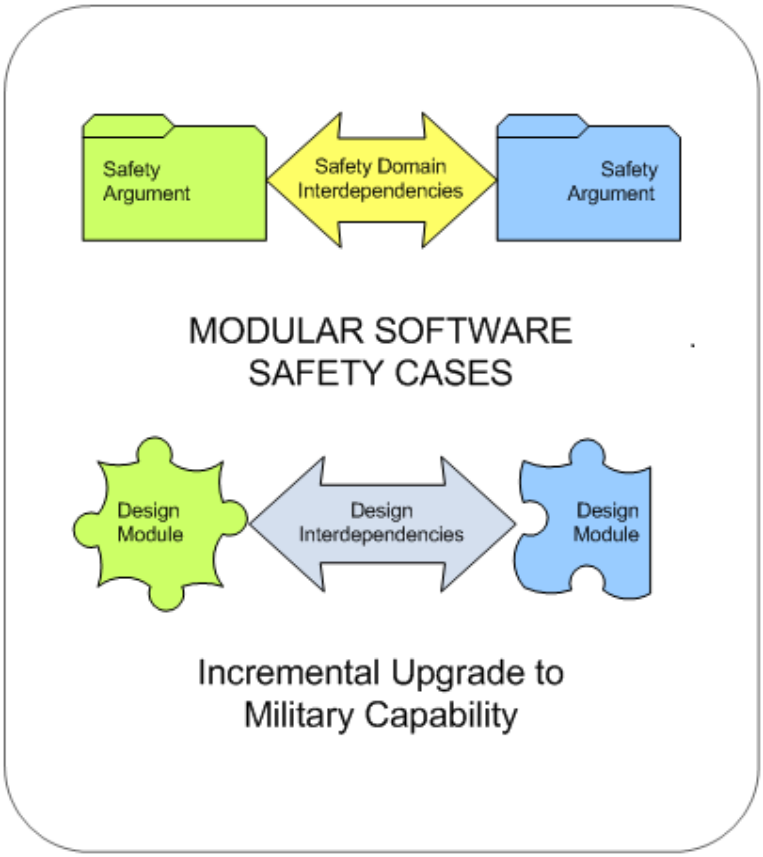
Modular Software Safety Case Process Glossary

Date: 19-Nov-2012



Glossary

Term	Abbrev'n	Explanation / Elaboration
Acquirer		An organisation that procures products for itself or another organisation.
Adequately Safe		This expression is used to mean that something is safe enough for the particular environment and manner in which it will be used. Where this expression is used in a SC those aspects must be precisely defined. (Used interchangeably with Sufficiently Safe.)
Allied Standards Avionics Architecture Council	ASAAC	A consortium, formed by European government and industry representatives (UK, France, Germany) established with the objectives of exploring IMA concepts, and defining and validating a set of Open Architecture Standards, Concepts & Guidelines for an Advanced Avionics Architecture applicable to new aircraft and upgrade programmes.
Application Layer	AL	In the context of IMS, the Application layer is that part of the software which gives the system the specific functionality typically defined in its operational specification. Other (generic) layers are considered to support the running of this software.
Application Manager	AM	Software which performs platform-specific management to control non-generic aspects of system management.
Application Programming Interface	API	The language and message format which must be used by one software component (e.g. an application program) to communicate with another (e.g. an operating system of a processor).
Architecture (Design domain)		The organisational structure of a system identifying its component parts, their interfaces, and a concept of execution between them.
Architecture (Safety Case)		The organisational structure of a Safety Case Document identifying the Safety Case Modules, their interactions and the interfaces between them.
Argument		A structured set of logical steps in which the conclusions from a previous step (or some new evidence) form the premise(s) of a subsequent step.
	ARINC	Aeronautical Radio, Incorporated
Artefact		A work product which records and report the results of completing an activity, such as a step of a process.
As Low as Reasonably Practicable	ALARP	A requirement that the risk must be reduced not merely to a tolerable level but also to a level which is as low as reasonably practicable.
Assumption		Acknowledgedly unsubstantiated statement that highlights a claim that is taken for granted by the central argument.
Assurance		The provision of argument and evidence, through due process, to establish confidence that safety requirements have been met.

