



Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MMM/YYYY):

Revision - Date (DD/MMM/YYYY):

Effective Date (DD/MMM/YYYY):

Retroactivity (Y/N): N

Title:	Clarification of “previously specified limits” in the MSG-3 Failure definition.
Submitter:	EASA

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

Issue:

While MSG-3 clearly states "Failure: The inability of an item to perform **within previously specified limits**", this aspect is not included in the definition of "Function".

In a lot of currently existing analysis these limits (especially that the function may fail below and above those, or that different performance levels are required as protective function) are not assessed.

Problem:

There are two fundamentally different types of functions:

- Those who do either “perform” or “fail to perform” altogether.
Typical examples are lights, that either light up do not light up when powered or switches/relays, that either open/close a circuit when operated or fail to do so.
- Those who are required to “perform within specified limits” and may be considered failed because they perform below or above those limits.
Typical examples are pressure regulators (fuel, hydraulics, pneumatics) that are intended to regulate an output pressure to a certain pressure range and may fail in low-pressure or high-pressure mode.

They will be addressed as “Quantitative” and “Qualitative” Function respectively in this document.

When identifying Functional Failures (FF) for Qualitative Functions, often only one single FF is identified (e.g. "fails to regulate bleed pressure"), leading to an incomplete analysis with respect to addressing the potentially completely different failure effects and completely different Level 1 Analysis / FEC determination for high pressure/low pressure failure.

Additionally different failures above/below limits may be caused by different failure causes. For example, the rupture of a membrane/diaphragm in a mechanical pressure regulator will always cause a failure in high pressure, while a clogged valve may only cause a failure in low pressure. Accordingly, a discard of the membrane (potentially during a restoration) will only be an effective task for the high-pressure failure, not for the low-pressure failure. If the high-pressure failure is only having economic effects (higher consumption rates, FEC9), it may justify to not select this task. If the low-pressure failure is having a safety effect (e.g. FEC8



Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MM/YYYY):

Revision - Date (DD/MM/YYYY):

Effective Date (DD/MM/YYYY):

Retroactivity (Y/N): N

for crew oxygen) analysing only a single FF (e.g. "fails to supply regulated oxygen to the crew") may have required to select this task, because the only FF then would have been FEC8.

As the MSG-3 glossary wording of Functional Failure “previously specified limits” implies, the limits should have been specified before, so when defining the Function, the relevant limits in which it is expected to perform an action should be specified.

So, instead of defining a function like “To power hydraulic System A”, it should be defined as “To power hydraulic System A at 3000 PSP” , or similar.

Certain systems are also required to perform within several limits, so it may as well be defined as “To power hydraulic System A at 3000 PSI pressure up to 40 gph flow”.

There might be different performance limits existing for the same item depending on the exact function:

a battery for example might be installed for

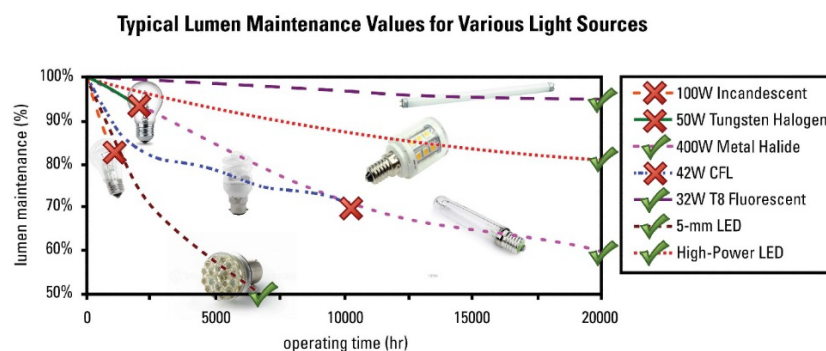
- engine/APU start, and
- as backup power supply with different performance requirements: “To Power DC Bus A with 24V up to 200A for engine start” and “To Power DC Bus A with 24V as backup for 45 minutes”.

An “Illuminating” Example

Several different types of lighting devices were tested for performance and durability, from traditional incandescent lightbulbs to modern high-power LED.

The test finished when either:

- the lights stopped illuminating (qualitative failure, detectable by operational check or evident),
- performed at less than 50% of their initial brightness (quantitative failure, detectable by functional check) or
- reached 20.000 hours of performance (no failure within the service life).



Source: Adapted from Bullough, JD. 2003. *Lighting Answers: LED Lighting Systems*. Troy, NY. National Lighting Product Information Program, Lighting Research Center, Rensselaer Polytechnic Institute.



Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MMM/YYYY):

Revision - Date (DD/MMM/YYYY):

Effective Date (DD/MMM/YYYY):

Retroactivity (Y/N): N

Three types of light failed completely during the test,

- the traditional light bulb at around 1000 hrs when still performing at more than 80% brightness,
- the halogen light bulb at around 2000 hrs when still performing at more than 90% brightness and
- the CFL “energy saver bulb” at around 10.000 hrs when still performing at more than 70% brightness.

Three types of light survived 20.000 hrs of constant operation,

- the fluorescent tube still performing at more than 95% brightness,
- the high-power LED still performing at more than 80% brightness and
- the metal halide bulb still performing at more than 60% brightness.

Only the first-generation LED light (based on the traditional 5mm LED technology of the 70s) was performing at less than 50% initial brightness at around 6500 hrs and further testing stopped, although it still worked. This would be a typical example of a functional failure to perform within specified limits: although the item still works, it is considered failed as it does not perform as required any more.

Type	Aircraft Use Example	Fails Test ?	Hours	Performance
100W Incandescent	Cockpit Lights (traditional)	Yes	1000	>80%
50W Tungsten Halogen	Landing Lights (traditional)	Yes	2000	>90%
400W Metal Halide	none	No	>20.000	>60%
42W CFL	none	Yes	10.000	>70%
32W T8 Fluorescent	Cabin Lighting (traditional)	No	>20.000	>95%
5mm LED	Position lights Cockpit Lights	Yes (underperforms)	6500	<50%
High Power LED	Landing Lights (new)	No	>20.000	>80%

This should help to understand the different type of functional failures that need to be considered during an MSG-3 analysis.



Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MM/YYYY):

Revision - Date (DD/MM/YYYY):

Effective Date (DD/MM/YYYY):

Retroactivity (Y/N): N

Furthermore, the following aspects do require special attention:

Evidence

Typically, a qualitative (complete) failure is recognized easily by the crew performing their normal duty, while a quantitative failure may not, especially if a system is not required to perform at full power every flight (e.g. an air conditioning system in moderate climate, an anti-ice system in summer).

Also, the evidence of performing above or below performance limits may be different, for example a low oil pressure warning may exist, but high pressure needs to be detected by instrument scan. Therefore, it is important to perform separate Level 1 analysis for quantitative and qualitative functional failures and for failing above/below limits.

Redundancy

For the analysis of redundant systems, it is important to consider that there are also two fundamentally different design concepts existing:

1. Redundancy through a backup (“qualitative redundancy”)

Let’s consider a hydraulic system powered by an engine-driven pump with an electric AC pump being available as backup, where in normal operation the engine driven pump does deliver 100% of the total required system flow and the AC pump is not active.

In case the engine driven pump fails, the AC pump is activated and delivers 100% of the required flow.

2. Redundancy through parallel operating items (“quantitative redundancy”)

Let’s consider a hydraulic system powered by two engine-driven pumps (each engine drives one pump), where in normal operation both pumps do deliver around 50% of the total required system flow. In case one pump fails, the other pump changes to 100% flow delivery.

During normal operation, each pump only performs at below 50% of its inherent performance, the hydraulic system will not fail if both pumps are deteriorated to 60% of their initial performance, as they are still able to deliver more hydraulic power than required. As such, this performance reduction of the pumps to 60% will remain hidden, as 2x60%, so more than 100% performance is still available. However, at that point the system has already lost redundancy, in case one pump fails, the remaining one will not be able to provide the nominal performance of the system. Therefore, the system has not failed to deliver hydraulic power, but it has already failed to deliver redundant hydraulic power.

Although this is clearly a quantitative issue of pumps no longer performing within their specified limits, still an OPC may be enough to detect the failure condition (e.g. to power the system by a single pump and check for no "low press" message).



Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MMM/YYYY):

Revision - Date (DD/MMM/YYYY):

Effective Date (DD/MMM/YYYY):

Retroactivity (Y/N): N

To summarize:

- The potentially quantitative nature of a function should not only be considered in the definition of “*functional failure*”, but already in the definition of “*function*”. The current “previously defined” wording of MSG-3 is obviously not widely understood as a requirement to define it when identifying the functions.
- It should be clearly stated that, for quantitative functions, normally at least two functional failures should be identified, i.e. one “performing below” and one “performing above” specified limits. Potentially also the functional failure of “not performing at all” may be existing.
- Also, it should be mentioned that those two different functional failures of “performing below” and “performing above” specified limits may have different failure effects and can be caused by different failure causes.

