.
Integration Testing Results
Definition: Results from the evaluation of the interaction between the components of a system.
Techniques: software integration testing; hardware integration testing; interfaces testing.
Model Checking Results
Definition: Results from the verification of the conformance of a critical system to a given specification by providing a formal guarantee. The critical system under verification is modelled as a state transition system, and the specifications are expressed as temporal logic formulae that express constraints over the system dynamics.
Techniques: CCS; CSP; LOTOS; temporal logic; Lustre; ASA; ClawZ; Uppaal; lambda calculus; schedule ability analysis; Time Petri Nets. **Tools:** Uppaal
Modification Procedures Plan
Synonyms: maintenance procedures
Definition: Description of the instructions as to what to do when performing a modification in a critical system in order to make corrections, enhancements or adaptations to the validated system, ensuring that the required safety is sustained.
Techniques, tools and artifacts: changes propagation; non-regression testing; maintenance plan; inspection procedures; repair time; change assessment.
Non-operational Testing Results
Definition: Results from evaluation of a critical system in an environment that does not correspond to but replicates its actual operational environment.
Normal Range Testing Results
Definition: Results from the verification of the behaviour of a system under normal operational conditions.

Techniques: Equivalence classes and input partitioning testing.
Object Code
Definition: Computer instructions and data definitions in a form output by an assembler or compiler.
Operation Procedures Plan
Definition: Description of the instructions and manuals necessary to ensure that safety of a critical system is maintained during its use.
Artifacts: user manual; target staff description; installation procedure; operational staff support description; installation structure plan; training plan; incident registration procedures; performance monitoring plan; installation and operation facility procedures; evacuation procedures; description of the allocation of system functions between equipment and operators.
Operational Testing Results
Definition: Results from the evaluation of a critical system in its actual operating environment.
Operator Competence Specification
Definition: Specification of the skills or knowledge that the parties involved in the operation procedures need in order to perform the activities assigned to them.
Techniques, tools and artifacts: operational staff training needs specification; manning requirements specification. **Information:** operator competence; user experience.
Performance Testing Results
Definition: Results from the verification of the performance requirements (e.g., capacity and response time) of a critical system.
Synonyms: resource consumption analysis.
Techniques: memory use; timing analysis; memory partitioning analysis. **Information:** memory use.
Project Monitoring Plan
Definition: Description of how, on a regular basis and during project execution, data about the actual progress of the activity planning of a critical system is collected and compared with the baseline plans.
Artifacts: meetings schedule; project and organization chart.
Reliability Testing Results
Definition: Results from the verification of fault-free behaviour in a critical system.
Synonyms: failure analysis
Techniques: statistical testing; probabilistic testing.
Requirements Specification
Definition: Specification of the external conditions and capabilities that a critical system must meet and possess, respectively, in order to (1) allow a user to solve a problem or achieve an objective, or (2) satisfy a contract, standard, or other formally imposed documents
Artifacts: (specifications of) performance requirements; derived requirements; software safety requirements; software requirements; high-level requirements; low-level requirements; functional requirements; interface requirements; safety requirements; failure requirements; monitoring requirements; software requirements; MMEL/CDL.
Reused Component Specification
Definition: Specification of the characteristics of an existing system that is (re-)used to make up a critical system.
Artifacts: reused component requirements specification; reused component functions specification; fault pattern library; reused component reliability specification; product safety accreditation; OS/RTOS certification; supplier information; reused component safety case; reused component safety analysis results; equipment requirements specification.
Reused Component Historical Service Data Specification
Definition: Specification of the dependability of a component reused in a critical system based on past observation of the behaviour.
Artifacts: field service experience; product service history; fault log; maintenance reports; studies and reviews of operation safety and environmental experience; maintenance records and surveys. **Information:** probability of failure on demand (from past behavior); prior field reliability in similar applications; failure frequency; failure rate; MTTF; MTTR; MTBF.
Review Results
Definition: Description of a process or meeting during which a work product or set of works products is presented to some interested party for comment or approval.
Synonyms: walkthrough (usually used to refer to a review led by a designer or programmer).
Artifacts: (results from, usually reports of) source code walkthrough; independent audit review; source

code review; design review.
Risk Analysis Results
Definition: Specification of the expected amount of danger when an identified hazard will be activated and thus become an accident in a critical system.
Synonyms: risk assessment results
Techniques: FTA; ETA; PHA; SHA; FMEA; FMECA; Markov Analysis; FMES; FPTC; FPTN; PHA; FMES; IHA; RASP; HRA. **Information:** likelihood, severity.
Risk Management Plan
Definition: Description of the activity regarding the development and documentation of an organized and comprehensive strategy for identifying project risks. It includes establishing methods for mitigating risk and for tracking risk.
Robustness Testing Results
Definition: Results from the verification of the behaviour of a critical system in the presence of faulty situations in its environment.
Techniques: fault injection testing; SWIFI; EMFI.
Safety Management Plan
Definition: Description of the coordinated, comprehensive set of processes designed to direct and control resources to optimally manage the safety of an operational aspect of an organization.
Simulation Results
Definition: Results from the verification of a critical system by creating a model that behaves like the system when provided with a set of inputs.
Techniques: symbolic execution; emulation; hardware-in-loop testing; animation **Tools:** Matlab/Simulink; TargetLink; Stateflow.
Source Code
Definition: Computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator.
Artifacts: ADA code; C code; C++ code.
Stress Testing Results
Definition: Results from the verification of the behaviour of a critical system at the maximum design load, as well as beyond it.
Techniques: boundary value testing; exhaustive input testing; sensitivity testing.
Structural Coverage Testing Results
Definition: Results from the verification of the behaviour of a critical system by executing all or a percentage of the statements or blocks of statements in a program, or specified combinations of them, according to some criteria.
Synonyms: structural coverage analysis.
Techniques: MC/DC testing (or coverage); control flow analysis; data flow analysis; statement coverage; branch coverage; subroutines coverage; safety requirements coverage. **Information:** element under analysis; coverage percentage.
System Historical Service Data Specification
Definition: Specification of the dependability of a system based on past (prior-certification) observation of the behaviour.
System Inception Specification
Definition: Specification of initial details about the characteristics of a critical system and how it will be created.
Artifacts: PSAC; EUC specification; scoping document. **Information:** suitability of notations; soundness of methods; quality of development method.
System Testing Results
Definition: Results from the evaluation of the behaviour of a whole critical system. External interfaces to other applications, utilities, hardware devices, or the operating environment are also evaluated at this level.
Test Cases Specification
Definition: Specification of the tests inputs, execution conditions, and predicted results for a critical system to be tested.
Theorem Proving Results
Definition: Results from the verification of a critical system by formally expressing its properties in a common language based on mathematical logic and using a theorem prover. A property can be shown to be a logical consequence of a set of axioms if it can be formally derived from the axioms with a set of deduction steps, which are instances of the set of inference rules that are allowed in the common language.

Techniques: HOL; Z; proof-carrying code; TPTP; PVS.
Tool Support Specification
Definition: Specification of the different tools that will be used in the system lifecycle plan.
Artifacts: tool verification report; tool qualification report; certificate of software development tool; certificate of code generator; tool assurance case; tool reliability report; V&V tools report; tool safety analysis results.
Traceability Specification
Definition: Specification of the relationship between two or more pieces of information related to the development (process information or product information) of a critical system
Artifacts: tables**;** (specifications of traceability from) safety requirements to fault tree gates and events; design to low-level requirements; low-level requirements to tests; requirements to tests; safety requirements to tests; requirements to source; safety requirement to hazard; hazard to safety goal; safety requirement to safety goal; safety goal to safety requirements; safety goal to hazard; safety requirement to system requirement, component, architecture or safety concept; safety concept to system requirements; safety concept to safety requirement, component or software architecture; requirements to design elements; requirements to code; model to code generated
Unit Testing Results
Definition: Results from the evaluation of the functioning in isolation of software pieces, which are separately testable. Depending on the context, these could be the individual subprograms or a larger component made of tightly related units. Unit testing typically occurs with access to the code being tested and with the support of debugging tools.
Synonyms: module testing
V&V Plan
Definition: Description of how and by whom the V&V activities for a critical system will be executed.
Artifacts: verification environment specification; reviews plan; SVP; tests plan.

Extracted Data:

Ref	Year	Domain	Standard	Evidence	Techniques for Specification	Techniques for Assessment	Challenges addressed	Tool support	Evidence Level	Validation
[1]	2010	Unspecified	IEC61508	Software module testing, MC/DC coverage, boundary value testing, SRS, SDD, DRR, DVR	-	Qualitative Assessment - Argumentation	Construction of safety cases		Generic	-
[2]	2008	Generic	Generic	Quality management report; safety management report; technical safety report	Argumentation-induced Evidence Structure - GSN, CAE, trust cases	-	Certification of systems made up of components and subsystems (modular certification)	DECOS test bench	Safety Standard level + domain level	Action research
[3]	2011	Avionics	DO178B	Structural coverage analysis; PSAC; SDP; SVP; SCMP; SQA plan; transition criteria between processes; design specification; source code; exhaustive input testing; structural coverage analysis review checklist	-	-	Better development processes and better evidence about process compliance (V&V activities for DO-178B level A)	VerO-Link analysis tool	System type-level based on the domain and standard levels	-
[4]	2006	Unspecified	Unspecified	Dependence diagram; FTA; Markov Analysis; HAZOP; FMECA; root cause analysis; sensitivity testing	-	-	Capturing the degree of credibility or relevance of the evidence, Construction of safety cases		Generic	-
[5]	2005	Unspecified	ISO/IEC 15408:1999, RTCA/DO-178B, SO 14971 Medical devices	SRS; design specification; SQA records; risk management file	Argumentation-induced Evidence Structure - GSN, ASCAD	Qualitative Assessment - Argumentation	Specification of evidence content, Construction of safety cases (structuring of evidence).	ASCE	Safety standard level	Action Research
[6]	2009	Avionics	Unspecified	FHA; PRA; CMA; HHA, FHA; IHA; ECHA; RASP; CMA; MMEL/CDL; FMEA; FMES; safety assessment reliability prediction; equipment CMAs	-	-	Better development processes and better evidence about process compliance (V&V activities)		Domain level + specific system level	Case study
[7]	2008	Maritime	UK Defense Standards 00-56	Operating instructions; maintenance instructions; design specifications; hazard logs; risk assessment results; system historical service data; safety and engineering meeting minutes; safety management policies, processes, internal audits and reviews (records); operator competence specification; material maintenance records and surveys	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	Construction of safety cases (for ships)		System type level	-
[8]	2008	Unspecified	Unspecified	Source code; source code review; FTA; model from which code has been generated; certified code generator; proof carrying code	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content (formal methods)		Generic	-
[9]	2010	Aerospace	Unspecified	Theorem proving; requirements specification; source code review	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content (code generated automatically)	AUTOCERT	System type Level	Field Study
[10]	2009	Unspecified	Unspecified	Theorem proving, documents containing the model from which the source code has been generated	Argumentation-induced Evidence Structure - GSN (extension with information from formal specification)	Qualitative Assessment - Argumentation	Construction of safety cases (from code generated automatically)	ASCE	Generic	-

[11]	2009	Unspecified	Unspecified	Domain assumptions	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (corresponding to formal proofs), Specification of evidence content (formal proofs and their assumptions)	Unnamed tool	Generic	-
[12]	2000	Unspecified	UK Defense standards, D0178B, DO254, IEC 61508	Worst case execution time analysis; source code static analysis; hardware/software integration testing; data and control flow analysis; object code static analysis	-	-	Specification of evidence content (super-scalar processor)		Safety Standard level	-
[13]	2009	Generic - FPGA	U.K. defense standard 00-56, IEC 61508, DO-254/DO178B,	FMEA; FPTC	-	-	Construction of safety cases (from FPGA design)		Specific system type	-
[14]	2003	Avionics	Unspecified	FMEA; FTA	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Certification of systems made up of components and subsystems (architecture components)		Domain level	-
[15]	2008	Medical	IEC60601, ISO14971	Traceability requirements-test cases; certified OS.	-	-	Specification of evidence content (for medical devices)		Generic	-
[16]	2001	Unspecified	IEC 61508, ISO/IEC TR 15504	Design specification, ETA, FMEA, FMECA, CCA, software safety requirements specification; software safety validation plan; software architecture design description; software architecture integration test specification; software/programmable electronics integration test specification; software architecture design description; software architecture integration test specification; software/programmable electronics integration test specification development tools and coding standards; selection of development tools; software system design specification; software system integration test specification; software module design specification; source code listing; code review report; software module test results; verified and tested software modules; software system integration test results; verified and tested software system; software architecture integration test results; programmable electronics integration test results; verified and tested integrated programmable electronics; software operation and modification procedures; software safety validation results; validated software; software modification impact analysis results; software modification log; appropriate verification report – depends on phase; software functional safety assessment report, structured design methods, strongly typed programming language, coding standards, functional black box testing, performance testing, and walk-through/design reviews, certified language translator, and a library of verified modules, using semi- formal design methods, dynamic testing, static verification, boundary value analysis, performance modeling, control flow analysis, and design reviews, use of specification and design tools, cause failure analysis, structure-based testing, fault tree analysis, finite state machine model- ling, time Petri nets,	-	-	Ambiguities in safety standard, Specification of evidence content		Safety standard level	-

				decision tables, and symbolic execution, probabilistic testing, formal proofs, performance modeling, and Fagan inspections.						
[17]	2011	Medical	Unspecified	Code reviews, unit testing, non-operational testing, robustness testing, functional testing	-	-	Specification of evidence content (testing)		Domain-level	Action research
[18]	1998	Unspecified	Unspecified	Statistical testing	-	-	Capturing the degree of credibility or relevance of the evidence (and adequacy)		Generic	-
[19]	2009	Unspecified	IEC61508	Development staff competence; FSM plan; configuration management plan; tool support specification used; change control procedures; V&V plan; project and organization chart	Textual Template - Template Add-on	Check Add-on, Checklist	Specification of evidence content (for ISO61508), Better development processes and better evidence about process compliance (generic development process for ISO61508)		Safety standard-level	Action research
[20]	1998	Multi-domain	UK defense standards	Timing analysis; MTTF; MTTR; reliability testing; compliance with quality standards; developers skills and experience; FTA; reliability of components; Failure rate; diagnostic coverage; repair time; past reliability in similar applications; design specifications; SHA; HRA; results of QA audits; problems resolution plan.	Argumentation-induced Evidence Structure - CAE	Qualitative Assessment - Argumentation	Construction of safety cases, Need for providing argumentation		Generic	Field study on EU Project SHIP and was then further developed in the UK Nuclear Safety Research Program (the QUARC Project)
[21]	2011	Unspecified	Unspecified	Failure rate	-	-	Capturing the degree of credibility or relevance of the evidence (in claims)		Generic	-
[22]	2010	Unspecified	Unspecified	FTA, ETA, FMEA and HAZOPs.	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation		ASCE	Generic	-
[23]	1999	Unspecified	Unspecified	Design specification; system requirements specification; developer experience	Argumentation-induced Evidence Structure - BBN	Quantitative Assessment - BBN	Capturing the degree of credibility or relevance of the evidence (judgment of evidence sources)		Generic	Action Research Project SERENE
[24]	2010	Avionics	UK Defense standards, IEC 61508	Reviews of personnel competence, project monitoring plans, design specification	-	-	Construction of safety cases, Certification of systems made up of components and subsystems (modular)		Domain-level + Standard level	Field Study
[25]	1990	Unspecified	UK defense Standards	Simulation	-	-	Ambiguities in safety standards (how UK Ministry of Defense standards dealt with new development procedures)		Safety Standard level	-
[26]	1994	Unspecified	Unspecified	FMEA; FTA	-	-	Better development processes and better evidence about process compliance (design and implementation)		Generic	-
[27]	2003	Avionics	ED-12/DO-l78B	Unit testing; software integration testing; acceptance testing; structural coverage analysis.	-	-	Specification of evidence content (code generated automatically)		Domain-level	-

