CS25 Definitions and Abbreviations

NOTE: An effort has been made to maintain consistency between the definitions in ARP4754 and those in this document.

AIRWORTHINESS: The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function.

ANALYSIS: An evaluation based on decomposition into simple elements.

APPROVAL: The act of formal sanction of an implementation by a certification authority.

APPROVED: Accepted by the certification authority as suitable for a particular purpose.

(ICAO) ASSESSMENT: An evaluation based upon engineering judgment.

ASSUMPTIONS: Statements, principles and/or premises offered without proof.

ASSURANCE: The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements. (RTCA DO 178B)

"AT RISK" TIME: The period of time during which an item must fail in order to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition.

AUTHORITY: The organization or person responsible within the State (Country) concerned with the certification of compliance with applicable requirements.

AVAILABILITY: Probability that an item is in a functioning state at a given point in time.

CERTIFICATION: The legal recognition that a product, service, organization, or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval, or other documents as required by national laws and procedures.

CERTIFICATION AUTHORITY: Organization or person responsible for granting approval on behalf of the nation of manufacture.

COMMON CAUSE: Event or failure which bypasses or invalidates redundancy or independence.

COMMON CAUSE ANALYSIS: Generic term encompassing Zonal Analysis, Particular Risks Analysis and Common Mode Analysis.

COMMON MODE FAILURE: An event which affects a number of elements otherwise considered to be independent.

COMPLEXITY: An attribute of systems or items which makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.

COMPLIANCE: Successful performance of all mandatory activities; agreement between the expected or specified result and the actual result.

COMPONENT: Any self-contained part, combination of parts, subassemblies or units, which perform a distinct function necessary to the operation of the system.

CONFORMITY: Agreement of physical realization of the item with the defining document.

CRITICALITY: Indication of the hazard level associated with a function, hardware, software, etc., considering abnormal behavior (of this function, hardware, software, etc.) alone, in combination or in combination with external events.

DEFECT: State of an item consisting of the non-performance of specified requirements by a characteristic of the item. A defect may, but need not, lead to a failure.

DEMONSTRATION: A method of proof of performance by observation.

DERIVED REQUIREMENTS: Additional requirements resulting from design or implementation decisions during the development process. Derived requirements are not directly traceable to higher level requirements; though derived requirements can influence higher level requirements.

DESIGN: The result of the design process.

DESIGN PROCESS: The process of creating a system or an item from a set of requirements.

DEVELOPMENT ASSURANCE: All those planned and systematic actions used to substantiate, to an adequate level of confidence, that development errors have been identified and corrected such that the system satisfies the applicable certification basis.

DEVELOPMENT ERROR: A mistake in requirements determination or design.

ERROR: (1) An occurrence arising as a result of an incorrect action or decision by personnel operating or maintaining a system. (JAA AMJ 25.1309)   (2) A mistake in specification, design, or implementation.

EVENT: An occurrence which has its origin distinct from the aircraft, such as atmospheric conditions (e.g., wind gusts, temperature variations, icing, lightning strikes), runway conditions, cabin and baggage fires. The term is not intended to cover sabotage. (JAA AMJ 25.1309) Note: This definition, as it is stated here, describes an "External Event". There are other uses of "event" that cover other aspects (e.g., FTA events).

EXCHANGED FUNCTION: Interdependencies between functions.

EXPOSURE TIME: The period of time between when an item was last known to be operating properly and when it will be known to be operating properly again.

FAILURE: A loss of function or a malfunction of a system or a part thereof. Note: This differs from the ARP 4754 definition and conforms to the AC/AMJ 25.1309 definition.

FAILURE CONDITION: A condition with an effect on the aircraft and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operation or environmental conditions. A Failure Condition is classified in accordance to the severity of its effects as defined in FAA AC 25.1309-1A or JAA AMJ 25.1309.

FAILURE EFFECT (FE): A description of the operation of a system or an item as the result of a failure; i.e., the consequence(s) a failure mode has on the operation, function or status of a system or an item.

FAILURE MODE (FM): The way in which the failure of an item occurs.

FAILURE RATE: The gradient of the failure distribution function divided by the reliability distribution function at time t. it --.: $F'(t)/(1-F(t))$

If the failure distribution function is exponential, the failure rate is constant and the failure rate can be approximately calculated by dividing the number of failures within a hardware item population, by the total unit operating hours. Note: Failure rate could also be expressed in terms of failures per flight hour or per cycle.

