International MRB Policy Board

Issue Paper (IP)

IP Number: CIP IND 2022-01
Initial Date: (DD/MMM/YYYY): TBD
Revision / Date: (DD/MMM/YYYY): TBD
Effective Date: (DD/MMM/YYYY): TBD
Retroactivity (Y/N): N

Title:	Fault-Tolerant System Definition
Submitter:	MPIG

Applies To:	
MSG-3 Vol 1	X
MSG-3 Vol 2	X
IMPS	

Issue:

With the introduction of IP 112, guidance was provided for fault-tolerant systems on Section 2-3-4. Clarification on the proper consideration of functional failure statements of fault-tolerant systems added important guidance to the systems MSG-3 document.
However, the text introduced in the glossary is incorrect as it implies that a fault-tolerant system is a system that '*by design the aircraft may be operated indefinitely with the fault(s) while still satisfying all certification and airworthiness requirements.*'

The use of the phrase '*aircraft may be operated indefinitely with the fault(s) while still satisfying all certification and airworthiness requirements.*' goes beyond the definition of 'Fault-tolerant Systems' and may be incorrectly used in the MSG-3 methodology.

The concept of 'Failure-Tolerant' or 'Fault-Tolerant' system is one that uses redundancy of components or other system function(s) in order to enable the aircraft to continue operation despite of failures or malfunctions. In fault-tolerant systems, the function may or may not be degraded or failed after the failure of one of the redundant elements. One example of a system that achieves fault tolerance is Engine controllers that revert to 'Alternate Control Mode' when a fault is present (See FAA AC 33.28-2).

Fault-tolerance can be achieved by redundant components within the system (1), or redundant functions of other systems (2);
Examples of the scenarios (1) and (2) above are:

1. Redundant temperature sensors of a Hydraulic System Reservoir, where the failure of one sensor would not cause the loss of the temperature sensing function. This is an example of single-fault tolerant system;
2. Redundant means to provide electrical alternating current (AC) power to the aircraft Main AC bus is achieved by two generators (one per engine) from the primary electrical power generation system and one Ram Air Turbine (RAT) from the emergency power generation system. This is an example of multi-fault tolerant system where redundancy can be achieved by a separate system function.

Note that the function definition is important when analysing failure-tolerant systems. In the example (1) above, the failure effect for 'Loss of hydraulic temperature data.' would be 'Loss of redundancy. The redundant sensor would provide the hydraulic system temperature to the aircraft systems.'. Should the analyst be analysing for erroneous signal from the temperature sensor (e.g. drift), assuming the system receiving the data has no other means to vote for the correct signal, the failure effect for 'Incorrect temperature data from hydraulic system' would be 'Erroneous high temperature of hydraulic system is displayed to the operating crew.'. Therefore, the correct abstraction level for determining if a system is redundant or not (fault-tolerant) depends on which function and functional failure is under analysis. A fault-tolerant system may have redundant functions, while other functions within the same system may not be redundant. One can only ascertain if a function within a system is redundant or not by performing the analysis, thus the importance of the MSG-3 level 1 analysis and correct assessment of the failure effects.

<u>Use of the term 'fault-tolerant' in the industry:</u>
An evaluation of some industry documents was performed to check if the definition of fault-tolerance was tied to satisfying certification requirements for the life of the aircraft.

For example, FAA AC 25.954-1 defines fault-tolerant design irrespective of compliance with safety requirement for the life of the aircraft when the fault is present:
FAULT-TOLERANT DESIGN. A design that precludes fuel systems ignition sources even when a fault is present.

Furthermore, FAA AC 33.28-2 introduces the term single-fault tolerant to identify the level of redundancy of the system, nonetheless the definition is not tied to satisfying certification requirements for the life of the engine or aircraft:
Single-Fault Tolerant. Single-fault tolerant refers to the capability of the EEC system design architecture to accommodate the occurrence of any single EEC system fault to prevent an unsafe condition.

The NASA Technical Handbook – Fault Management Handbook – NASA-HDBK-2002 DRAFT-2 provide the following definitions:
Failure Tolerance: The ability to perform a function in the presence of any of a specified number of coincident, independent failure causes of specified types.
Fault Tolerance: a synonym of Failure Tolerance.
Redundancy: duplicate functions or mechanisms.

IP Number: CIP IND 2022-01
Initial Date: (DD/MMM/YYYY): TBD
Revision / Date: (DD/MMM/YYYY): TBD
Effective Date: (DD/MMM/YYYY): TBD
Retroactivity (Y/N): N

Therefore, it was concluded that the definition of fault-tolerance is not tied to satisfying certification requirements for the life of the aircraft.

Problem:
The use of the phrase '*aircraft may be operated indefinitely with the fault(s) while still satisfying all certification and airworthiness requirements.*' in the glossary entry for 'Fault-Tolerant Systems' goes beyond the definition of 'Fault-tolerant Systems' and may be incorrectly used in the MSG-3 methodology.

Recommendation (including Implementation):

Glossary change (blue for additions, red for deletions) [Applies to Vol 1 and 2]:

Fault-Tolerant~~tce System~~	When the design of systems or functions contain ~~A system or function that is designed with~~ redundant elements ~~that can fail without impact on safety or operating capability. Redundant elements of the system may fail (fault), but the system itself has not failed. Individually, and in some combinations, these faults may not be annunciated to the operating crew, but by design the aircraft may be operated indefinitely with the fault(s) while still satisfying all certification and airworthiness requirements.~~ such that a failure of one (single-fault tolerant) or more (multiple-fault tolerant) elements would still allow its function to be provided to the aircraft uninterrupted.

NOTE: The original CIP proposal was submitted by Archer.

IMRBPB Position:	
Date:	
Position:	
Recommendation for Implementation:	

Status of the Issue Paper:		Active
		Incorporated in MSG-3 / IMPS (with details)
		Archived