[28]	2006	Avionics	UK defense Standards	Static code analysis, regression testing, walkthroughs, control and data flow analysis, design reviews, peer reviews and Fagan inspections	-	-	Specification of evidence content (V&V-based), Better development processes and better evidence about process compliance (V&V based)		Safety standard specific	-
[29]	2009	Generic	UK defense Standards	FFA; simulation; competence of staff in development or operation; safety management plan; methods for development; tool support specification	-	-	Construction of safety cases		Safety standard level	-
[30]	2004	Avionics	UK Defense Standards 00-56	Design reviews; FMEA; hazard log; operational testing	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	First-time certification or recertification of “proven-in-use” systems (evolution of a system)		Specific System level	Field study
[31]	2008	Railways	CENELEC standards, EN 50126, EN 50128, EN 50129	Change propagation; FMEA; failure checklist	-	-	Capturing the degree of credibility or relevance of the evidence (safety case in railways domain, according to CENELEC railway standards)		Safety Standard + Domain Level	-
[32]	2009	Generic - FPGA	DO-254, lEC 61508 Part 2 and Defense Standard (DS) 00-54	Simulation; timing static analysis	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Need for providing argumentation (for FPGA development)		Specific system type	-
[33]	2010	Generic - FPGA	DO-254, lEC 61508 Part 2 and Defense Standard (DS) 00-54	FTA; FMEA; FPTC	-	-	Construction of safety cases (from FPGA design)		Specific system type	-
[34]	2007	Avionics	DO178B and the UK military standard 00-56	FMEA; FTA	-	-	Demonstration of compliance for novel technologies (MDD-based systems)		Domain-level	Action Research
[35]	2006	Railways	EN 50121, EN 50126, 28, 29	Hazard logs, engineer competence, requirements specification, Design specification	-	-	Specification of evidence content		Safety standard specific + Domain specific	-
[36]	1999	Multi-domain	Unspecified	Reliability testing, simulation	-	-	Specification of evidence content (V&V-based)		Generic	-
[37]	2000	Automotive	Unspecified	FMEA; warranty data records; system change record	-	-	Capturing the degree of credibility or relevance of the evidence (provision of convincing evidence)		System type level	-
[38]	2000	Nuclear	Unspecified	FMECA; acceptance testing; quality control documents	Argumentation-induced Evidence Structure - BBN	Quantitative Assessment - BBN	Construction of safety cases (evidence combination), Capturing the degree of credibility or relevance of the evidence		Generic	-
[39]	2010	Automotive	ISO26262	Domain assumptions, FMEA, FTA, BDD	-	-	Specification of evidence content		Domain level	-
[40]	2011	Unspecified	Unspecified	Design inspections, traceability specification, inspections of high-level requirements and system-level safety requirements	-	-	Specification of evidence content	SafeSlice	Generic	Field Study
[41]	2011	Avionics	Unspecified	Non-operational testing; system historical service data specification	Argumentation-induced Evidence Structure - GSN	Quantitative Assessment - BBN	Capturing the degree of credibility or relevance of the evidence (in arguments)		Specific system type	-

[42]	2008	Avionics	Unspecified	Theorem proving; TPTP; source code review	-	-	Specification of evidence content (code generated automatically)	AUTOCERT	Generic but case study is Specific system type	Field study
[43]	2012	Avionics	Unspecified	Requirements, Design, proofs and tests, pre-flight checklist, pre-deployment checklist	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases	AdvoCATE (Assurance Case Automation Toolset)	Domain Level	Action Research
[44]	2010	Unspecified	UK Def Stan 00-56, DO 178B,	Unit test results, component historical service data, structural coverage testing, domain knowledge, hazard mitigation specification, traceability btw high level requirements and COTS components, traceability btw COTS requirements and evidence.	-	-	Specification of evidence content, Certification of system of systems (COTS)		Generic	-
[45]	2008	Unspecified	RTCA DO178B	Traceability design to low-level requirements; traceability low-level requirements to tests; requirements specification; acceptance testing; system testing	-	-	Specific need of some development activities (W model)	DOORs TraceLine	Safety standard level	-
[46]	2010	Automotive	ISO26262	PHA; safety concept; FTA; FMEDA; safety requirements specification; V&V plan; failure and monitoring requirements; safety goals and technical requirements specification; process relevant rules and requirements; safety requirements linked to the associated fault tree gates and events	-	Checklist	Ambiguities in safety standards (difficulty in applying them), Construction of safety cases (for ISO26262)	Excel Isograph ft+	Standard-level, system type-level + specific system-level	Action research?
[47]	2012	Avionics	RTCA DO178B	MC/DC coverage	-	GQM-based checklist	Specification of evidence content (audits)		Domain level	Field Study
[48]	1999	Unspecified	MIL-STD 882C, DO178B, Australian Defense Standard Def (Aust) 5679.	Configuration management plan; performance requirements specification; risk assessment results; operation procedures; interface design; operator competence; installation, maintenance and inspection procedures; simulation	-	-	Ambiguities in safety standards (framework to assess them)		Safety Standard level	-
[49]	2002	Unspecified	Unspecified	Petri Nets; Lustre; ASA.	-	Checklist	Specification of evidence content (B formal method-based)		Generic	-
[50]	1998	Railways	EN50129 [CEN.l, CEN.21 and IEC 1508 [IEC.95].	Statistical testing; acceptance testing	ACRuDA Safety Case Structure.	Checklist	Ambiguities in safety standards (planning and execution of safety assessment in the railways domain)		Safety Standard level	Field Study on DIGISAFE, SARA and EL, EKTRA.
[51]	2004	Railways	CENELEC EN50126, EN50128, ENV50129	System definition; quality manual; safety manual; technical safety report; reused component safety case; installation structure; theorem proving; risk analysis results	Textual Template - CENELEC template	Checklist	Construction of safety cases (for a legacy system)	GTO	Safety standard-level + specific system-level	Action research, survey
[52]	2011	Unspecified	ISO/IEC 14598	Functional testing; robustness testing; stress testing; reliability testing	-	-	Certification of systems made up of components and subsystems (COTS)		Safety Standard level	-
[53]	2008	Generic	Defense Standard 00-56 Issue 4 and civil standards, DO0178B / ARP4754 / ARP4761 and	FTA; functional testing; hazard causes specification; performance testing; boundary value analysis; control flow analysis, data flow analysis; developers competence	-	-	Ambiguities in safety standards (how D0178B/ARP4754/ARP4761 and lEC61508 meet the requirements of DS00-56 Issue 4)		Safety Standard level	-

			IEC61508.							
[54]	2011	Generic	Generic	Probabilistic testing; simulation; functional testing	Model-based Evidence Specification - Conceptual models	-	Specification of evidence content (agreement with certification body)	Evidence Agreement tool	Generic	-
[55]	2011	Aerospace	NASA-STD-8719	Worst-case execution time analysis; MC/DC coverage	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (in NASA)	ASCE	Specific system type	Action research on NASA critical system
[56]	2010	Aerospace	Unspecified	MTBF; FMEA; resource consumption analysis; performance analysis	-	-	Demonstration of compliance for novel technologies (MDD-based systems)	OSATE	-	Case study
[57]	2005	Aerospace	UK defense Standard	Unit testing	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Safety Evidence Assurance Level (SEAL)	Capturing the degree of credibility or relevance of the evidence (adequacy of evidence and argument)		Generic	-
[58]	1998	Unspecified	Unspecified	Competence of the development team; architecture specification	Argumentation-induced Evidence Structure - BBN	Quantitative Assessment - BBN	Construction of safety cases (evidence combination), Capturing the degree of credibility or relevance of the evidence	Hugin Explorer	Generic	-
[59]	2001	Avionics	RTCA DO178B	Component historical service data, operating experience, proven-in-use data, and item history	-	-	Certification of systems made up of components and subsystems (COTS)		Safety Standard level	-
[60]	2009	Unspecified	ISO26262	FTA,	-	-	Specification of evidence content, Capturing the degree of credibility or relevance of the evidence		Generic	-
[61]	2000	Generic	IEC61508	Safety requirements specification; SRS; performance requirements specification; scoping document; PHA; integrity requirements specification; equipment requirements specification; integration report; validation report; procedures report; development plan; verification report	Argumentation-induced Evidence Structure - GSN	-	Ambiguities in safety standards (IEC61508 in transport-infrastructure)		Standard-level + system type-level	Action research
[62]	2005	Avionics	RTCA DO178B	Unit testing; integration testing; CLawZ results, MC/DC testing, theorem proving; model checking; derived requirements specification; design specification; element under analysis (structural coverage testing); coverage percentage	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content (formal methods instead of testing)	CLawZ toolset	Safety standard level	-
[63]	1999	Generic	Unspecified	Consequence Analysis (accident specification), causal analysis (cause specification), Operational knowledge.	-	-	Specification of evidence content (V&V-based)		Generic	Action Research
[64]	2006	Avionics	RTCA DO178B	Design specification, model checking, architecture specification	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Better development processes and better evidence about process compliance (development of a dependable architecture)		Standard level	-
[65]	2007	Unspecified	Unspecified	Test plans; reused component safety case	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (developed at the time as the system)		Specific system type	-

[66]	2009	Unspecified	DO-178B, UK Defense Standard 00-56	Traceability requirements-tests; integration testing; structural coverage analysis; development plan; maintenance plan; operation plan; design method; FTA; state machines	Argumentation-induced Evidence Structure - GSN	Checklist	Capturing the degree of credibility or relevance of the evidence (formal methods-based evidence)		Safety standard level	-
[67]	2008	Aerospace and Automotive	IEC 61508, RTCA DO 178B	Model checking; statistical testing; competence of developers; suitability of notations; soundness of methods; HAZOP; FPTC; requirements inspections; software architects system experience; tool qualification report	Model-based Evidence Specification - Tree-based Process models, Argumentation-induced Evidence Structure - GSN	GQM-based checklist	Better development processes and better evidence about process compliance (reliability of development methods)		Domain Level + Safety standard level	Action research
[68]	2007	Unspecified	UK Defense STD 00-56	C/S State machine, FTA, hazard directed test results, Experience, authority and training of staffs, Safety requirement coverage assessment, Final version of the object code	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (integration of process-based and product-based perspectives)		Generic	-
[69]	2006	Generic	IEC 61508, UK Defense Standards	State machine; FTA; experience, authority and training of developers; safety requirement coverage assessment; target platform; object code; tool training; tool verification report	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content (product-based information vs. process-based information), Construction of safety cases (integration of process-based and product-based perspectives)		Safety standard level	-
[70]	2007	Unspecified	Unspecified	Model checking results; developers training and experience; requirements specification	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (relationship between goals, requirements and arguments)		Generic	-
[71]	2008	Avionics	Unspecified	Operator competence, Architecture specification, FFA; FTA,	Argumentation-induced Evidence Structure - GSN, ASCAD	-	Better development processes and better evidence about process compliance		Domain Level	-
[72]	2011	Unspecified	DO-178B, IEC 61508	Safety management plan, software development and verification plans, HAZOP, software design specification, integration test results, static analysis of code, design reviews, normal range testing, traceability specification.	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	Specification of evidence content		Generic	-
[73]	2010	Nuclear	IEC 60880, IEC 61226	Statistical testing; model checking; control flow analysis; data flow analysis; structural coverage testing; interface testing; simulation, probabilistic testing; system design specifications; QA plan; software design review; test report; FTA; ETA; common failure analysis; symbolic execution; fault injection testing; Software FFA; analysis of common cause failures; diversity analysis, path testing; design and implementation reports; software safety requirements specification; software architecture specification; unit and integration tests; software module testing	-	-	Ambiguities in safety standards (comparison of IEC60880 and IEC61508 for the nuclear domain)		Domain- level	Action research on Project CERFAS (Certification facilities for software)
[74]	2011	Unspecified	Unspecified	Design report; analysis report; Stress testing results for component; control flow analysis; functional testing	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Need for providing argumentation, Capturing the degree of credibility or relevance of the evidence in (arguments)		Generic	-
[75]	2010	Generic	Unspecified	SSR, historical service data, manual design review,	-	Qualitative	Specification of evidence content		Generic	-

