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

Initial Date (19/Nov/2009):
IP Number: 2009-3
Revision 1 / Date (21/Jan/2010):

Title: Fault Tolerant Systems

Submitter: Bombardier

Issue: Statement in Fault Tolerant Systems paragraph prevents deriving tasks from functions defined as redundant

Problem:
Current MSG-3 Document states:
"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."

If the paragraph doesn't clearly say that the statement applies only to fault-tolerant design introduced in excess to certification requirements, then the paragraph effectively tells us that there is no place for redundant functions in MSG-3 analysis. That would have a huge impact on maintenance programs developed by MSG-3 analysis.

Let's examine some MSG-3 examples which show systems with fault-tolerant functions:

Example 1

Function: Provides redundant N1 signal to FADEC.
Functional Failure: Fails to provide redundant N1 signal to FADEC
Failure Effect: None, alternate signal continuously provided by dual channel N1sensor and separate cables. Lost redundancy.
Failure Cause: W1 or W2 cable failure.
Failure Category: 7

Task: General visual inspection of engine W1 and W2 cables is applicable and effective

Example 2

Function: Provide Redundant Means of Holding Thrust Reverser Stowed In-Flight
Functional Failure: Fails to Provide Three Redundant Means of Mechanical Locking to Prevent Deployment in Flight
Failure Effect: Hidden Degraded Redundancy
Failure Cause: Cowl Lock Failed Open
Failure Category: 9
Task: An operational check of the cowl lock can protect against the economic effect of further degradation

Example 3

Function: To provide redundant primary yaw control
Functional Failure: Fails to provide redundant primary yaw control
Failure Effect: Unannunciated loss of redundancy of rudder control system
Failure Cause: Disconnection of dual control path on one side
Failure Category: 9
Task: DI of rudder control cables and DI of rudder mechanical control path for condition and security as well as FC of control cables for tension are applicable and effective

All three examples show functions which are redundant because of certification requirements.
In all of these cases, without having a Function defined as a redundant, there would be no Failure Effect, since the system still operates as intended, and we would not be able to derive tasks.
There are numerous examples like the three above, and they all produce valid tasks.

The Fault Tolerant Systems paragraph, as it stands now, makes all the tasks derived from redundant functions null and void, by stipulating: "Such tasks are NOT developed by use of MSG-3, NOR should they be submitted for the subsequent MRB report."

It is very important to make clear that the above statement applies only to a fault-tolerant design implemented in excess to certification requirements.

Before analyzing the fault-tolerant system, it should be established if the redundancy was driven by certification requirements or in order to enhance the in-service system availability.

1. **The fault-tolerant design driven by certification requirements must be analyzed by MSG-3**
2. **The fault-tolerant design providing redundancy in excess to certification requirements, may not be a part of MSG-3.**

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

Initial Date (19/Nov/2009):
IP Number: 2009-3
Revision 1 / Date (21/Jan/2010):

Recommendation (including Implementation):

Add to the Fault Tolerant Systems paragraph, under 2-3-4 Procedure (add at the end of existing paragraph):

"This applies only to a fault-tolerant design implemented in excess to certification requirements.

Before analyzing the fault-tolerant system, it should be established if the redundancy was driven by certification requirements or in order to enhance the in-service system availability.

1. **The fault-tolerant design driven by certification requirements must be analyzed by MSG-3**
2. **The fault-tolerant design providing redundancy in excess to certification requirements, may not be a part of MSG-3."**

IMRBPB Position:

Date:
Position:

Status of Issue Paper (when closed state the closure date):

Recommendation for implementation:

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