Term	Abbrev'n	Explanation / Elaboration
Block		An identifiable part (or group of parts) of the S/W implementation that is chosen by the SC Architect to be the subject of a Safety Case Module.
	BIT	Built-in Test
Catastrophic Severity		A term used when classifying hazards based on of the seriousness of their impacts. A hazard of Catastrophic Severity could result in complete mission failure, death or loss of system.
Cell		An element of S/W implementation that is to be treated as moveable between Blocks for the purpose of defining an optimal set of Blocks for the development of a Modular Software Safety Case.
Certification		The process and declaration of the acceptance of a safety case by a Certification authority.
Change scenario		The circumstances and/or nature of a change, either known, predicted or likely, that may be applied to a system at a future date. The change may introduce a change impact on the safety case.
Claim		In the context of MSSC, an assertion relating directly or indirectly to the safety of a system.
	CM	Configuration Management
Computer Software Component	CSC	A component of software that exists as a separate entity but is not necessarily identifiable as a “configuration item”.
Computer Software Configuration Item	CSCI	An aggregation of software that satisfies an end use function and is designated for separate configuration management by the acquirer
Confidence		The degree of certainty that a party places in the truth of a claim.
Consumer		Any claim that, after integration, is supported outside the SC module in which it is made is a consumer of that external support, as is a SC module containing such claims. The term is also applicable to guarantees which are provided and consumed.
Context		*Used generally:* Information about the development, production and operating environments for a block. Compatibility between required and offered Context is assured during Safety Case Integration. *Used in relation to GSN claim (GSN Context):* Background or reference information relating to a claim. GSN Context includes assumptions and justifications.
Critical Severity		A term used when classifying hazards based on of the seriousness of their impacts. A hazard of Critical Severity could result in major mission degradation, severe injury, occupational illness or major system damage.
Declaration of Design Performance	DDP	The assurance by a manufacturer that products built according to a specified design standard comply with the defined dimensions and performances, based on qualification tests.

Term	Abbrev'n	Explanation / Elaboration
Dependency		Anything (service, operation or behaviour) that is needed by a Block in order for it to uphold its Guarantees.
Dependency - Guarantee Contract	DGC	A linkage formed by the integrator between a Dependency in one Block and a Guarantee offered by another. A DGC is created to support a safety case contract.
Dependency - Guarantee Relationship	DGR	The definition of some guaranteed service, operation or behaviour offered by a Block that is relevant to the safety case, together with any external services, operations or behaviour on which that guarantee depends.
DO 178B	DO178B	Radio Technical Commission for Aeronautics (RTCA) Software process: Software Considerations in Airborne Systems and Equipment Certification.
Error		An omission or incorrect action, or a mistake in requirements, design, or implementation.
Essential (MSSC)		An activity which must be performed to be able to make a valid claim that the MSSC process has been followed.
Evidence (SW)		Any recorded analysis or observation of a system that can contribute to confidence in the truth of a claim relating to it.
Exception		An event that changes the normal flow of control in a program. Exceptions include reset, interrupt or a signal from a memory management unit.
Failure		An occurrence, which affects the operation of a component, part, or element such that it does not function as intended, (this includes both loss of function and malfunction).
Failure Mode		A way in which a system or component may fail.
Failure Mode Effect Analysis	FMEA	A procedure for the analysis of potential failure modes within a system and the determination of their effects upon the system.
Failure Mode Effect Criticality Analysis	FMECA	A procedure for the analysis of potential failure modes within a system, the determination of their effects upon the system and the classification of each failure mode by its probability of occurrence and the severity of its impact.
Fault		An internal defect in an individual hardware or software component such that it may not perform to specification.
Fault Manager	FM	An aspect of System Management that is responsible for locating faults and performing any specified corrective actions.
Fault Tree Analysis	FTA	A top-down analysis which determines the logical relationship between sub-system and component failures and how they combine to cause system failures.
Final Software Safety Case		The software safety case presents arguments supported by evidence that the top level hazards have been mitigated in the software implementation. It becomes final when it has passed independent assessment and is about to be certified.
Formal Qualification Test	FQT	Formal Test of a CSCI such that it may be approved for formal release.

Term	Abbrev'n	Explanation / Elaboration
Formal Unit Testing		Formal testing conducted at "software unit" level (i.e. lower level than the deliverable CSCI).
Functional Configuration Audit	FCA	A review of a configuration item's test and analysis data to validate the item satisfies its specified functionality.
Functional Requirement		A requirement which defines how a system shall operate, or its reaction to a stimulus.
Generic System Management	GSM	The part of the generic middle-ware that is responsible for management of the system such as configuration, health monitoring and fault management.
Globally At Least Equivalent to	GALE	Safety argued by claiming that the new system is at least as safe as the referenced system.
Goal		A diagrammatic encapsulation of a claim in GSN
Goal Structuring Notation	GSN	A graphical argument notation showing claims, context and solutions together with their relationships.
Guarantee		A formally defined outcome (e.g. provision of a service, event, resource, data) that a Block assumes responsibility for providing at its interface to other components.
Hardware Configuration Item	HCI	An aggregation of hardware that satisfies an end use function and is designated for separate CM.
Hardware Configuration Item	HWCI	An aggregation of hardware that satisfies an end use function and is designated for separate CM.
Hazard		Any source of potential damage, harm or adverse effects, such as a high voltage supply or toxic chemical.
Health Monitor	HM	A function within generic system management that provides error/fault detection (e.g. BIT) and fault masking.
	HMI	Human Machine Interface Hazardously Misleading Information
	HW	Hardware
	H/W	Hardware
	IAWG	The Industrial Avionics Working Group
	IFS	Inspectorate of Flight Safety
Incremental Safety Case		See *Safety Case Increment*
Incremental Certification		A certification process for system changes that is based on re-use of the existing system certification, plus a safety assessment of the change.
Infrastructure Layer		The application independent software of a processor that provides a platform on which applications can be supported.
Instantiation		The process by which a generically applicable template is applied specifically to produce a specific *instance*. This typically means that instantiation parameters identified in the template are replaced with specific values.