				Requirements specification, code review, coverage testing/analysis, integration testing, functional testing results, HAZOP, evidence from auditing activities, V&V staff competence.		Assessment - Argumentation				
[76]	2009	Unspecified	Unspecified	HAZOP; requirements specifications	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Capturing the degree of credibility or relevance of the evidence (and arguments)		Generic	-
[77]	2001	Avionics	RTCA DO178B	MCDC Coverage, structural coverage analysis,	-	-	Specification of evidence content (V&V-based), Better development processes and better evidence about process compliance (V&V based)		Safety standard specific	-
[78]	2007	Generic	IEC 61508 [34], DO-178B [71], and the former (British) Defense Standards 00-55 and 00-56	PHA; FMECA; FTA; HAZOP; MC/DC testing	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	-	SAM	Generic	-
[79]	2010	Aerospace	NASA-STD-8719.13B	Software FTA; peer reviews and inspections of safety requirements; unit testing	-	Checklists - Taxonomy based Questionnaire (TBQ)	First-time certification or recertification of “proven-in-use” systems (legacy system)	LSRD	Generic + Safety standard level	-
[80]	2008	Unspecified	Unspecified	FTA	Argumentation-induced Evidence Structure – Structured Text	Qualitative Assessment - Argumentation	Construction of safety cases (structure)		Generic	-
[81]	2009	Unspecified	IEC61508	FMEA, fault injection test, Architecture specification and Integration Testing.	-	-	Specification of evidence content		Safety standard Level	-
[82]	2009	Railways	EN50128	Validation plan; SCADE model; C++ code; unit testing; metrics for function-code-size	(UML profile-based) GSN	Logic-based Assessment - OCL and quality model	Capturing the degree of credibility or relevance of the evidence (argument adequacy)	Extension to papyrus/Eclipse	Generic (partially applied In railways)	-
[83]	2010	Medicine	IEC 62304	Time Petri Nets; data flow and control flow analysis; model checking	Argumentation-induced Evidence Structure - GSN	Logic-based Assessment - OCL Pre and post constraints, Qualitative Assessment - Activity-based Quality model	Capturing the degree of credibility or relevance of the evidence (in argument)		Safety standard level	-
[84]	2010	Medicine	Unspecified	Model checking with Uppaal; timing analysis; code review results; worst-case execution time analysis	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases for a (pacemaker)	Uppaal model checker, AiT tool for Worst case execution time analysis	Specific system type	-
[85]	2010	Nuclear	IEC 61508, IEC60880, IEC 61513	Source code static analysis; failure injection testing; failure analysis; statistical testing; model checking; SQA plan; V&V plan; SRS; software design specification; source code; source code review;	-	-	Specification of evidence content (process-based information)		Generic	-

				module testing						
[86]	2005	Avionics	Unspecified	Hazard logs, architectural blueprints, HAZOP	Argumentation-induced Evidence Structure - GSN Models	-	Construction of safety cases		Domain- level	-
[87]	2009	Railways	IEC 61508, IEC 62278 and IEC 62279. IEC 62278	Unit testing; software integration testing; hardware integration testing	-	-	Ambiguities in safety standards (definition of safety criteria for the railways domain)		Domain-level	-
[88]	1999	Unspecified	IEC61508	Simulation, reliability block diagrams, FTA, Markov analysis, FMEDA, The Random Intelligent Failure Injection Technique (RIFIT) (simulation)	-	Design guidelines, checklists and expert experience	Specification of evidence content (V&V-based)		Safety standard level	-
[89]	2003	Avionics and Railways	UK defense standards, CENELEC 50129	Quality Management Report, Safety Management Report, Technical Safety Report, reused component specifications, FTA.	Argumentation-induced Evidence Structure - GSN	-	Construction of safety cases, Certification of system of systems (Modular Certification)		Domain level	-
[90]	2008	Multi-domain	UK Defense Standard 00-56, DO-178B.	Control flow analysis; schedulability analysis; HAZOP; FFA; failure analysis	-	-	Ambiguities in safety standards (commonalities DS00-56 and DO-178B)		Generic	-
[91]	2008	Avionics	RTCA DO178B	Reused component specification, architecture design documents, federated architecture documents (detailed design), team communication results.	-	-	Certification of systems made up of components and subsystems (COTS)		Domain Level	-
[92]	2011	Unspecified	UK Defense standards, IEC 61508, CAP 670/SW01	System historical service data specification	-	-	Construction of safety cases (scientific method-based)		Generic	-
[93]	2009	Avionics	RTCA DO-254, RTCA DO-178B	FFPA method; certified RTOS; certified complier; structural coverage testing; certified software development tools; cyclomatic complexity; MC/DC coverage; worst-case execution time; memory use; precision and stability of floating-point computations; simulation; Ada code; C code; C++ code	-	-	First-time certification or recertification of “proven-in-use” systems (Real time safety critical systems)	SofCheck & GrammaTech	Safety Standard level	Survey on tools used
[94]	1994	Others - Machinery	UK Ministry of Defense Standard 00-56	FTA, Petri net, safety quality plan, risk analysis, Safety Requirements Specification,	-	Qualitative Assessment - Argumentation	Specification of evidence content (V&V-based)	VORD	Safety Standard level	Field Study
[95]	2009	Avionics	DEF STAN 00-35, SAE ARP 4754	FMEA	-	-	First-time certification or recertification of “proven-in-use” systems (system in operation)		Generic	-
[96]	2003	Unspecified	IEC 61508 and PES Guidelines	Statistical testing; coding standards; module testing	-	Quantitative Assessment - Evidence Volume Approach (EVA)	Capturing the degree of credibility or relevance of the evidence (degree of compliance)	Unnamed tool based on Excel	Safety Standard level	-
[97]	2010	Nuclear	IEC 61508 & 60880	Structural coverage testing, Requirements specification, architectural design, traceability	-	-	Ambiguities in safety standards		Safety Standard level	-

				specification, reused components (software)						
[98]	1994	Nuclear	Unspecified	Design and requirement specifications	-	-	Ambiguities in safety standards (success factors in the nuclear domain)		Domain-level	-
[99]	2009	Avionics	Unspecified	HAZOP; human factor hazard analysis; FHA.	Argumentation-induced Evidence Structure - GSN, Model-based Evidence Specification - Entity-relationship model	Qualitative Assessment - Argumentation	Construction of safety cases (as a information modeling problem)	ASCE	System type level	-
[100]	2009	Avionics	Unspecified	Simulation; historical service data; design rules; FTA; simulation	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	Need for providing argumentation (for aircraft certification)	VAM-LIFE	Domain level	-
[101]	2007	Unspecified	Unspecified	Operational testing	-	Quantitative Assessment - BBN	Capturing the degree of credibility or relevance of the evidence (in argument)		Generic	-
[102]	1995	Multi-domain	Unspecified	Safety requirements specification; FTA; FMECA; FPTN	-	-	Specification of evidence content (formal methods-based)		Generic - multiple types of systems are targeted	Survey of the state of practice (but not based on a systematic survey approach)
[103]	2008	Avionics	UK Defense Standards	FMECA; PHA; failure analysis; functional testing	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (for a harrier)		System type level	Field study
[104]	2008	Aerospace	Unspecified	Simulation; contingencies; barriers; FMECA; FTA; analysis of fault propagation	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (how fault modeling can ease it)	TEAMS-RT	Domain- level	Filed Study on project ADAPT (Advanced Diagnostics and Prognostics Test bed)
[105]	2007	Avionics	UK Defense Standards	FHA, Z, static code analysis, SPAR, Alloy for theorem proving, FFA, FTA.	-	-	Specification of evidence content (V&V-based), Better development processes and better evidence about process compliance (V&V based)		Safety standard level	Field Study
[106]	2009	Unspecified	Unspecified	Competence of developers; CV of engineers; FTA; FMEA.	-	Checklist (qualifications gained through training prior to joining had been checked and recorded, raining and experience gained since joining the company was	Specification of evidence content (staff competence)		Generic	-

						well recorded)				
[107]	1994	Unspecified	Unspecified	FMEA; FTA; Markov analysis	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (structuring), specific of some development activities (design)		Generic	-
[108]	1991	Unspecified	UK Draft Defense Standard 00-55, DO 178a,	Failure rate	-	-	Need for providing argumentation		Generic	-
[109]	2001	Multi-domain	DS00-55, DO-178B, IEC61508, DefAust 5679, ARP4761, SW01, CAP670	MC/DC testing; FTA; FFA; HAZOP; SHARD; control flow analysis; schedulability analysis; integrity analysis; source code static analysis; analysis of memory partitioning.	Argumentation-induced Evidence Structure - GSN	Checklist (mixed with argumentation)	Ambiguities in safety standards, Specification of evidence content (product-based information vs. process-based information), Capturing the degree of credibility or relevance of the evidence (use of ALARP)		Generic + domain-level + safety standard-level	Action research
[110]	1996	Avionics	Unspecified	FTA; reliability testing; FMEA; system testing; functional configuration audits; physical configuration audit; acceptance testing	-	-	Specific need of some development activities (design)		Specific system type	Case study
[111]	2009	Avionics	DO-178B, DOD-STD- 2167A or MIL-STD-498	Development Plans, Design specification, Source Code, Executable Code, Configuration Management plans, Quality Assurance plans, traceability between the software code and the design coding standards, test plans, integration testing.			First-time certification or recertification of “proven-in-use” systems (legacy system)		Domain- level	
[112]	2009	Unspecified	UK Defense standards 00-56	HAZOP	Argumentation-induced Evidence Structure - GSN	Checklist, Qualitative Assessment - Argumentation	Capturing the degree of credibility or relevance of the evidence (sufficiency)		Generic	-
[113]	2009	Unspecified	DS 00-56 Issue 4	Design specification; development plans; verification environment; reused component safety case; experience report or user testimonial; fault logs; maintenance reports from past operation	-	Checklist (Set of guide questions that probe to see if the evidence is sufficient)	Certification of systems made up of components and subsystems (COTS)		System type level	Case study
[114]	2010	Medicine	Unspecified	Model checking; functional testing; design reviews; design checklist	-	(Design) checklist	Specification of evidence content (formal methods)	RODIN Model prover, ProB tool for model analysis	Domain level	Field study on Pacemaker software
[115]	2007	Unspecified	ISO/IEC 9126, ISO/IEC 14598 or ISO/IEC 25051	Fault injection and statistical analysis, reused component specification, RTOS (RTEMS and RTLinux), operational testing, FMEA, software Evaluation Requirement Analysis, software Evaluation Specification, software Evaluation Design.	-	-	First-time certification or recertification of “proven-in-use” systems (Real time safety critical systems)		Safety standard level	Field study
[116]	2011	Medicine	Unspecified	Assumptions about the code and the environment in which the code executes; expert knowledge about code and environment assumptions (review)	-	-	Specification of evidence content (environment and code assumptions)	Alloy based tool	At the level of software code - generic in the sense that it applies to any type of software	Case study
[117]	2011	Aerospace	Unspecified	System requirements specification, theorem proving or model checking, process standards and measurement and enforcement practices (QA plan), FMEA,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content + Construction of safety cases		Domain specific	Field Study

				integration testing, operational testing, boundary value testing, stress testing.						
[118]	2001	Railways	CENELEC (pre-) standards EN 50126, EN 50128 and prEN 50129	Requirements specification; architecture specification; interfaces specification; document versions info; quality management report; quality management plans and procedures; project's organization; project execution report; safety management report; safety requirements-source of requirements traceability; safety management plans and procedures; safety management execution report; technical safety report; assumptions and conditions specifications; manufacture report; installation procedure; test plan; facilities for operation and maintenance, developers competence; development plan	Textual Template - CENELEC template	Checklists	Construction of safety cases (for computer-based interlocking system of the railway domain)		Standard-level	Action research
[119]	2003	Railways	Unspecified	FTA; risk analysis; test plans; risk reduction methodology	-	-	Specification of evidence content (electromagnetic compatibility)		Domain-level	-
[120]	2010	Automotive	ISO26262	FMEA; competency and independence of the reviewers; quality of the development method	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (for ISO26262)		Specific system level	Field study
[121]	2010	Unspecified	IEC61508	Requirements specifications; architecture specification; operation procedures; source code; maintenance log; maintenance plan; module testing, source code review report	Model-based Evidence Specification - Conceptual models (UML class diagram)	Logic-based Assessment - OCL constraints	Specification of evidence content, Construction of safety cases (structuring of evidence)		Safety Standard level	-
[122]	2011	Maritime	IEC61508	Module testing, operator competence.	Model-based Evidence Specification - UML profiles, and conceptual models	Logic-based Assessment - OCL constraints	Specification of evidence content, use of MDE for evidence specification and analysis		Generic	Field Study
[123]	2003	Avionics	Unspecified	FTA, Probabilistic Risk Assessment, HAZOP, state charts.	-	-	Specification of evidence content (V&V-based)		Generic	Field Study
[124]	1999	Generic	EUROCAE/SAE aerospace guidelines, the CENELEC railway standards and IEC-61508	FHA; CCA; FTA; FMEA; FMES; Markov analysis; dependence diagrams; PRA; CMA; hazard log; CCS; CSP; HOL; LOTOS; OBJ; Temporal Logic; Z; B; development method; acceptance testing; integration testing	-	-	Ambiguities in safety standards (common treatment), Better development processes and better evidence about process compliance (common process model), Construction of safety cases		Safety standard level	-
[125]	2005	Avionics	Multi-Standard	FHA; operational testing; performance testing; non-regression testing, independent assessment of tests; FMEA; reliability testing	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (for air traffic control system)		Specific system level	-
[126]	1997	Generic – Defense systems fault detecting processors	UK Defense Standard	Source code static analysis; FMEA; FTA; animation	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Need for providing argumentation	SAM	System type level	Action research on Project VIPER
[127]	2004	Unspecified	IEC 61508 and MOD 00-55	Previous usage analysis; FMEA; FTA	-	-	Certification of systems made up of components and subsystems (COTS)		Safety standard level	-