Recommendation (including Implementation):

As a general initial consideration, it is recommended not to introduce the terms “qualitative” and “quantitative” into MSG-3, as “quantitative” in CS/FAR 25.1309 refers to assessment by mathematical methods, which may confuse MSG-3 users. (*DEFINITIONS. Quantitative: Those analytical processes that apply mathematical methods to assess system and aeroplane safety*).

Therefore, those terms will not be used in the following recommendations.

a) To amend MSG-3 (both Volumes) chapter 2-3 as follows:

2-3-2. Analysis Procedure

After the MSI's have been selected, the following must be identified for each MSI:

- a) Function(s) - the normal characteristic actions of an item
- b) Functional Failure(s) - Failure of an item to perform its intended function within specified limits
- c) Failure Effect(s) - what is the result of a functional failure
- d) Failure Cause(s) - why the functional failure occurs

Defining some functions may require specifying performance limits, for example “to supply hydraulic system A with 3000 psi” or “to retract the landing gear within 8 seconds”.

Defining some functional failures may require a detailed understanding of the system and its design principles. For example, for system components having single element dual load path features, such as concentric tubes or back-to-back plates, the function of



Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MMM/YYYY):

Revision - Date (DD/MMM/YYYY):

Effective Date (DD/MMM/YYYY):

Retroactivity (Y/N): N

both paths should be analyzed individually. The degradation and/or failure of one path may not be evident. It should be considered that some functions may only fail completely while some may degrade and fail to perform within specified limits. A function with specified limits may fail above, below or completely, so different functional failures (and related failure effects and failure causes) may exist for a single function and require individual analysis.

Failure Causes should describe specifically why and how a function fails i.e. which component is causing the failure and by which behaviour (For Example: check valve stuck open, gland seal leaking, filter clogged, membrane ruptured) to aid in maintenance task and interval determination as well as for Failure Cause transfers among MSIs.

When listing functions, functional failures, failure effects, and Failure Causes, care should be taken to identify the functions of all protective devices. These include devices with the following functions:

- a) to draw the attention of the operating crew to abnormal conditions
- b) to shut down equipment in the event of a failure
- c) to eliminate or relieve abnormal conditions which follow a failure
- d) to take over from a function that has failed

Protective function statements should describe the protective function itself, and should also include the words "if" or "in the event of" followed by a brief description of the events, ~~or~~ circumstances or performance limits that would activate or require activation of the protection. For example, "To open the relief valve to atmosphere in the event of system X pressure exceeding 300 psi."

It should be considered that "activation" may mean starting to perform a function as well as performing a function at a different level of performance than during normal operation, for example "to provide 105% contingency power in single engine operation".

1. Evident or Hidden Functional Failure

QUESTION 1:	IS THE OCCURRENCE OF A FUNCTIONAL FAILURE EVIDENT TO THE OPERATING CREW DURING THE PERFORMANCE OF NORMAL DUTIES?
--------------------	---

This question asks if the operating crew will be aware of the ~~loss~~-(failure) of the function during performance of normal operating duties. It should be considered that the total loss of a function may be easier to detect than the failure to perform within specified limits,



Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MMM/YYYY):

Revision - Date (DD/MMM/YYYY):

Effective Date (DD/MMM/YYYY):

Retroactivity (Y/N): N

especially if the full performance of a system is not used every flight or is only used as a protective function in case another function has failed. Question 1 must be asked for each functional failure of the item being analyzed. The intent is to segregate the evident and hidden functional failures. The operating crew consists of qualified flight compartment and cabin attendant personnel who are on duty. Normal duties are those duties associated with the routine operation of the aircraft on a daily basis.

System failures which are indicated to the operating crew when performing their normal duties shall be considered as evident.

b) To amend MSG-3 (both Volumes) Appendix A. “Glossary” as follows:

[...]

Failure The inability of an item to perform within previously specified limits.

[...]

Function The normal characteristic actions of an item. It may require the identification of specific performance limits.



International MRB Policy Board

Issue Paper (IP)

IP Number: CIP EASA 2025-05_R00

Initial Date (DD/MMM/YYYY):

Revision - Date (DD/MMM/YYYY):

Effective Date (DD/MMM/YYYY):

Retroactivity (Y/N): N

IMRBPB Position:	
Date:	
Position:	
Recommendation for Implementation:	

Status of the Issue Paper:	<input type="checkbox"/>	Active
	<input type="checkbox"/>	Incorporated in MSG-3 / IMPS (with details)
	<input type="checkbox"/>	Archived