International Maintenance Review Board Policy Board (IMRBPB)
Issue Paper (IP)

Initial Date: 28/04/2011
IP Number: 112
Revision / Date :

Title: Fault Tolerant System, Definition and Procedure

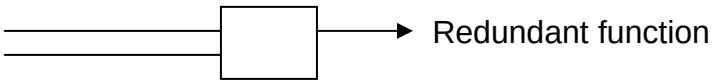
Submitter: Zoran Jovanovic, Bombardier Aerospace

Issue: When discussing analysis of Fault Tolerant Systems it became obvious that the current definition for Fault Tolerant System in the MSG-3 Glossary is incomplete.
Procedure for Fault Tolerant systems has been updated to reflect the current MPIG position.

Problem:

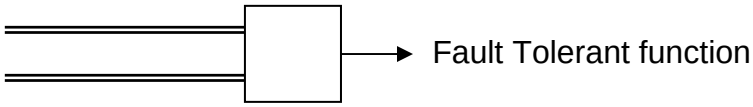
The following describes a difference between Redundant and Fault Tolerant Systems.

A. Redundant System



A redundant system consists of 2 redundant paths – either one provides a full system function. This is a redundant function but not a fault tolerant function. If one path fails, the function is no longer redundant and correction is required before the next flight.

B. Fault Tolerant System



A fault tolerant system consists of 2 redundant paths – either one provides full system function. This time each path has two channels. Each channel is monitored but failure of single channel is sent to a 'Central Maintenance Computer' and is thus hidden. Periodic check will enhance dispatch reliability. Failure to do task will result in decreased DR – extent of reduction depends on probability of channel fault.

Initial Date: 28/04/2011
IP Number: 112
Revision / Date :

Recommendation (including Implementation):

GLOSSARY

Fault Tolerant System

A system 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.

2-3-4 Procedure
Fault Tolerant Systems

~~For the purposes of this MSG-3 analysis, a fault-tolerant system is defined as one that is designed with redundant elements that can fail without impact on safety or operating capability. In other words, 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.~~

~~Consequently, this means that the implementation of fault-tolerant system design by the manufacturer enhances the in-service system availability.~~

~~MSG-3 is only to be applied to each MSI's functional failure and failure cause for the purpose of maintaining the inherent safety and reliability levels of the aircraft, NOT to maintain enhanced in-service system availability. Tasks may be used to enhance in-service availability by identifying the faults of the fault-tolerant system of operational or economic benefit to an operator.~~
~~Such tasks are NOT developed by use of MSG-3, NOR should they be submitted for the subsequent MRB report~~

By definition, the implementation of fault-tolerant system design by the manufacturer may be required to achieve necessary safety and reliability levels of the aircraft and/or to enhance the in-service system availability.

In Fault Tolerant Systems, after a Function has been defined as redundant, a failure of one element is often not a valid Failure Cause, since it has another level of redundancy built in on a sub level. It is up to the WG to decide if it is practical and effective to consider a sub level failure, which is actually a Fault (see a Glossary definition). A Functional Failure in this case is a degradation of redundancy.

Tasks may be selected in cases where the identification of faults within a fault tolerant system is considered effective to support inherent safety and reliability levels. In the case of reliability, the task shall only be selected if it is considered of

Initial Date: 28/04/2011
IP Number: 112
Revision / Date :

operational or economic benefit to the operator in maintaining the required reliability levels.

Tasks with the sole intent to enhance in-service availability i.e. tasks to support dispatch guarantees that go beyond maintaining inherent reliability levels, do not form part of the minimum set of tasks required for an operators initial maintenance program and thus shall not be included in the MRB Report.

IMRBPB Position:

Date: 28/04/2011
Position:
IMRBPB agrees with the proposed changes for the incorporation into MSG-3 on next revision.

Status of Issue Paper (when closed state the closure date): closed 28/04/2011

Recommendation for implementation:

Incorporation into MSG-3 on next revision.

Important Note: The IMRBPB positions are not policy. Positions become policy only when the policy is issued formally by the appropriate National Aviation Authority.