[128]	2010	Avionics	RTCA DO178B	SRS; software design specification; interface design specification; source code static analysis	-	Qualitative Assessment - (Evidence) Safety Assurance Levels (and its "adaptations" for claims and architecture)	Capturing the degree of credibility or relevance of the evidence (and arguments)		Domain-level + Standard level	-
[129]	2006	Avionics	RTCA/DO-178B	FFA; FTA; FMECA; HAZOP; SHARD; emulation	-	-	Specification of evidence content (emulation)		Specific system level	Case Study
[130]	2007	Generic	UK Defense Standard	Target audience descriptions; allocation of system functions between equipment and operators; adoption of appropriate human factors guidelines and standards in the design of the system; safety features to provide protection from expected operator or equipment failures; anthropometric and workload assessments; non-operational acceptance testing; FTA; assumption and conditions specification; HAZID; evacuation studies; hazards mitigation specification; training needs analyses; operator competence; a program for monitoring operator performance and periodic review of skills; manning requirements under different operations	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content (human factors)		Safety standard level	-
[131]	2007	Automotive	ISO26262	Hazard identification and mitigation; requirements specification; requirements source (traceability); hazard checklist; PHA; traceability safety requirements-hazard; trace table hazard against safety goal; trace table safety requirement against safety goal; trace table safety goal against safety requirements; trace table safety goal against hazard; PHA; HAZOP; unit testing; C code; trace table safety requirement against element from system requirement, component, software architecture or safety concept; trace table safety concept against element from system requirement, component or software architecture	Argumentation-induced Evidence Structure - GSN	Logic-based Assessment - OCL constraints (for completeness of traceability of the GSN model)	Construction of safety cases (for ISO26262)	Toolnet	Safety standard-level	-
[132]	1999	Avionics	RTCA DO-178B/EUROCAE ED-12B	Statement coverage; MC/DC coverage; Structural coverage testing	-	-	Specification of evidence content (OO technology)		Generic	-
[133]	2010	Unspecified	Unspecified	Requirements specifications; test plans; HAZOP; FHA; FTA; model checking; FMEA	-	-	Capturing the degree of credibility or relevance of the evidence (formal methods-based assessment of arguments)		Generic	-
[134]	2007	Avionics	DO-254, lEC 61508	FTA; FMEA; HAZOP; MC/DC testing; source code review	-	Quantitative Assessment - BBN	Certification of systems made up of components and subsystems (compositional certification), Demonstration of compliance for novel technologies (adaptive systems) Construction of safety cases (goal-based)		Safety Standard level	-
[135]	2011	Avionics	RTCA DO178B	Development plans, Requirement specification, design specification, MC/DC coverage, high-level software	-	-	Ambiguities in safety standards (certification challenges for aircraft		Safety Standard level	-

				requirements, model checking, Simulation and modeling (e.g., Stateflow/Simulink), object-oriented programming.			software)			
[136]	2008	Avionics	RTCA DO178B	MC/DC testing; FTA; FMEA; specification of high- and low-level software requirements	-	-	Demonstration of compliance for novel technologies (adaptive systems)		Generic + safety standard-level	-
[137]	2011	Maritime and Energy	DNV RP-A203 and OSS-401	Simulation, maintenance procedure, environmental conditions.	Argumentation-induced Evidence Structure - GSN, KAOS	Quantitative Assessment - Modus	Specific need for some development activities	MODUS	Generic	Field Study
[138]	1995	Unspecified	IEC/SC65A	Requirements specifications; vulnerability analysis source code walkthroughs; source code static analysis; HAZOPS; FMEA; FTA; ETA	Argumentation-induced Evidence Structure - SSG	-	Capturing the degree of credibility or relevance of the evidence		Safety standard level	-
[139]	2011	Unspecified	Unspecified	FTA; development plan; coding guidelines; operational testing	-	-	Demonstration of compliance for novel technologies (open adaptive systems)		System type level	-
[140]	2006	Unspecified	IEC61508	V&V pan; FTA; FMECA; HAZOP; theorem proving; model checking; UML modeling (design); MatLab/Simulink (simulation and modeling); functional testing; SWIFI and EMFI testing; configuration management plan; V&V tools	-	Checklist	Specification of evidence content (V&V-based), Better development processes and better evidence about process compliance (V&V), Construction of safety cases (for V&V)	DECOS test bench	Safety standard-level	Field study
[141]	1994	Unspecified	Multi-Standard	Target staff specification; system requirements specification; hazard log; safety program plan; safety criteria report; PHA; independent safety audit report; system design specification; safety compliance assessment report, safety audit report; safety compliance assessment report; independent safety audit report review	-	-	Ambiguities in safety standards		Safety standard level	-
[142]	2006	Unspecified	Unspecified	Validation plan, theorem proving, formal code inspections, written records from code inspections, pair-programming, syntax and static analysis, lambda calculus.	-	-	Better development processes and better evidence about process compliance (record and maintenance of V&V activities)	Programatica, DevCOP SCMS Eclipse Plug-in	Generic	-
[143]	2004	Medicine	Unspecified	Hazard barriers/mitigation; HAZOP; FMEA; environmental conditions; reused components specification; user competence; user manual; operation procedures; safety culture; user experience; FHA; safety requirements specification; review of different operating procedures; user training; operational performance testing	-	-	Specification of evidence content (barriers to hazards)		Generic + specific system-level	Action research
[144]	2003	Avionics	Unspecified	Configuration control records; design specifications; developers competence; simulation	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Ambiguities in safety standards (autonomous vehicles)		Domain level	-
[145]	2005	Unspecified	DEF-STAN 00-55 and 00-56, MIL-STD-882C, ARP 4761, ARP 4754, IEC 61508, DEF AUST 5679 and RTCA/DO-178B	FTA, HAZOP, SHARD, Software Deviation Analysis.	-	Qualitative Assessment - Argumentation	Ambiguities in safety standards		Safety Standard level	-

[146]	2010	Avionics	RTCA DO178B	System requirements specification; high-level requirements specification; low-level requirements specification; functional requirements specification; performance requirements specification; interface requirements; safety requirements; source code; normal range testing; robustness testing; FMECA; FTA	-	-	Demonstration of compliance for novel technologies (model-based testing)		Domain-level	-
[147]	2011	Unspecified	IEC61508	Functional testing; module testing; integration testing; boundary value analysis; equivalence classes testing; input partition testing; simulation.	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (goal-based, reuse)		Safety standard level	-
[148]	2010	Unspecified	UK Defense Standard 00-56, IEC 61508, DO-178B	Development and V&V staff competence, safety committee meeting reports and a diary of meeting dates should be provided (activity records), traceability specification, risk management, Hazard Identification.	-	-	Specification of evidence content (V&V-based), Better development processes and better evidence about process compliance (V&V based)	Unnamed tool	Safety standard specific	-
[149]	2011	Unspecified	Unspecified	HAZOP; FTPC; FFA; FMEA; HEP; HRA	-	-	Certification of systems made up of components and subsystems (hazard analysis), Construction of safety cases (for systems of systems)		Generic	-
[150]	2007	Medicine	UK Medical Devices Regulations 2002 (MDR 2002), Medical Devices Directive, IEC60601-1	Risk analysis results; risk management process; reused component specification; communication channels (between service provider, device manufacturer and corresponding regulatory authorities); installation procedure; maintenance procedure; training and support to the operational staff; user manual; incidents registration procedure; performance monitoring procedures; changes impact assessed procedures; audit of product quality assurance system; organizational communication and education materials; human factors analysis	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (for medical devices)	ASCE	Domain-level	-
[151]	2011	Avionics	DO 178B, SAE ARP 4754A, DO-297/ED-124,	Configuration management report; FTA; state machines; hazard directed test results; human factors analysis	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (for an aircraft)		Safety standard level	-
[152]	2003	Unspecified	UK Defense standards, DO 178B,	Safety audit reports, architecture specification, development and safety management plans, hazard and accident identification, causal and consequence analysis, hazard mitigation, specification, hazard log report, safety plan, PHA, SHA, Hazard Log Report, Safety Requirements.	-	-	Construction of safety cases	eSafetCase Toolset	Generic	-
[153]	2001	Multi-domain	IEC 61508, UK Defense Standard 00-54,55,56	FTA, FMEA, FHA, tool and test audits, Operational experience, inspection, historical data, timing analysis result.	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (maintenance)	SAM	Generic	-
[154]	2010	Avionics	EC 61508, DO178B, DS 00-55	HAZOP, historical service data of previous hazards, code reviews, static code analysis	Argumentation-induced Evidence Structure - GSN, CAE	-	Specification of evidence content		Domain specific	-
[155]	2007	Avionics	RTCA DO178B	FTA, architecture specification, coding standards	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Certification of systems made up of components and subsystems (Modular systems)		Domain specific	Field study

[156]	2008	Automotive	ISO 26262, MISRA safety guidelines	Traceability specification	-	-	Construction of safety cases		Domain- level	Survey (Interviews with domain experts)
[157]	2010	Railways	CENELEC standards EN50126, EN50128 and EN50129	PHA, FTA, hazard log, safety requirements, traceability of the requirements flow down, architectural design, Independent Verification and Validation, Quality assurance of the development process, requirements traceability between models and formal requirements, Review and static analysis at the model level to guarantee compliance to modeling standards, Functional verification of the models by using requirements based test vectors, Automatic code generation with built in traceability between the source code and the models, Code review, Equivalence testing, System Requirements Specification; safety Requirements Specification, Safety Assessment Report.	-	-	Suitability to safety standards, Specification of evidence content		Safety standard level + specific system type	-
[158]	1999	Medicine	IEC1508	User manual, system requirements, architecture specification, test procedures, inspection procedures, Requirements Specification, Design Specification, coding standards.	-	-	Specification of evidence content (V&V-based), Better development processes and better evidence about process compliance (V&V based)		Safety standard specific	-
[159]	2010	Automotive	IEC61508	Fault pattern libraries; Testing using fault injection; Simulation; Simulink/Stateflow/TargetLink models	Argumentation-induced Evidence Structure - GSN Models	Qualitative Assessment - Argumentation	Ambiguities in safety standards (safety assurance methods for the automotive domain)		Domain-level + System type level	Case study
[160]	2002	Maritime	Unspecified	PHA, FMECA and HAZOP.	-	-	Construction of Safety cases (for ships)		Domain level	Field Study
[161]	2005	Unspecified	Unspecified	Causal analysis; FTA; state machines; hazard directed test results	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Need for providing argumentation		Generic	-
[162]	2003	Unspecified	Unspecified	FTA, FMEA.	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - SAL	Capturing the degree of credibility or relevance of the evidence (in a safety case)		Generic	-
[163]	2006	Unspecified	Unspecified	CV of developers	-	-	Capturing the degree of credibility or relevance of the evidence (in safety case)		Generic	
[164]	1996	Unspecified	Unspecified	Reliability testing; common mode failure analysis; FMECA; FTA; ETA; HAZOP; FFA	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Capturing the degree of credibility or relevance of the evidence	SAM	Generic	Field Study
[165]	2006	Avionics	DoD 2167, MIL-Std 498, IEEE 12207, Mil-Std 882c, IEC1508, IEC 61508, DefStan 00-55, DefStan 00-56, CENELEC	FTA; FMECA; Functional FMEA; FFA; hazard log; reliability testing; historical service data specification; customer feedback reports; design review; reliability, availability and maintainability modeling and prediction reports; module testing; integration testing; hazard checklist; hazard log	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (for voice communication system)		Safety standard level	-

			50126, 50128, 50129.							
[166]	2006	Avionics	RTCA DO178B	Data coupling analysis; control coupling analysis; timing analysis; memory analysis; software integration testing; hardware-software integration testing; Robustness testing	-	-	Certification of systems made up of components and subsystems (software component reuse)		Domain-level	-
[167]	2007	Avionics	ARP4761	Competence of the allocated development team; FTA	Argumentation-induced Evidence Structure - GSN	Quantitative Assessment - BBN (OOBBN)	Specification of evidence content (architecture-based)	Hugin Explorer	Generic	-
[168]	2007	Unspecified	Unspecified	FTA; ETA; FFA	Argumentation-induced Evidence Structure - GSN	Quantitative Assessment - BBN	Specification of evidence content (design-based)		Generic	Field study
[169]	2009	Avionics	RTCA DO178B	Historical service data	-	-	Ambiguities in safety standards (and comparison among them)		Safety Standard level	-
[170]	2004	Unspecified	Unspecified	FTA; historical service data; HAZOP	-	Qualitative Assessment - SAL	Certification of systems made up of components and subsystems (COTS based systems)		Generic	-
[171]	2012	Unspecified	IEEE 603	QA activities report; historical service data	-	Qualitative Assessment - Evidence-confidence conversion process	Better development processes and better evidence about process compliance (efficiency of the certification process)	Markup tool unnamed	Domain level + Safety standard level	-
[172]	2011	Avionics	RTCA DO178B	Traceability of requirements through design elements, source code and object code; software design and implementation techniques; safety requirements specifications; PSAC	Model-based Evidence Specification - UML profiles, and conceptual models	Logic-based Assessment - OCL	Better development processes and better evidence about process compliance (communication and collaboration among stakeholders)		Safety Standard Level	Field Study
[173]	2011	Automotive	ISO26262	Safety Requirements Specification, simulation, safety plan, project plan	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases	ASCE	Standard level	-
[174]	2012	Avionics	RTCA/DO-178B	Operating System, code review, code inspection, branch coverage testing, test plan, boundary values testing, test case specification	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	Capturing the degree of credibility or relevance of the evidence , Need for providing argumentation	Visio plugin for GSN and ASCE	Specific system level	Action Research
[175]	2012	Avionics	RTCA/DO-178B and DO178C	PHA, SSHA, FMEA, FTA, concepts of operation, operating procedures, assumptions made in theoretical models (of flight control / aerodynamic stability), simulations and computational models, proof of correct implementation, results of reviewing the corresponding specification, data sheets for the air-data (pitot) probe, the results of wind tunnel experiments to calibrate the probe, theorem proving, formal proofs of specification, requirement specification, hazard logs, hazard analysis results, traceability specification, event trees, formal proofs that the code correctly implements the formalized software safety requirements.	Argumentation-induced Evidence Structure - BBN	Quantitative Assessment - BBN	Construction of safety cases	AUTOCERT	Specific system level	-
[176]	2007	Medicine	ISO 14971:2000	Risk analysis results, system historical information.	Argumentation-induced Evidence Structure - Trust cases		Ambiguities in safety standards	TCT editor	Standard level	N

