Glossary* & Acronyms

Acceptance Criteria – Criteria that a system, software build, or component must satisfy in order to be accepted by an Acquirer, acceptance authority, or a certification authority.

Acquirer – Stakeholder that acquires or procures a product or service from a supplier. The Acquirer may be one of the following: buyer, customer, owner, or purchaser.

Baseline – Specification or product that has been formally reviewed and agreed upon that thereafter serves as the basis for further development and that can be changed only through formal change management procedures.

Causal Factors – (1) The particular and unique set of circumstances that can contribute to a hazard. (2) The combined hazard sources and initiating mechanisms that may be the direct result of a combination of failures, malfunctions, external events, environmental effects, errors, inadequate design, or poor judgment.

Contributing Safety-Significant Requirements – A subcategory of the defined safety requirements of a system. CSSRs are requirements contained within the specifications that contribute to the safety risk potential of a system by the functionality that they will perform. CSSRs do not mitigate risk.

Control Entity – The specific entity that provides autonomous, semi-autonomous, or responsive situational awareness command or control authority over unmanned system functionality. The entity may be human, software logic, or the logic programmed into firmware or programmable logic devices.

Developer – A private or government enterprise or organizational element engaged to provide services or products within agreed limits specified by the Acquirer.

Failure – The inability of an item to perform its intended function.

Failure Mode – A term used to describe one (of possibly many) mechanisms that could contribute to failure. In context to a hazard, the failure modes are descriptors of the overall mechanisms that could lead to a hazards existence. Individual failure modes consist of causal factors, causal pathways, and pathway initiation events.

Firmware – The combination of a hardware device and computer instructions and/or computer data that resides as read-only software on the hardware device.

Function – A task, action, or activity that must be performed to achieve a desired outcome.

---

* Reference: Joint Services – Software Safety Authorities (JS-SSA)
Software System Safety, Implementation Process and Tasks Supporting MIL-STD-882E
Dated April 1, 2016

Generic Safety-Significant Requirements – A subcategory of the defined safety requirements of a system. GSSRs are a product of documented system development, safety best practices, and lessons learned from legacy programs.

Level-of-Rigor – A specification of the depth and breadth of software analysis, test, and verification activities necessary to provide a sufficient level of confidence that a safety significant software function will perform as required.

Mishap – An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Mishap Probability – The aggregate probability of occurrence of the individual events or hazards that might create a specific mishap.

Mishap Risk – An expression of the impact and probability of a mishap in terms of potential mishap severity and probability of occurrence.

Mishap Severity – An assessment of the consequences of the most reasonable credible mishap that could be caused a specific hazard or combination of hazards.

Mitigating Safety-Significant Requirements – A subcategory of the defined safety requirements of a system. MSSRs are normally identified during in-depth mishap and hazard causal analysis and are derived for the purpose of mitigating or controlling failure pathways to the mishap or hazard.

Qualification Testing – Testing conducted to determine whether a system or component is suitable for operational testing.

Regression Testing – The testing of software to confirm that functions that were previously performed correctly continue to perform correctly after a change has been made.

Requirement – (1) A condition or capability needed by a user to solve a problem or achieve an objective. (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents. (3) A documented representation of a condition or capability as in (1) or (2).

Residual Mishap Risk – The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted in accordance with the system safety design order of precedence.

Safety Critical – A term applied to a condition, event, function, operation, process, or item of whose mishap severity consequence is determined to be either Catastrophic or Critical by definition.

Safety Requirements Analysis – An analysis which identifies, categorizes, prioritizes, and justifies the safety requirements to be implemented on a system to influence the design of that system from a safety perspective.

Safety Related – A term applied to a condition, event, function, operation, process, or item of whose mishap severity consequence is determined to be either

Marginal or Negligible (less than critical) by definition.