Term	Abbrev'n	Explanation / Elaboration
Integrated Modular Avionics	IMA	A highly-integrated avionics environment in which multiple avionics systems share computing and I/O resources assembled from common hardware modules. The boundaries between systems are enforced by partitioning mechanisms, such that the platform presents a standardised interface to application software, representing an independent, scalable virtual machine.
Integration Area	IA	A grouping of applications that are managed as a subset of the full platform set
Integration Argument		A form of product argument that focuses on claims relating to the characteristics or behaviour of the software as a whole, when integrated with the supporting hardware. For example an integration claim may take the form: *"The processing resources are sufficient to meet the combined worst-case operational demands of all the software blocks."*
Interim Software Safety Case		A snap shot of the arguments and evidence taken from the design phase of the development lifecycle indicating that the top level hazards have been mitigated in the software design. Typically the SC as submitted for independent assessment.
	I/O	Input/Output
	IPT	Integrated Project Team
	IPR	Intellectual Property Rights
	IRS	Interface Requirements Specification
	ISA	Independent Safety Assessor
	ITE	Independent Technical Evaluator
	IV&V	Independent Verification and Validation
Latency		The time interval between an initiating event and the achievement of some specified consequential result.
Logical Interface		An interface that exists at an abstract level, supported by some underpinning transport mechanism.
Low Coupling		The existence of relatively few different paths of interaction between two modules.
	MIL-STD	US military standards
	MLU	Mid Life Update
	MMI	Man Machine Interface
	MMU	Memory Management Unit
	MOD	Ministry of Defence
Modified Condition/Decision Coverage	MC/DC	The level of coverage of software testing that aims to exercise every path through the code, every decision between branches, every possible value of each term (or condition) within a decision and all the possible transitions between them.
Module (Safety Case)		See *Safety Case Module*.
	MSSC	Modular Software Safety Case

Term	Abbrev'n	Explanation / Elaboration
	N/A	Not Applicable
Non-functional Requirement / Property	NFP	A property that may affect system behaviour or the safety assessment, but is not directly related to the functional requirements (e.g. time / resource limits, independence, maintainability).
	OFP	Operational Flight Programme
Partition		(in relation to software applications) A bounded and policed area of computing resource within which processes may be performed.
Pattern (Argument)		A generic form of argument that can be tailored for use in many different situations.
	PDR	Preliminary Design Review
	PHA	Preliminary Hazard Analysis
Physical Domain		perspective of a system that relates to elements of *implementation* (as opposed to elements of safety argument)
Platform Level	PL	The level in a hierarchy of elements that encompasses the entire platform (e.g. aircraft).
Preliminary Software Safety Case		The preliminary software safety case presents safety arguments derived during the System Requirements phase of the development lifecycle that the required top level hazard mitigations have been captured in the software requirements.
Process Argument		A form of argument that focuses on claims relating to the processes followed, as opposed to a “Product Argument” that focuses on claims relating to the characteristics or behaviour of the resulting product.
Product Argument		A form of argument that focuses on claims relating to the design characteristics or behaviour of a product, as opposed to a “Process Argument” that focuses on claims relating the processes followed in producing it.
Producer		Any claim that, after integration, provides support to argument outside the SC module in which it is made is a *producer* of that support, as is the SC module owning such claims. The term is also applicable to guarantees which are provided and consumed.
Project Safety Engineer	PSE	Project Safety Engineer
Public *(adj.)*		An element is referred to as public if it can be referenced by another element outside the scope in which it is defined.
	QA	Quality Assurance
Random Failure		An unpredictable failure that results from degradation mechanisms in hardware. System failure rates arising from random hardware failures can be statistically quantified (unlike systematic failures).