[177]	2012	Unspecified	IEC 61508	User competency, review of safety manual.	Argumentation-induced Evidence Structure - BBN	Quantitative Assessment - BBN (Using AND/OR)	Capturing the degree of credibility or relevance of the evidence (in argument)	None	Generic	N
[178]	2007	Unspecified	IEC 61508, DO178B	Statistical testing, MCDC testing, static analysis, model checking, SAT solvers,			Ambiguities in safety standards	None	Standard level	N
[179]	2009	Avionics	D0-178B	Safety assessment plan, Requirements test Specification, Integration test specification, PHA, Safety plan, Acceptance testing, module testing, Detailed hazard analysis, data coupling analysis, control coupling analysis, timing analysis, memory analysis, stack analysis, software integration testing, requirements-based test coverage, hardware-software integration testing, robustness testing of component functions			Specification of evidence content (for Reused components)		Generic	
[180]	2004	Generic - FPGA	Unspecified	Manual code inspection, operational testing, CRC checks, model checking, traceability of source code and compilation levels, simulation and coverage testing, requirements-based testing, design specification, syntactic checker for checking syntax with language reference manual, traceability of code to requirements, Code reviews, Control flow analysis, Data flow analysis, Information flow analysis, Range checking, Main memory usage analysis, Stack usage analysis, Timing analysis, Worst case analysis, Object code analysis, Equivalence class testing, boundary testing, statement coverage testing, branch coverage testing, MCDC, static analysis, traceability analysis, Unit testing and scenario-based testing,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content		System specific	None
[181]	2001	Unspecified	UK def standards, DO178B, DO254, IEC61508,	Worst Case execution time analysis, static code analysis, manual code review, hardware/software integration testing, control flow analysis, data flow analysis, code inspection, FTA,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Certification of systems made up of components and subsystems (COTS)		System specific	None
[182]	2010	Multi domain	IEC 61508 and ISO 26262, RTCA DO-178B	Unit testing, Integration testing, functional testing, performance testing, Requirements Traceability, modeling and coding guidelines, functional, requirements-based testing, simulation, tool qualification, Architecture and design specification			Better development processes and better evidence about process compliance (V&V activities, design and implementation)		Standard level	None
[183]	2004	Unspecified	UK Def standards	Execution time analysis, exhaustive testing, single fault criterion testing, MTTF, MTTR, reliability testing, staff compliance & experience, static analysis, code review	Argumentation-induced Evidence Structure - GSN, CAE		Safety case Development (Goal based safety cases)	SAM	Generic	None
[184]	2000	Avionics	Unspecified	Markov Models			Better development processes and better evidence about process compliance (V&V activities)		Domain Level	None
[185]	1998	Unspecified	DOD-STD-2167A	"Project Management Plan (PMP), Software Quality Programme Plan (SQPP), Software Development Plan (SDP), Software Quality Evaluation Plan (SQEP), Software Configuration Management Plan (SCMP - split out from SDP), Formal Qualification Testing (FQT), Software Safety Programme Plan (SSPP), Operational Concept Document (OCD), System/Segment Specification (SSS), System/Segment Design Document (SSDD), Software	Argumentation-induced Evidence Structure - Structured text with HTML tags		Safety case Development	HTML webpage		

				Requirements Specification (SRS), Software Design Document (SDD), Software Test Plan (STP), Software Test Description - procedures (STD), Software Test Description - cases (STD), Software Test Results (STR), Software Users Manual (SUM), Software Programmers Manual (SPM), Computer Resources Integrated Support Manual (CRISD), RAM Analysis (RAM), FMECA, FT, List of Risks (LoR) or Hazard Analysis (HA), Hazard Analysis Report, V&VReport						
[186]	2001	Unspecified	Unspecified	Field service experience	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	Safety case Development (Reuse of safety cases)	ASCE, SAM	Generic	None
[187]	2011	Avionics	Unspecified	FHA, Monte Carlo simulation, Model checking,			First-time certification or recertification of “proven-in-use” systems (Unmanned Autonomous systems)	Unnamed tool	Domain Level	Action Research
[188]	2002	Space	IEC 61508, UK def standards	Execution time analysis, Exhaustive testing, Coding standards, reliability testing, Staff competence and experience, statistical testing, design reviews, configuration management, coverage testing, module testing, requirements based testing, operational testing, stress testing, regression testing, inspection, walkthroughs, static analysis (control and data flow), semantic analysis, simulation,			Better development processes and better evidence about process compliance (V&V activities, design and implementation)		Domain Level	Action Research
[189]	2011	Railways	DO 178B, SAE ARP 4761,	FHA, FTA, FMEA, SDP, SRS, SDD, STP, STD (Software test Description), Software Requirements Review (SWRR) and the Preliminary and Critical Design Reviews (PDR and CDR), Structural coverage testing, MCDC testing, Configuration management plan, Development plan, QA plan, Requirements Specification, Functional FMEA, traceability specification, coding standards, static analysis of code (code complexity analysis, reachability analysis, and data-flow analyses),			Better development processes and better evidence about process compliance (V&V activities), Specification of evidence content		Standard level	None
[190]	2006	Space	Unspecified	SFMECA, SFTA, Bi- Directional Safety Analysis (BDSA= SFMECA + SFTA),		Qualitative Assessment - Argumentation	Better development processes and better evidence about process compliance (V&V activities)		Domain Level	None
[191]	2008	Automotive	IEC 61508	Traceability specification between requirements and models, Traceability specification between models and code, Traceability specification between models and test cases, requirements based testing, structural coverage testing, Integration testing, MCDC testing, Equivalence testing			Better development processes and better evidence about process compliance (V&V activities)		Standard Level	None
[192]	2009	Robotics	IEC 61508	Theorem proving, formal proofs,			Capturing the degree of credibility or relevance of the evidence (Formal method based evidence)		Standar level	Action Research
[193]	2006	Avionics	Unspecified	Operator competence,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Capturing the degree of credibility or relevance of the evidence (Confidence in safety case)		Domain level	Survey
[194]	2002	Unspecified	IEC 61508	Expert Judgment, Probabilistic risk assessments use of system components which are certified by accepted independent authorities (System historical service data), simulation and modeling, design philosophies, operating procedures and emergency mitigation procedures,	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	Construction of safety cases (Structuring of Evidence)	ASCE, SAM	Generic	None

[195]	2010	Automotive	ISO26262	Design Specification and traceability among them, Environmental assumptions, SysML Models, Hazard Classification review reports, simulation and in-service history.	Argumentation-induced Evidence Structure - GSN		Construction of safety cases (Structuring of Evidence, Association and integration of process based and product based perspectives)		Standar level	
[196]	2010	Unspecified	UK Def standards, IEC 61508 and DO178B	Statistical testing, operational experience, hazard logs, state machine analysis, team competency, testing traceability, Model checking, theorem Proving,	Argumentation-induced Evidence Structure - GSN		Specification of evidence content		Generic	None
[197]	2000	Aerospace	ARP-475, ARP- 4761, DS 00-5, DS 00-56, MilStd 882C	MTTF, WCRT			Certification of systems made up of components and subsystems (Modular certification)		Domain Level	None
[198]	2008	Aerospace	DO 178B	software verification plan, requirements specification, Software review, simulation, tatic analysis, code reviews, traceability analyses, and coverage analyses,Software Verification Test Cases and Procedures, Plan for Software Aspects of Certification (PSAC),Monte Carlo analysis,			Demonstration of compliance for novel technologies (Open adaptive systems)		Domain Level	None
[199]	2009	Automotive	ISO26262	Modelling, FMEA, FTA, Requirements Sepcification,			Better development processes and better evidence about process compliance		Standard Level	None
[200]	2010	Unspecified	IEC 61508	fault tree analysis, data flow diagrams, simulations, configuration management and structured programming, traceability specification, Hazard identification specification, hazard mitigation specification, Software management plan, software development plan, QA plan, integration plan, maintainence plan, training plan, operation plan, safety plan, Configuration management plan, Requirements specification, Design specification, Architecture specification, code listings, system build documents, operation manuals, installation,configuration tables, maintainence manuals, training manuals, Requirements analysis and reports, design analysis and reports, code implementation and test analysis and reports, intergration and test analysis and reports, validation and test analysis and reports, installation and test analysis and reports, change analysis and report, CM requirements report, CM design report, CM implementation report, CM integration report, CM validation report, CM installation report, CM chnage report, FHA,			Better development processes and better evidence about process compliance		Standard Level	None
[201]	2004	Unspecified	UK Def standards	FTA, FMEA, Hazard logs, Requirments specification, safety plan audits, reviews, Tools specification, black box test results, C/S State machines, Hazard directed test results, safety plans, PHA, HAZOP, High level system description,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (Structuring of Evidence)		Generic	None
[202]	2004	Unspecified	UK Def standards	FTA,FMEA,black box test results, C/S State machines, Hazard directed test results	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (Structuring of Evidence)		Generic	None
[203]	2006	Aerospace	ARP4754 and ARP4761	FTA, FMEA, FMES, FMECA, raceability between design and analysis artefacts, Failure Logic Models, Failure injection			Better development processes and better evidence about process compliance		Generic	Action Research

[204]	2003	Aerospace	ARP4754 and ARP4761	PSSA, FHA, FFA, safety requirements specification, FTA, FMEA, FMES, CCA, Architechture specification, System safety analysis (SSA), inspection or analysis of the software specification, HAZOP, SHARD,			Better development processes and better evidence about process compliance		Standard level	Action Research
[205]	2000	Aerospace	ARP4754 and ARP4762	Zonal analysis, Requirements specification,	Argumentation-induced Evidence Structure - GSN		Certification of systems made up of components and subsystems (Modular certification)		Domain level	None
[206]	2007	Railways	CENELEC standards	Requirements specification,			Better development processes and better evidence about process compliance (Design and implementation)		Domain level	None
[207]	1998	Unspecified	Unspecified	State machines, Simulation and animation, Design reviews and checks,			Better development processes and better evidence about process compliance (V&V)	DOVE	Generic	None
[208]	2008	Avionics	DO178B/C	MCDC testing, FMEA, FTA, software requirements specification, source code			Construction of safety cases		Domain/Standard level	None
[209]	2010	Unspecified	Def Stan 00-56	hazard analysis,FMEA, configuration control, traceability and test coverage analysis, test evidence concerned with the transformation from the SCADE input source to the equivalent C code, expert analysis of potential failure conditions using architectural models and systematic analysis, HAZOP, MCDC coverage testing, traceability from the failure conditions to the data-flow architectural model of the KCG tool, staff competence Safety management, Configuration management, software unit test reports, functional test results and coverage data, SCADE validation evidence for software safety requirement,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Specification of evidence content (automatically generated code)	KCG qualified code generator	Standard level	None
[210]	2000	Unspecified	Unspecified	Software testing plan, software testing reports, requiremenrts specification, design specification,			Specification of evidence content		Generic	None
[211]	2000	Maritime & energy	Multi-standards	FTA, Consequence analysis, ETA, Structural review of risks, requirements analysis, safety requirements specifications , Systematic audit to confirm the safety requirements specifications meets software, semantic analysis, software reliability growth models (SRGMs), formal methods like Z; Vienna Development Method (VDM); Communicating Sequential Processes (CSP); and Calculus of Communicating System (CCS), FMECA, PHA,			Specification of evidence content (formal methods instead of testing)		Domain Level	None
[212]	1999	Avionics	DEF STAN 00-55 , DO 178B	FTA, ETA, FMEA, HAZOP, static code analysis, Flow analysis; Semantic analysis; Compliance analysis, control flow, data flow and information flow analysis, bench mark testing,			Better development processes and better evidence about process compliance (V&V)	Exception analyser	Domain Level	Action Research
[213]	2008	Unspecified	Def(Aust) 5679	SSR, CSR, formal modelling of the System Safety requirements, a formal architecture model, formalisation of the Component Safety Requirements, and a formal proof that the Component Safety Requirements taken together satisfy the System Safety Requirements with B Models, Safety Management Plan, Safety Case Summary, Safety Review Report, Hazard analysis report, safety architecture report (requirements for documenting the Criticality Assessment and the Architecture Test Plan), Desgin and assurance report (requirements for documenting the Design Testing Plan, Implementation Technology, Component Safety Specifications (CSSs), a Design			Ambiguities in safety standards		Standard level	None

				Model, Design Verification, Maintenance Design), Safety Evaluation Plan, Safety Evaluation Report, safety personnel competencies, plans for configuration management, document control,Operating Manual,						
[214]	1995	Unspecified	Unspecified	the results of hardware reliability calculations, Common mode failure analysis, PHA, hazard log, HAZOP, FFA, FTA, ETA, FMECA, Risk tables, MTBF, QA plan,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Construction of safety cases (Goal based safety cases)	SAM	Generic	None
[215]	2004	Unspecified	Unspecified	control-flow analysis results, Preliminary Hazard Identification (PHI), System Hazard Analysis (SHA), FTA			Certification of systems made up of components and subsystems (COTS)		Generic	None
[216]	2011	Unspecified	Unspecified	HAZOP, FTA, MCDC testing, manual code review and automatic code analyzer,	Argumentation-induced Evidence Structure - GSN, CAE	Qualitative Assessment - Argumentation	Capturing the degree of credibility or relevance of the evidence (Arguments and their adequacy)		Generic	None
[217]	2002	Unspecified	Unspecified	FMEA, static code analysis, analysis of scheduling and timing failures, WCET, competency of the development personnel, configuration control, system historical data,	Argumentation-induced Evidence Structure - GSN	Qualitative Assessment - Argumentation	Ambiguities in safety standards , Need for providing argumentation		Generic	

Abreviations and Definitions

ACRuDA	Assessment and Certification Rules for Digital Architectures
ASA	Automated and Structured Analysis
ASCAD	Adelard Safety Claims Arguments Data
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
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
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
KAOS	Keep All Objectives Satisfied
MDE	Model-Driven Engineering
MC/DC	Modified Condition/Decision Coverage
MMEL	Master Minimum Equipment List
MTBF	Mena Time Between Failures
MTTF	Mean Time To Failure
OCL	Object Constraint Language
OS	Operating System
PHA	Preliminary Hazard Analysis
PRA	Particular Risk Analysis
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
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
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
V&V	Verification and Validation

References:

[1] Alan Wassyng, Tom Maibaum, Mark Lawford, and Hans Bherer. Software certification: is there a case against safety cases?. In *Proceedings of the 16th Monterey conference on Foundations of computer software: modeling, development, and verification of adaptive systems* (FOCS'10), Radu Calinescu and Ethan Jackson (Eds.). (2010)

[2] Althammer, E., Schoitsch, E., Sonneck, G., Eriksson, H., Vinter, J.: Modular certification support - the DECOS concept of generic safety cases. In: 6th IEEE International Conference on Industrial Informatics (INDIN 2008) (2008)

[3] Andersen, B.S., Romanski, G.: Verification of Safety-critical Software. Queue 9(8) (2011)