Safety Significant - A term applied to a condition, event, function, operation, process, or item that possesses a mishap or hazard severity consequence by definition. That which is defined as safety significant can either be safety-critical or safety-related.

Validation – The determination that the requirements for a product are sufficiently correct and complete.

Verification – The evaluation of an implementation of requirements to determine that they have been met.

ACRONYMS

ALARP	As Low as Reasonably Practical
AMRDEC	U.S. Army Aviation and Missle Research, Development and Enginnering Center
AT	Autonomous
BAR	Broadly Acceptable Region
COTS	Commerical Off-the-Shelf
CPLD	Complex Programmable Logic Devices
CSC	Computer Software Component
CSCI	Computer Software Configuration Item
CSU	Computer Software Unit
DAL	Design Assurance Level
DoD	Department of Defense
DOE	Department of Energy
EAL	Evidence Assurance Level
EBTA	Energy Barrier and Trace Analysis
EFOC	Equipment Operational Flight Certification
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EMR	Electromagnetic Radiation
EOFC	Equipment Operational Flight Certification
ESD	Electrostatic Discharge
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FDAL	Functional Design Assurance Level
FHA	Functional Hazard Analysis
FIT	Failure Immunity Testing
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FMETS	Failure Moreds Effects Testing
FPGA	Field Programmable Gate Array
FQT	Formal Qualification Testing
G&C	Guidance & Control
GAL	Generic Array Logic
GFE	Government Furnished Equipment
GSN	Goal Structuring Notation
HMMP	Hazardous Materials Management Plan
HSE	Health and Safety Executive
HTS	Hazard Tracking System
I/O	Input/Output
IARA	Identify, Assess, Reduce, Accept
IAW	In Accordance With
IDAL	Item Design Assurance Level
INCOSE	International Council of System Engineering
JSSSH	Joint Software System Safety Handbook
JUONS	Joint Urgent Operational Need
LE	Lightning Effects
LOR	Level of Rigor
MBD	Model-Based Development
MBSE	Model-Based System Engineering
MCDC	Modified Condition / Decision Coverage
MDA	Model-Driven Architecture
MISRA	Motor Industry Software Reliability Association
NDI	Non-Developmental Item

NSI	No Safety Impact
O&SHA	Operating and Support Hazard Analysis
OMG	Object Management Group
PHA	Preliminary Hazard Analysis
PLA	Programmable Logic Arrays
PLD	Programmable Logic Devices
PSM	Platform Specific Models
PST	Power Supply Transients
RAN	Release Authorization Notice
RBT	Requirements-Based Testing
REF	Rapid Equipping Force
REQ	Rapid Equipping Force
RFT	Redundant Fault Tolerant
ROM	Read Only Memory
RTOS	Robust Real Time Operating Systems
SAR	Safety Assessment Report
SAT	Semi-Autonomous
SC	Safety Case
SCC	Software Control Category
SCF	Safety-Critical Function
SCSF	Safety-Critical Software Function
SD	Software Development
SDD	Software Design Document
SDP	Software Development Plan
SEAL	Safety Evidence Assurance Level
SED	Software Engineering Directorate
SEMP	System Engineering Management Plan
SF	Safety Function
SHA	System Hazard Analysis
SIL	Software Integrity Levels
SIR	Software Integrity Requirements
SOW	Statement of Work
SPLD	Simple Programmable Logic Devices
SRD	Software Requirements Document
SRSF	Safety-Related Software Function
SSA	Software Safety Analysis
SSF	Safety Significant Function
SSHA	Sub System Hazard Analysis
SSP	Software Safety Plan
SSPP	System Safety Program Plan
SSRA	System Safety Risk Assessment
SSSF	Safety-Significant Software Function
SSWG	System Safety Working Group
STD	Software Test Description
STP	Software Test Plan
STR	Software Test Report
SW	Software
SwCI	Software Criticality Index
SwSS	Software System Safety
UML	Uniform Modeling Language
UR	Unacceptable Region