FAULT: An undesired anomaly in an item or system.

FUNCTIONAL HAZARD ASSESSMENT (FHA): A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity. GUIDELINES: Recommended procedures for complying with regulations.

HARDWARE: An object that has physical being. Generally, refers to LRUs, circuit cards, power supplies, etc.

HAZARD: A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof.

IMPLEMENTATION: The act of creating a physical reality from a specification.

INDEPENDENCE: (1) A design concept which ensures that the failure of one item does not cause a failure of another item. (Derived from JAA AMJ 25.1309.) (2) Separation of responsibilities that assures the accomplishment of objective evaluation.

INSPECTION: An examination of an item against a specific standard.

INTEGRATION:

(1) The act of causing elements of an item to function together.

(2) The act of gathering a number of separate functions within a single implementation.

ITEM: One or more hardware and/or software elements treated as a unit.

LATENT FAILURE: A failure which is not detected and/or annunciated when it occurs.

MALFUNCTION: The occurrence of a condition whereby the operation is outside specified limits.

NOVELTY: Applicable to systems using new technology and to systems using a conventional technology not previously used in connection with the particular function in question.

PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA): A systematic evaluation of a proposed system architecture and implementation based on the Functional Hazard Assessment and failure condition classification to determine safety requirements for all items.

PRODUCT: An item generated in response to a defined set of requirements.

REDUNDANCY: Multiple independent means incorporated to accomplish a given function.

RELIABILITY: The probability that an item will perform a required function under specified conditions, without failure, for a specified period of time.

REQUIREMENT: An identifiable element of a specification that can be validated and against which an implementation can be verified.

RISK: The frequency (probability) of occurrence and the associated level of hazard.

SEGREGATION: The maintenance of independence by means of a physical barrier between two hardware components.

SEPARATION: The maintenance of independence by means of physical distance between two hardware components.

SIMILARITY: Applicable to systems similar in characteristics and usage to systems used on previously certified aircraft. In principle, there are no parts of the subject system more at risk (Due to environment or installation) and that operational stresses are no more severe than on the previously certified system.

SOFTWARE: Computer programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system.

SPECIFICATION: A collection of requirements which, when taken together, constitute the criteria which define the functions and attributes of a system, or an item.

SYSTEM: A combination of inter-related items arranged to perform a specific function(s).

SYSTEM SAFETY ASSESSMENT (SSA): A systematic, comprehensive evaluation of the implemented system to show that the relevant safety requirements are met.

SYSTEM SAFETY ASSESSMENT PROCESS: The complete process applied during the design of the system to establish safety objectives and to demonstrate compliance with FAR/JAA 25.1309 and other safety related requirements.

VALIDATION: The determination that the requirements for a product are sufficiently correct and complete.

VERIFICATION: The evaluation of an implementation to determine that applicable requirements are met.

ABBREVIATIONS

AC   Advisory Circular

NC   Aircraft

ACJ   Advisory Circular Joint

AMJ   Advisory Material Joint

ARP   Aerospace Recommended Practice (SAE)

CCA   Common Cause Analysis

CMA   Common Mode Analysis

CMR   Certification Maintenance Requirement (FAA AC 25-19)

DD   Dependence Diagram

FAA   Federal Aviation Administration

FAR   Federal Aviation Regulation

FC   Failure Condition

FC&C   Failure Conditions and Classifications

FE   Failure Effects

FHA   Functional Hazard Assessment

FM   Failure Modes

FMEA   Failure Modes and Effects Analysis

FMES   Failure Modes and Effects Summary

FTA   Fault Tree Analysis

H/W   Hardware

HIRF   High Intensity Radiated Fields

JAA   Joint Aviation Authorities

JAR Joint Aviation Requirements

LRU Line Replaceable Unit

MA Markov Analysis

MRB Maintenance Review Board

MSG-3 Maintenance Steering Group 3

PRA Particular Risks Analysis

PSSA Preliminary System Safety Assessment

RTCA (Previously) Radio Technical Commission for Aeronautics

SAE Society of Automotive Engineers, Inc.

SSA System Safety Assessment

SAN Software

ZSA Zonal Safety Analysis

Next Steps

Sofema Aviation Services (www.sassofia.com) offers training to cover CS 25 System Safety Assessments – please see the following link https://sassofia.com/course/type-certification-system-safety-assessment-5-days/

For additional questions or comments – please email team@sassofia.com