[4] Anderson, K. J.: Common Law Safety Case Approaches to Safety Critical Systems Assurance. In: Redmill, F., Anderson, T. (eds.) Developments in Risk-based Approaches to Safety, Part4, pp 171-183). Springer, London (2006)

[5] Ankrum, T.S., Kromholz, A.H.: Structured assurance cases: three common standards. In: 9th IEEE International Symposium on High-Assurance Systems Engineering (HASE 2005) (2005)

[6] Arthasartsri, S., Ren, H.: Validation and verification methodologies in A380 aircraft reliability program. In: 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009) (2009)

[7] Bain, A.D., Dobson, S.: Safety Cases for Legacy Warships: A Systematic Approach. In: 3rd IET International Conference on System Safety (2008)

[8] Basir, N., Denney, E., Fischer, B.: Constructing a Safety Case for Automatically Generated Code from Formal Program Verification Information. In: Harrison, M., Sujan, M.A. (eds.) SAFECOMP 2008, LNCS 5219, pp 249-262. Springer, Heidelberg (2008)

[9] Basir, N., Denney, E., Fischer, B.: Deriving Safety Cases for Hierarchical Structure in Model-Based Development. In E. Schoitsch (ed.) SAFECOMP 2010, LNCS 6351, pp 68-81. Springer, Heidelberg (2010)

[10] Basir, N., Denney, E., Fischer, B.: Deriving Safety Cases for the Formal Safety Certification of Automatically Generated Code. Electronic Notes in Theoretical Computer Science 238(4): 19-26 (2009)

[11] Basir, N., Denney, E., Fischer, B.: Deriving safety cases from automatically constructed proofs. In: 4th IET International Conference on Systems Safety (2009)

[12] Bate, I., Conmy, P., McDermid, J.: Generating evidence for certification of modern processors for use in safety-critical systems. In: 5th IEEE International Symposim on High Assurance Systems Engineering (HASE 2000) (2000)

[13] Bate, I., Conmy, P.: Certification of FPGAs - Current Issues and Possible Solutions. In: Dale, C., Anderson, T. (eds.), Safety-Critical Systems: Problems, Process and Practice, pp 149-165. Springer, London (2009)

[14] Bate, I., Kelly, T.: Architectural Considerations in the Certification of Modular Systems. Reliability Engineering & System Safety 81(3): 303-324 (2003)

[15] Becker, U.: Applying Safety Goals to a New Intensive Care Workstation System. In: Harrison, M., Sujan, M.A. (eds.) SAFECOMP 2008, LNCS 5219, pp 263-276. Springer, Heidelberg (2008)

[16] Benediktsson, O., Hunter, R. B. and McGettrick, A. D. Processes for software in safety critical systems. Softw. Process: Improve. Pract., (2001),

[17] Benet, A. F. A Risk Driven Approach to testing Medical Device Software. In C. Dale & T. Anderson (Eds.), *Advances in Systems Safety Proceedings of the 19th SafetyCritical Systems Symposium* (pp. 157-168). Springer London. (2011).

[18] Bertolino, A., Strigini, L.: Assessing the risk due to software faults: estimates of failure rate versus evidence of perfection. Software Testing, Verification and Reliability 8(3): 155-166 (1998)

[19] Bilich, C., Hu, Z.: Experiences with the Certification of a Generic Functional Safety Management Structure According to IEC 61508. In: Buth, B., Rabe, G., Seyfarth, T. (eds.) SAFECOMP 2009, LNCS 5775, pp 103-117. Springer, Heidelberg (2009)

[20] Bishop, P., Bloomfield, B.: A Methodology for Safety Case Development. In: Industrial Perspectives of Safety-Critical Systems: Proceedings of the 6th Safety-critical Systems Symposium (SSS'98) (1998)

[21] Bishop, P., Bloomfield, R., Littlewood, B., Povyakalo, A., Wright, D.: Toward a Formalism for Conservative Claims about the Dependability of Software-Based Systems. IEEE Transactions on Software Engineering 37(5): 708-717 (2011)

[22] Bloomfield, R., Bishop, P.: Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective. In Dale, C., Anderson, T. (eds.) Making Systems Safer, pp. 51-67. Springer, London (2010)

[23] Bouissou, M., Martin, F., Ourghanlian, A.: Assessment of a safety-critical system including software: a Bayesian belief network for evidence sources. In: Annual Reliability and Maintainability Symposium (1999)

[24] Brown, A.; Fenn, J; Menon, C.; , "Issues and considerations for a modular safety certification approach in a Service-Oriented Architecture," *System Safety 2010, 5th IET International Conference on*. (2010)

[25] Brown, M.J.D.: Rationale for the development of the UK defense standards for safety-critical computer software. IEEE Aerospace and Electronic Systems Magazine 5(11): 31-37 (1990)

[26] Burns, A., McDermid, J.A.: Real-time safety-critical systems: analysis and synthesis. Software Engineering Journal 9(6): 267-281 (1994)

[27] Camus, J.L.: Efficient development of safety-critical software. IET Electronic Systems and Software 1(1): 38-43 (2003)

[28] Caseley, P. R., & Hadley, M. J. (2006). Assessing the effectiveness of static code analysis. *1st IET International Conference on System Safety* (Vol. 2006, pp. 227-237). Iee. doi:10.1049/cp:20060221

[29] Caseley, P.R., White, T.A.D.: The MOD procurement guidance on software safety assurance - assessing and understanding software evidence. In: 4th IET International Conference on Systems Safety (2009)

[30] Chinneck, P., Pumfrey, D., McDermid, J.: The HEAT/ACT preliminary safety case: a case study in the use of goal structuring notation. In: 9th Australian workshop on Safety critical systems and software (SCS '04) (2004)

[31] Cichocki, T.: Safety Case Development - How can I continue the work? In: Redmill, F., Anderson, T. (eds.) Improvements in Systems Safety, pp 59-76. Springer, London (2008)

[32] Clegg, J.R.: Arguing the safety of FPGAs within safety critical systems. 4th IET International Conference on Systems Safety (2009)

[33] Conmy, P., Bate, I.: Component-Based Safety Analysis of FPGAs. In: IEEE Transactions on Industrial Informatics 6(2): 195-205 (2010)

[34] Conmy, P., Paige, R.F.: Challenges when using Model Driven Architecture in the development of Safety Critical Software. In: 4th International Workshop on Model-Based Methodologies for Pervasive and Embedded Software (MOMPES '07) (2007)

[35] Corrie, J.D.; , "Safety assurance and safety assessment," *Railway Signalling and Control Systems, 2006. The 11th IET Professional Development Course,* June (2006)

[36] Cruz-Neira, C., & Lutz, R. R. Using immersive virtual environments for certification. *IEEE Software*, *16*(4), 26-30. (1999).

[37] Czerny, B.J., D'Ambrosio, J.G., Murray, B.T.: Providing convincing evidence of safety in X-by-wire automotive systems. In: 5th IEEE International Symposium on High Assurance Systems Engineering. (HASE 2000) (2000)

[38] Dahll, G.: Combining disparate sources of information in the safety assessment of software-based systems. Nuclear Engineering and Design 195(3): 307-319 (2000)

[39] Daniel Schneider and Mario Trapp. Conditional safety certificates in open systems. In *Proceedings of the 1st Workshop on Critical Automotive applications (*2010)

[40] Davide Falessi, Shiva Nejati, Mehrdad Sabetzadeh, Lionel Briand, and Antonio Messina. SafeSlice: a model slicing and design safety inspection tool for SysML. In *Proceedings of the 19th ACM SIGSOFT symposium and the 13th European conference on Foundations of software engineering* (ESEC/FSE '11) (2011)

[41] Denney, E., Pai, G., Habli, I.: Towards Measurement of Confidence in Safety Cases. In: International Symposium on Empirical Software Engineering and Measurement (ESEM 2011) (2011)

[42] Denney, E., Trac, S.: A Software Safety Certification Tool for Automatically Generated Guidance, Navigation and Control Code. In: IEEE Aerospace Conference (2008)

[43] E. Denney, G. Pai, A lightweight methodology for safety case assembly, in: Computer Safety, Reliability, and Security, Springer, 2012, pp. 1-12.

[44] Despotou, G., Bennett, M., & Kelly, T. Evaluation and Integration of COTS in Evidence based Assurance Frameworks. In C. Dale & T. Anderson (Eds.) (2010)

[45] Dick, A.J.J., Wills, S.C.B.: Evidence-Based Development - Applying Safety Engineering Techniques to the Progressive Assurance and Certification of Complex Systems. In: 3rd IET International Conference on System Safety (2008)

[46] Dittel, T., Aryus, H.J.: How to "Survive" a Safety Case According to ISO 26262. In: Schoitsch, E. (ed.) SAFECOMP 2010, LNCS 6351, pp 97-111. Springer, Heidelberg (2010)

[47] Dodd, I., Habli, I.: Safety certification of airborne software: An empirical study. Reliability Engineering & System Safety 98(1): 7-23 (2012)

[48] Eastaughffe, K.A., Cant, A., Ozols, M.A.: A framework for assessing standards for safety critical computer-based systems. In: 4th IEEE International Symposium and Forum on Software Engineering Standards (1999)

[49] El Koursi, E.M., Mariano, G.: Assessment and certification of safety critical software. In: 5th Biannual World Automation Congress (2002)

[50] El Koursi, E.M., Meganck, P.: Assessment criteria for safety critical computer. In: 1998 IEEE International Conference on Systems, Man, and Cybernetics (1998)

[51] Eriksson, L.H.: Using Formal Methods in a Retrospective Safety Case. In: Heisel, M., Liggesmeyer, P., Wittmann, S. (eds.) SAFECOMP 2004, LNCS 3219, pp 31-44. Springer, Heidelberg (2004)

[52] Esposito, C., Cotroneo, D., Barbosa, R., Silva, N.: Qualification and Selection of Off-the-Shelf Components for Safety Critical Systems: A Systematic Approach. In: 5th Latin-American Symposium on Dependable Computing Workshops (LADCW 2011) (2011)

[53] Evans, J.R., Kelly, T.P.: Defense Standard 00-56 Issue 4 and Civil Standards - Appropriateness and Sufficiency of Evidence. In: 3rd IET International Conference on System Safety (2008)

[54] Falessi, D., Briand, L., Sabetzadeh, M., Turella, E., Coq, T., Panesar-Walawege, R.: Planning for Safety Evidence Collection: A Tool-Supported Approach Based on Modeling of Standards Compliance Information. IEEE Software (accepted paper) (2011)

[55] Feather, M.S., Markosian, L.Z.: Building a Safety Case for a Safety-Critical NASA Space Vehicle Software System. In: IEEE 4th International Conference on Space Mission Challenges for Information Technology (SMC-IT 2011) (2011)

[56] Feiler, P.H.: Model-based validation of safety-critical embedded systems. In: 2010 IEEE Aerospace Conference (2010)

[57] Fenn, J., Jepson, B.: Putting Trust into Safety Arguments. In: Redmill, F., Anderson, T. (eds.) Constituents of Modern System-safety Thinking, pp 21-35. Springer, London (2005)

[58] Fenton, N., Littlewood, B., Neil, M., Strigini, L., Sutcliffe, A., Wright, D.: Assessing dependability of safety critical systems using diverse evidence. In: IEE Proceedings Software Engineering 145(1): 35-39 (1998)

[59] Ferrell, T.K.; Ferrell, U.D.; , "Use of service history for certification credit for COTS," *Digital Avionics Systems, 2001. DASC. 20th Conference*. (2001)

[60] Forster, M., & Trapp, M. Fault tree analysis of software-controlled component systems based on second-order probabilities. *Proceedings International Symposium on Software Reliability Engineering ISSRE* (Vol. Compendex, pp. 146-154). (2009).

[61] Fowler, D., Bennett, P.: IEC 61508 - A Suitable Basis for the Certification of Safety-Critical Transport-Infrastructure Systems?? In: Koornneef, F., van der Meulen, M. (eds.) SAFECOMP 2000, LNCS 1943, pp 250-263. Springer, Heidelberg (2000)

[62] Galloway, A., Paige, R.F., Tudor, N.J., Weaver, R.A., Toyn, I., McDermid, J.: Proof vs testing in the context of safety standards. 24th Digital Avionics Systems Conference (DASC 2005) (2005)

[63] Good, J.; Blandford, A.; , "Incorporating human factors concerns into the design and safety engineering of complex control systems," *Human Interfaces in Control Rooms, Cockpits and Command Centres, 1999. International Conference on* , vol., no., pp.51-56, 21-23 Jun (1999)

[64] Graydon, P., Knight, J., & Strunk, E. Achieving Dependable Systems by Synergistic Development of Architectures and Assurance Cases. In R. De Lemos, C. Gacek, & A. B. Romanovsky (Eds.), *Architecting Dependable Systems IV* (Vol. 4615, pp. 362-382). Springer. (2006).

[65] Graydon, P.J., Knight, J.C., Strunk, E.A.: Assurance Based Development of Critical Systems. In: 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07) (2007)

[66] Habli, I., Kelly, T. A Generic Goal-Based Certification Argument for the Justification of Formal Analysis. Electronic Notes in Theoretical Computer Science 238(4): 27-39 (2009)

[67] Habli, I., Kelly, T.: A Model-Driven Approach to Assuring Process Reliability. In: 19th International Symposium on Software Reliability Engineering (ISSRE 2008) (2008)

[68] Habli, I., Kelly, T.: Achieving integrated process and product safety arguments. In. Redmill, F., Anderson. T. (eds.) The Safety of Systems, Part 2, pp 55-68. Springer, London (2007)

[69] Habli, I., Kelly, T.: Process and product certification arguments: getting the balance right. ACM SIGBED Review 3(4): 1-8 (2006)

[70] Habli, I., Wu, W., Attwood, K., Kelly, T.: Extending Argumentation to Goal-Oriented Requirements Engineering. In: Hainaut, J.L., et al. (eds.) ER Workshops 2007, LNCS 4802, pp 306-316. Springer, Heidelberg (2007)

[71] Hall, J., & Rapanotti, L. Assurance-driven design. *Software Engineering Advances 2008 ICSEA 08 The Third International Conference on*, 379-388. IEEE Computer Society Press. (2008).

[72] Hamilton, V. Accounting for Evidence: Managing Evidence for Goal Based Software Safety Standards. In C. Dale & T. Anderson (Eds.), (pp. 41-51). Springer London. (2011).