Term	Abbrev'n	Explanation / Elaboration
Region		A Region refers to the collection of blocks which share the same categorisation in relation to their assurance level and likelihood of change (e.g. high assurance or low assurance, high change or low change).
Risk		The potential for the occurrence of an undesirable event (e.g. an accident). Risks are classified according to the likelihood of occurrence of the event and the severity of the consequences.
Safe		Free from those conditions which present risk of death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.
Safety Argument		An argument that demonstrates how it can be reasonably concluded from the evidence available that a system is acceptably safe. (The safety argument together with the appropriate evidence make up a Safety Case)
Safety Case	SC	A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.
Safety Case Architecture	SCA	The identification of SC modules that make up a safety case, their public interfaces and their interactions
Safety Case Contract Module		A module of safety argument that captures the agreed relationship between safety case modules. It can use GSN to reason about why the claims in the safety case modules support each other
Safety Case Increment		An update to a Final Safety Case in response to a system change that does not require unchanged safety case modules to be revisited.
Safety Case Module		An element of a modular safety case which encapsulates some claims, argument and its supporting evidence that relate to a cohesive subject, such as the behaviour of one or more Blocks of software, or to a wider aspect of the software system.
	SAR	Safety Assessment Report
Safety Critical		A term applied to a condition, event, operation, process or item that is essential to safe system operation or use, e.g., safety critical function, safety critical path, and safety critical component. (Not to be confused with Critical Severity).
Safety Critical Item		An item whose failure can cause hazards of catastrophic or critical severity.
Safety Critical Software		Software, including firmware, used to implement a function or component where a fault or failure could cause an accident of Catastrophic severity
Safety Domain		The perspective on a system that relates to elements of the safety case, as opposed to elements of implementation.
Safety Integrity		The strength of assurance that a safety critical system satisfies its safety requirements under all stated conditions.

Term	Abbrev'n	Explanation / Elaboration
Safety Integrity Level	SIL	A classification of the required level of safety integrity defining the processes that must be applied to the development of safety-related software.
Safety Involved Software		Software where a design fault could, in conjunction with one or more other independent faults or failures, cause an accident of Catastrophic or Critical severity.
Safety Requirement		A requirement that, once met, contributes to the hazard mitigation of the system, and / or the evidence of the safety of the system.
	SDP	Software Development Plan
Service DGR		A guarantee and a set of dependencies described at the interface to a module that relate to a service call at the interface.
	SHARD	Software Hazard Analysis and Resolution in Design
	SW	Software
	S/W	Software
Software Configuration		A single static definition of the allocation of software processes, communications, scheduling and management data for a specific module.
Software Development Environment	SDE	All the components of the environment required for the development of [some specified] software.
	SQA	Software Quality Assurance
Software Requirements Specification	SRS	A document collating all the requirements for a specified software component.
Software Safety Case		A safety case that addresses only aspects relating to the contribution of software to safety
Software Safety Case Architecture		The high level organisation of the safety case into modules of arguments and evidence, the externally visible properties of these modules, and the interdependencies that exist between them
Software Unit		An element of SW within a CSCI
Solved by		Used in the context of GSN; goals are “solved by” the sub goals and evidence which justifies the goal (claim).
	SSR	Software Safety Requirements
	SSW	Software System Wide
	STD	Software Test Description
	STP	Software Test Plan
	STR	Software Test Report
Subsystem		An element of a system that in itself may constitute a system.

Term	Abbrev'n	Explanation / Elaboration
Sufficiently safe		This expression is used to mean that something is safe enough for the particular environment and manner in which it will be used. Where this expression is used in a SC those aspects must be precisely defined. (Used interchangeably with Adequately Safe.)
System		A composite, at any level of complexity, the elements of which are used together to perform a given task or achieve a specific purpose.
Systematic Failure		A failure that is due to faults in the specification, design, construction, operation, or maintenance of the system and its components. Systematic failures cause the system to fail under some particular combinations of inputs and / or under some particular environmental conditions. A system failure that is not caused by random failure is, by definition, a systematic failure. All failures in software are systematic failures.
	TBD	To Be Decided
	TDP	Technology Demonstrator Programme
Template (safety case)		A generic piece of argument and evidence which, through the process of instantiation, produces a number of specific arguments supported by specific evidence.
	T&EP	Test and Evaluation Plan
Time (shared resource)		In this context it is a measure of the amount of processor resource available.
	TRR	Test Readiness Review
	UK	United Kingdom
Unified Modelling Language	UML	General-purpose modelling language that includes a graphical notation used to create an abstract model of a system.
Unit Test		A test whose purpose is to show that a software unit's source code correctly implements the associated Design specification.
	UOR	Urgent Operational Requirement
Virtual Channel	VC	A mechanism to allow data to be passed from one process to one or more other processes.
Virtual Memory		Disparate elements of physical computer memory mapped to a virtual address space for use by a single process such that it appears to the user as a coherent, dedicated block.
Virtual Memory Area	VMA	An area of virtual memory used to support/contain a single IMS process.
	V&V	Verification and Validation