[73] Harju, H., Lahtinen, J., Ranta, J., Nevalainen, R., Johansson, M.: Software Safety Standards for the Basis of Certification in the Nuclear Domain. In: 7th International Conference on the Quality of Information and Communications Technology (QUATIC 2010) (2010)

[74] Hawkins, R., Kelly, T., Knight, J., Graydon, P.: A New Approach to creating Clear Safety Arguments. In: Dale, C., Anderson, T. (Eds.) Advances in System Safety, pp 3-23. Springer, London (2011)

[75] Hawkins, R.; Kelly, T.; , "A structured approach to selecting and justifying software safety evidence," *System Safety 2010, 5th IET International Conference*. (2010)

[76] Hawkins, R.D., Kelly, T.P.: Software safety assurance - what is sufficient? In: 4th IET International Conference on Systems Safety (2009)

[77] Hayhurst Kelly J. and Veerhusen Dan S... A Practical Approach to Modified Condition/Decision Coverage. Technical Report. NASA Langley Technical Report Server. (2001)

[78] Heimdahl, M.P.E.: Safety and Software Intensive Systems: Challenges Old and New. In: 2007 Future of Software Engineering (FOSE'07) (2007)

[79] Hill, J., Tilley, S.: Creating Safety Requirements Traceability for Assuring and Recertifying Legacy Safety-Critical Systems. In: 18th IEEE International Requirements Engineering Conference (RE'10) (2010)

[80] Holloway, C.M.: Safety Case Notations: Alternatives for the Non-Graphically Inclined? In: 3rd IET International Conference on System Safety (2008)

[81] Hu, Z., & Bilich, C. Experience with Establishment of Reusable and Certifiable Safety Lifecycle Model within ABB. Computer Safety Reliability and Security (Vol. 5775, pp. 132-144). Springer Berlin Heidelberg. . (2009).

[82] Huhn, M., Zechner, A.: Analyzing Dependability Case Arguments Using Quality Models. In: Buth, B., Rabe, G., Seyfarth, T. (eds.) SAFECOMP 2009, LCNS 5775, pp 118-131. Springer, Heidelberg. (2009)

[83] Huhn, M., Zechner, A.: Arguing for Software Quality in an IEC 62304 Compliant Development Process. In: Margaria, T., Steffen, B. (eds.) ISoLA 2010, Part II, LNCS 6416, pp 296-311. Springer, Heidelberg (2010)

[84] Jee, E., Lee, I., Sokolsky, O.: Assurance Cases in Model-Driven Development of the Pacemaker Software. In: Margaria, T., Steffen, B. (eds.) ISoLA 2010, Part II, LNCS 6416, pp 343-356. Springer, Heidelberg (2010).

[85] Johansson, M., Nevalainen, R.: Additional requirements for process assessment in safety–critical software and systems domain. Journal of Software Maintenance and Evolution: Research and Practice (2010)

[86] Jolliffe, G.; , "Producing a safety case for IMA blueprints," *Digital Avionics Systems Conference, 2005. DASC 2005.* (2005)

[87] Joung, E., Oh, S., Park, S., Kim. G.: Safety criteria and development methodology for the safety critical railway software. In: 31st International Telecommunications Energy Conference (INTELEC 2009) (2009)

[88] Karydas, D. M., & Brombacher, A. C. Reliability certification of programmable electronic systems. *Reliability Engineering System Safety*, . (1999).

[89] Kelly T. P., "Managing Complex Safety Cases," *in Proceedings of 11th Safety Critical System Symposium (SSS'03),* Springer (2003)

[90] Kelly, T. P.: Can Process-Based and Product-Based Approaches to Software Safety Certification be Reconciled? In: Redmill, F., Anderson, T. (eds.) Improvements in Systems Safety, pp 3-12. Springer, London (2008)

[91] Kesseler, E. Assessing COTS software in a certifiable safety-critical domain. Information Systems Journal, 18: 299–324. (2008),

[92] Kinnersly, S.: Safety Cases – what can we learn from Science? In: Dale, C., Anderson, T. (eds.) Advances in System Safety, pp. 25-40. Springer, London (2011)

[93] Kornecki, A., Zalewski, J.: Certification of software for real-time safety-critical systems: state of the art. Innovations in Systems and Software Engineering 5(2) 149-161 (2009)

[94] Kotonya, G., & Sommerville, I. Integrating safety analysis and requirements engineering. *Software Engineering Conference*, (1994).

[95] Kritzinger, D.: Safety cases & safety assessments. In: 4th IET International Conference on Systems Safety (2009)

[96] Kuball, S., Hughes, G.: Decision-support for certification by calculating the evidential volume of a product. In: 2003 International Conference Dependable Systems and Networks (2003)

[97] Lahtinen, J., Johansson, M., Ranta, J., Harju, H., & Nevalainen, R. Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the Nuclear Domain. In E. Schoitsch (Ed.), (Vol. 6351, pp. 55-67) (2010).

[98] Lawrence, J.D., Persons, W.L., Preckshot, G.G., Gallagher, J.: Evaluating software for safety systems in nuclear power plants. In: 9th Annual Conference on Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security (COMPASS'94) (1994)

[99] Lewis, R.: Safety Case Development as an Information Modelling Problem. In: Dale, C., Anderson, T. (eds.) Safety-Critical Systems: Problems, Process and Practice, pp 183-193. Springer, London (2009)

[100] Linling, S. Kelly, T.: Safety arguments in aircraft certification. In: 4th IET International Conference on Systems Safety (2009)

[101] Littlewood, W.; Wright, D.; , "The Use of Multilegged Arguments to Increase Confidence in Safety Claims for Software-Based Systems: A Study Based on a BBN Analysis of an Idealized Example," *Software Engineering, IEEE Transactions on* , vol.33, May (2007)

[102] Liu, S., Stavridou, V., Dutertre, B. The practice of formal methods in safety-critical systems. Journal of Systems and Software 28(1): 77-87 (1995)

[103] Lucas, J.: Safety Case Experiences from Harrier. In: Redmill, F., Anderson, T. (eds.) Improvements n System Safety, pp 77-91. Springer, London (2008)

[104] Lutz, R., Patterson-Hine, A.: Using Fault Modeling in Safety Cases. In: 19th International Symposium on Software Reliability Engineering (ISSRRE 2008) (2008)

[105] Mannering, D., Hall, J., & Rapanotti, L. Safety process improvement with POSE and Alloy. *Improvements in System Safety* (Vol. 4680, pp. 252-257). Springer. (2007).

[106] Mayo, P.R.: Creating a competence argument to support a safety case. In: 4th IET International Conference on Systems Safety (2009)

[107] McDermid, J.A.: Proving the design in the safety case. IEE Colloquium on Designing Safety-Critical Systems (1994)

[108] McDermid, J.A.: Safety arguments, software and system reliability. In: 1991 International Symposium on Software Reliability Engineering (1991)

[109] McDermid, J.A.: Software safety: where's the evidence? In: 6th Australian workshop on Safety critical systems and software (SCS '01) (2001)

[110] McDonnell, S., Melhart, B.E.: Software assessment to support certification for an existing computer-based system. In: IEEE Symposium and Workshop on Engineering of Computer-Based Systems (1996)

[111] Meacham, D.J.; Michael, J.B.; Man-Tak Shing; Voas, J.M.; , "Standards interoperability: Applying software safety assurance standards to the evolution of legacy software," *System of Systems Engineering, 2009. SoSE 2009. IEEE International Conference (*2009)

[112] Menon, C., Hawkins, R., McDermid, J.: Defense Standard 00-56 Issue 4: Towards Evidence-Based Safety Standards. In: Dale, C., Anderson, T. (eds.) Safety-Critical Systems: Problems, Process and Practice, Part 7, pp 223-243. Springer, London (2009)

[113] Menon, C., McDermid, J., Hubbard, P.: Goal-based safety standards and cots software selection. In: 4th IET International Conference on Systems Safety 2009 (2009)

[114] Méry, D., Singh, N.K.: Trustable formal specification for software certification. In: Margaria, T, Steffen, B. (eds.) ISoLA 2010, Part II, LNCS 6416, pp 312-326. Springer, Heidelberg (2010)

[115] Moraes, R., Durães, J., Martins, E., & Madeira, H. Component-Based Software Certification Based on Experimental Risk Assessment. In A. Bondavalli, F. Brasileiro, & S. Rajsbaum (Eds.), (2007).

[116] Near, J.P., Milicevic, A., Kang, E., Jackson, D.: A lightweight code analysis and its role in evaluation of a dependability case. In: 33rd International Conference on Software Engineering (ICSE '11) (2011)

[117] Nguyen, E.A.; Ellis, A.G.; , "Experiences with Assurance Cases for Spacecraft Safing," *Software Reliability Engineering (ISSRE), 2011 IEEE 22nd International Symposium* Dec (2011)

[118] Nordland, O.: Presenting a Safety Case - A Case Study - In: Voges, U. (ed.) SAFECOMP 2001, LNCS 2187, pp 56-65. Springer, Heidelberg (2001)

[119] Ogunsola, A., Pomeroy, S.: EMC assurance and safety critical apparatus in a railway environment. In: 2003 IEEE International Symposium on Electromagnetic Compatibility (EMC'03) (2003)

[120] Palin, R., Habli, I.: Assurance of Automotive Safety - A Safety Case Approach. In: Schoitsch, E. (ed.) SAFECOMP 2010, LNCS 6351, pp 82-96. Springer, Heidelberg (2010)

[121] Panesar-Walawege, R.K., Sabetzadeh, M., Briand, L., Coq, T.: Characterizing the Chain of Evidence for Software Safety Cases: A Conceptual Model Based on the IEC 61508 Standard. In: 3rd International Conference on Software Testing, Verification and Validation (ICST 2010) (2010)

[122] Panesar-Walawege, R.K.; Sabetzadeh, M.; Briand, L.; , "A Model-Driven Engineering Approach to Support the Verification of Compliance to Safety Standards," *Software Reliability Engineering (ISSRE), 2011 IEEE 22nd International Symposium (*2011)

[123] Papadopoulos, Y. Model-based system monitoring and diagnosis of failures using statecharts and fault trees. *Reliability Engineering System Safety*, *81*(3), 325-341. (2003).

[124] Papadopoulos, Y., McDermid, J.A.: The Potential for a Generic Approach to Certification of Safety-Critical Systems in the Transportation Sector. Reliability Engineering & System Safety 63(1): 47-66 (1999)

[125] Pierce, R., Baret, H.: Structuring a Safety Case for an Air Traffic Control Operations Room. In: Redmill, F., Anderson, T. (eds.) Constituents of Modern System-safety Thinking, pp 51-64. Springer, London (2005)

[126] Pygott, C., Wilson, S.P.: Justifying reliability claims for a fault-detecting parallel architecture, Journal of Systems Architecture 43(10): 735-751 (1997)

[127] Redmill, F.: Analysis of the COTS debate. Safety Science 42(5): 355-367 (2004)

[128] Reinhardt, D. W., McDermid, J.A.: Assurance of claims and evidence for aviation systems. In: 5th IET International Conference on System Safety (2010)

[129] Reinhardt, D.: Certification criteria for emulation technology in the Australian defense force military avionics context. In: 11th Australian workshop on Safety critical systems and software (SCS'06) (2006)

[130] Rich, K.J.N., Blanchard, H., McCloskey, J.: The Use of Goal Structuring Notation as a Method for Ensuring that Human Factors is Represented in a Safety Case. In: 2nd IET International Conference on System Safety (2007)

[131] Ridderhof, W., Gross, H.G., Doerr, H.: Establishing Evidence for Safety Cases in Automotive Systems - A Case Study. In: Saglietti, F., Oster, N. (eds.) SAFECOMP 2007, LNCS 4680, pp 1-13. Springer, Heidelberg (2007)

[132] Rierson, L.K.: Object-oriented technology (OOT) in civil aviation projects: certification concerns. In. 18th Digital Avionics Systems Conference (1999)

[133] Rushby, J. Formalism in Safety Cases. In: Dale, C., Anderson, T. (eds.) Making Systems Safer, pp 3-17. Springer, London (2010)

[134] Rushby, J.: Just-in-Time Certification. In: 2th IEEE International Conference on the Engineering of Complex Computer Systems (ICECCS 2007) (2007)

[135] Rushby, J.: New Challenges In Certification For Aircraft Software. In: 9th ACM international conference on Embedded software (EMSOFT'11) (2011)

[136] Rushby, J.: Runtime Certification. In: Leucker, M. (ed.) SAFECOMP 2008, LNCS 5289, pp 21-35. Springer, Heidelberg (2008)

[137] Sabetzadeh, M., Falessi, D., Briand, L., di Alesio, S., McGeorge, D., Ahjem, V., Borg, J.: Combining Goal Models, Expert Elicitation, and Probabilistic Simulation for Qualification of New Technology. In: 213th IEEE International Symposium on High-Assurance Systems Engineering (HASE 2011) (2011)

[138] Saeed, A., de Lemos, R., Anderson, T.: On the safety analysis of requirements specifications for safety-critical software. ISA Transactions 34(3): 283-285 (1995)

[139] Schneider, D., Trapp, M.: A Safety Engineering Framework for Open Adaptive Systems. In: 5th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2011) (2011)

[140] Schoitsch, E., Althammer, E., Eriksson, H., Vinter, J., Gönczy, L., Pataricza, A., Csertan, G.: Validation and Certification of Safety-Critical Embedded Systems - The DECOS Test Bench. In: J. Górski (ed.) SAFECOMP 2006, LNCS 4166, pp 372-385. Springer, Heidelberg (2006)

[141] Shaw, R.: Safety-critical software and current standards initiatives. Computer Methods and Programs in Biomedicine 44(1): 5-22 (1994)

[142] Sherriff, M., Williams, L.: DevCOP: A Software Certificate Management System for Eclipse. In: 17th International Symposium on Software Reliability Engineering (ISSRE 2006) (2006)

[143] Smith, S., Harrison, M., Schupp, B.: How Explicit Are the Barriers to Failure in Safety Arguments? In: Heisel, M., Liggesmeyer, P., Wittmann, S. (eds.) SAFECOMP 2004, LNCS 3219, pp 325-337. Springer, Heidelberg (2004)

[144] Spriggs, J.: Developing a Safety Case for Autonomous Vehicle Operation on an Airport. In: 11th Safety-critical system symposium (2003)

[145] Squair, M.J.: Issues in the Application of Software Safety Standards. In: 10th Australian workshop on Safety critical systems and software (SCS'05) (2005)

[146] Stallbaum, H., Rzepka, M.: Toward DO-178B-compliant Test Models. In: 2010 Workshop on Model-Driven Engineering, Verification, and Validation (MoDeVVa) (2010)

[147] Stensrud, E., Skramstad, T., Li, J., Xie, J.: Towards Goal-Based Software Safety Certification Based on Prescriptive Standards. In: 1st International Workshop on Software Certification (WoSoCER 2011) (2011)

[148] Stephenson, Z. R., & McDermid, J. A. Supporting explicit interpretation of standards and guidance. *5th IET International Conference on System Safety 2010*, (2010).

[149] Stephenson, Z., Fairburn, C., Despotou, G., Kelly, T., Herbert, N., Daughtrey, B.: Distinguishing Fact from Fiction in a System of Systems Safety Case. In: Dale, C., Anderson, T. (eds.) Advances in Systems Safety, pp 55-72. Springer, London (2011)

[150] Sujan, M.A., Koornneef, F., Voges, U.: Goal-Based Safety Cases for Medical Devices: Opportunities and Challenges. In: Saglietti, F., Oster, N. (eds.) SAFECOMP 2007, LNCS 4680, pp 14-27. Springer, Heidelberg (2007)

[151] Sun Linling, Zhang Wenjin, Tim Kelly, Do safety cases have a role in aircraft certification?, Procedia Engineering, Volume 17, 2011, Pages 358-368, (2011)

[152] T. Cockram and B. Lockwood, "Electronic Safety Case: Challenges and Opportunities," in Safety-Critical Systems, Current Issues, techniques and standards, F. Redmill and T. Anderson, Eds., ed, (2003)

[153] T.P Kelly, J.A McDermid, A systematic approach to safety case maintenance, Reliability Engineering &amp; System Safety, Volume 71, Issue 3, March (2001)

[154] Tangming Yuan, Tianhua Xu, "Computer System Safety Argument Schemes," wcse, vol. 2, pp.107-110, 2010 Second WRI World Congress on Software Engineering, (2010)

[155] Tim Kelly. Using software architecture techniques to support the modular certification of safety-critical systems. In *Proceedings of the eleventh Australian workshop on Safety critical systems and software - Volume 69* (SCS '06) (2007)

[156] Torner, F.; Ohman, P.; "Automotive Safety Case A Qualitative Case Study of Drivers, Usages, and Issues," *High Assurance Systems Engineering Symposium, 2008. HASE 2008*. (2008)

[157] Valk, J.-L., Vis, H., & Koning, G. Phileas, a Safety Critical Trip around the World. In C. Dale & T. Anderson (Eds.), (pp. 115-126). Springer London. (2010).

[158] Varley, P. Techniques for development of safety-related software for surgical robots. *IEEE transactions on information technology in biomedicine a publication of the IEEE Engineering in Medicine and Biology Society*, *3*(4), 261-267. . (1999).

[159] Wagner, S., Schätz, B., Puchner, S., Kock, P.: A Case Study on Safety Cases in the Automotive Domain: Modules, Patterns, and Models. In: IEEE 21st International Symposium on Software Reliability Engineering (ISSRE 2010) (2010)

[160] Wang, J.: Offshore safety case approach and formal safety assessment of ships. Journal of Safety Research 33(1): 81-115 (2002)

[161] Weaver, R., Despotou, G., Kelly, j., MsDermid, J.: Combining Software Evidence – Arguments and Assurance. In: 2005 Workshop on Realising Evidence-Based Software Engineering (REBSE'05) (2005)

[162] Weaver, R., Fenn, J., Kelly, T.: A pragmatic approach to reasoning about the assurance of safety arguments. In: 8th Australian workshop on Safety critical systems and software (SCS'03) (2003)

[163] Weaver, R., Kelly, T., Mayo, P.: Gaining Confidence in Goal-based Safety Cases. In: Redmill, F., Anderson, T. (ds.) Developments in Risk-based Approaches to Safety, pp 277-290. Springer, London (2006)

[164] Wilson, S., McDermid, J.A., Kirkham, P.M., Fenelon, P.: The Safety Argument Manager: an integrated approach to the engineering and safety assessment of computer based systems. In: IEEE Symposium and Workshop on Engineering of Computer-Based Systems (1996)

[165] Winkelbauer, W., Schedl, G., Gerstinger: A. Safety Case Practice - Meet the Challenge. In: Redmill, F., Anderson, T. (eds.) Developments in Risk-based Approaches to Safety, pp 83-104. Springer, London (2006)

[166] Wlad, J.: Software Reuse in Safety-Critical Airborne Systems. In: 25th Digital Avionics Systems Conference (2006)

[167] Wu, W., Kelly, T.: Combining Bayesian Belief Networks and the Goal Structuring Notation to Support Architectural Reasoning About Safety. In: Saglietti, F., Oster, N. (eds.) SAFECOMP 2007, LNCS. 4680, pp 172-186. Springer, Heidelberg (2007)

[168] Wu, W., Kelly, T.: Towards Evidence-Based Architectural Design for Safety-Critical Software Applications. In: de Lemos, R., Gacek, C., Romanovsky, A. (eds.) Architecting Dependable Systems IV, LNCS 4615, pp 383-408. Springer, Heidelberg (2007)

[169] Yan, F.: Comparison of means of compliance for onboard software certification. In: 4th International Conference on Computer Science & Education (ICCSE'09) (2009)

[170] Ye, F., Kelly, T.: Contract-based justification for COTS component within safety-critical applications. In: 9th Australian workshop on Safety critical systems and software (SCS '04) (2004)

[171] Yih, S., Fan, C.F.: Analyzing the decision making process of certifying digital control systems of nuclear power plants. Nuclear Engineering and Design 242: 379-388 (2012)

[172] Zoughbi, G., Briand, L., Labiche, Y.: Modeling safety and airworthiness (RTCA DO-178B) information: conceptual model and UML profile. Software and Systems Modeling 10(3): 337-367 (2011)

[173] Palin, R., Ward, D., Habli, I., & Rivett, R.: ISO 26262 safety cases: Compliance and assurance. System Safety, 2011 6th IET, 1-6. (2011).

[174] Patrick Graydon, Ibrahim Habli, Richard Hawkins, Tim Kelly, John Knight,.: "Arguing Conformance," IEEE Software, vol. 29, no. 3, pp. 50-57 (2012).

[175] Denney, E., Pai, G., & Habli, I.: Perspectives on software safety case development for unmanned aircraft. IEEE/IFIP International Conference on Dependable Systems and Networks. DSN. (2012).

[176] Lukasz Cyra and Janusz Gorski.: Supporting Compliance with Security Standards by Trust Case Templates. In Proceedings of the 2nd International Conference on Dependability of Computer Systems (DEPCOS-RELCOMEX. (2007).

[177] Hobbs, C., & Lloyd, M.: The Application of Bayesian Belief Networks to Assurance Case Preparation. In C. Dale & T. Anderson (Eds.), Achieving Systems Safety SE - 12. pp. 159-176. (2012)

[178] Thomas, M.: Unsafe Standardization. Computer 40, 11 (November), 109-111. (2007).

[179] Åkerholm, M., & Land, R.: Towards Systematic Software Reuse in Certifiable Safety-Critical Systems. *International Workshop on Software Reuse and safety,* 3-7. (2009)

[180] I. Bate, S. Bates, J. McDermid.: Safety Arguments for use of an Ada to FPGA Compiler. Proceedings of the 22nd International System Safety Conference (2004)

[181] Bate, I., Conmy, P., Kelly, T., & McDermid, J.: Use of modern processors in safety-critical applications. *The Computer Journal*, *44*(6). (2001)

[182] Beine, M.: A Model-Based Reference Workflow for the Development of Safety-Critical Software. *Embedded Real Time Software and Systems* 1-6. (2010)

[183] Bishop, P., Bloomfield, R., & Guerra, S.: The future of goal-based assurance cases. In workshop *on Assurance Cases. (2004)*

[184] Limnios, N. MAINTENANCE OPTIMISATION OF A DIGITAL ENGINE CONTROL SYSTEM WITH LIMIT FAILURE RATE CONSTRAIN. In 22nd Congress of International Council of the Aeronautical Sciences, Harrogate, U. (2000)

[185] Brown,R.: "Improving the Production and Presentation of Safety Cases through the use of Intranet Technology". In Safety Critical Systems Club Symposium paper. (1998)

[186] Bush, D., & Finkelstein, A.: Reuse of safety case claims-an initial investigation. Proceedings of the London Communications Symposium, University College London 10th -11th September (2001)

[187] Cameron N et al.: Certification of a Civil UAS: A Virtual Engineering Approach. Proceedings of the 2011 AIAA Modelling SImulation and Technologies Conference and Exhibit. AIAA, Portland, Oregon pp 1 -15. (2011)

[188] Cleland, G. L., Blanquart, J. P., Carranza, J. M., Froome, P. K. D., Jones, C. C. M., & Muller, J. F.: A Framework for the Software Aspects of the Safety Certification of a Space System. In Joint ESA-NASA Space-Flight Safety Conference. (2002).

[189] Coe, D., Hogue, J., & Kulick, J. (n.d.). Software Safety Engineering Education. world-comp.org. Retrieved from http://world-comp.org/p2011/SER4081.pdf. (2011)

[190] J. Dehlinger and R. Lutz.: "Bi-Directional Safety Analysis For Product-Line, Multi-Agent Systems," Workshop on Innovative Techniques for Certification of Embedded Systems. (2006).

[191] I Fey-Safety, M Consultants, M Conrad,: Model-Based Design for Safety-Related Applications. In proceedings of Convergence. (2008)

[192] Udo Frese, Daniel Hausmann, Christoph L, Holger Taubig, and Dennis Walter.: The Importance of Being Formal. Electron. Notes Theoritical Computer Science. (2009).

[193] William S. Greenwell, John C. Knight, C. Michael Holloway, Jacob J. Pease.: A taxonomy of fallacies in system safety arguments. In Proceedings of the 2006 International System Safety Conference (2006)

[194] Gurr, C.: Argument Representation for Dependable Computer-Based Systems" Informal Logic. (2002).

[195] Habli, I., Ibarra, I., Rivett, R., & Kelly, T.: Model-based assurance for justifying automotive functional safety. Proc. 2010 SAE World. (2010)

[196] Habli, I., Hawkins, R., & Kelly, T.: Software safety: relating software assurance and software integrity. International Journal of Critical Computer-Based Systems. (2010).

[197] Nicholson M, Hollow P and McDermid JA. Approaches to Certification of Reconfigurable IMA Systems. INCOSE 2000, Minneapolis, USA, July (2000)

[198] Stephen Jacklin,: Closing the Certification Gaps in Adaptive Flight Control Software, Proc. 26th AIAA Applied Aerodynamics Conference, (2008)

[199] O Kath, R Schreiner, J Favaro.: Safety, Security and Software Reuse: A Model-Based Approach, In RESAFE 2009, 4th Int Workshop in Software Reuse and Safety. (2009)

[200] Katta, V., & Stalhane, T. A conceptual model of traceability for safety systems. CSDM-Poster Presentation, 1-12. (2010).

[201] Kelly, T. A systematic approach to safety case management. Proc. of SAE 2004 World Congress, Detroit, MI. (2004).

[202] Kelly, T., & Weaver, R.: The goal structuring notation–a safety argument notation. Proc. DSN 2004 Workshop on Assurance Cases. (2004).

[203] Lisagor, O., McDermid, J.A. and Pumfrey, D.J (2006) 'Towards a practicable process for automated safety analysis', inProceedings of the 24th International System Safety Conference (ISSC), Albuquerque, New Mexico, USA, August.

[204] Nicholson, M., and J. McDermid.: Extending PSSA for Complex Systems."Proceedings of the 21st International System Safety Conference (2003)

[205] Nicholson, Mark, et al.: Generating and maintaining a safety argument for integrated modular systems. In 5th Australian Workshop on Industrial Experience with Safety Critical Systems and Software. (2000)

[206] Ossami, D-D. Okalas, et al.: A method to model guidelines for developing railway safety-critical systems with UML.In Proceedings of the International Conference on Software and Technologies (2007)

[207] Ozols, M. A., et al.: DOVE: A tool for design modelling and verification in safety critical systems.In 16th International System Safety Conference. (1998)

[208] Rushby, John.: How Do We Certify For The Unexpected?.In AIAA Guidance, Navigation and Control Conference and Exhibit. (2008)

[209] Stephenson, Zoë, Tim Kelly, and Jean-Louis Camus.: Developing an Argument for Def Stan 00-56 from Existing Qualification Evidence. In Embedded Real-Time Software and Systems (2010)

[210] Vilkomir, Sergiy A., and Vjacheslav S. Kharchenko.: An 'Asymmetric'approach to the assessment of safety-critical software during certification and licensing. Project Control: the Human Factor, In Proceedings of ESCOM–SCOPE 2000 Conference. (2000)

[211] Wang, J.: Analysis of safety-critical software elements in offshore safety studies. *Disaster Prevention and Management* 9.4 (2000)

[212] Whiting, Liz, and Mike Hill.: Safety analysis of hawk in flight monitor. In *ACM SIGSOFT Software Engineering Notes* 24.5 (1999)

[213] Wildman, Luke, et al.: Guidance for Def (Aust) 5679 Issue 2. In *13th Australian Conference on Safety Related Programmable Systems, Australian Computer Society, System Safety and Quality Engineering Pty Ltd*.(2008)

[214] Wilson, S. P., Tim P. Kelly, and John A. McDermid.: Safety case development: Current practice, future prospects." *Proceedings 1st ENCRESS/12th Annual CSR Workshop*. (1995)

[215] Ye, Fan, and Tim Kelly.: Use of COTS Software Components in Safety-Critical Applications–A Defensible Approach. In *IEE Seminar Digests*. Vol. 907. (2004)

[216] Yuan, Tangming, and Tim Kelly.: Argument schemes in computer system safety engineering. In *Informal Logic* 31.2 (2011)

[217] Weaver, R. A., J. A. McDermid, and T. P. Kelly.: Software safety arguments: Towards a systematic categorisation of evidence. In *International System Safety Conference, Denver, CO*. (2002)