

# Requirements, hazards and FMEA: designing failures before they happen

## Guiding question

Concrete → interfaces → measurement → calculation → failure → recovery.

## Course map

The real phenomenon → Vocabulary and problem boundary → Course-specific system view → Mathematical relationship and reading the symbols → Worked calculations and interpretation

## 1 — The real phenomenon

Safety begins with explicit functions and hazards. An FMEA — Failure Modes and Effects Analysis — starts from a component or function, asks how it can fail, what effects follow, how the failure is detected and what barriers exist. The goal is not to fill a spreadsheet but to influence design.

The guiding question is: How do we turn a vague concern into verifiable requirements and scenarios? Reasoning starts with the physical or operational function before introducing the mathematical relationship. The goal is not to accumulate terminology, but to know which quantity changes, why it changes and what becomes hazardous when it leaves its domain. For “Requirements, hazards and FMEA: designing failures before they happen”, the first task here is therefore to identify the mechanism specific to this subject before searching for an equation or reference value.

## 2 — Vocabulary and problem boundary

In “Requirements, hazards and FMEA: designing failures before they happen”, distinguish the phenomenon, available measurement, any command, the margin and the success criterion. The calculation boundary states what is included and excluded; without that boundary, a percentage, mass or time may be mathematically correct but wrong as an engineering conclusion. For “Requirements, hazards and FMEA: designing failures before they happen”, the chosen boundary also states what would otherwise be double-counted or omitted from a mission budget.

failure rate, operating hours, margins, cycles, temperature, leaks, repair time and availability  
common cause, slow drift, uncovered fatigue, consumed margin or a repair introducing a new defect  
duration tests, reasoned accelerated cycling, FMEA/FMECA, injected faults and configuration tracking

## Equation - evidence - decision

$$\text{RPN} = \text{S} \times \text{O} \times \text{D}$$

Failure to test: The reference failure is not a vague “broken component.” For “Requirements, hazards and FMEA: designing failures before they happen”, test in particular common cause, slow drift, uncovered fatigue, consumed margin or a repair introducing a new defect. Diagnosis asks which symptoms appear first, which are only consequences and which action preserves the most options.

Requirements, hazards and FMEA: designing failures before they happen

3 — Course-specific system view

This lesson does not reuse one generic picture for every subject. The system view follows cause → measured quantity → decision or physical response → limit for “Requirements, hazards and FMEA: designing failures before they happen”. The English text remains fully equivalent while large translated illustrations are intentionally deferred until their dedicated artwork is supplied. For “Requirements, hazards and FMEA: designing failures before they happen”, the system view must expose inputs, outputs, measured quantity and the consequence of drift without relying on a generic module diagram.

4 — Mathematical relationship and reading the symbols

Read aloud : in a teaching method, a risk-priority number can be the product of severity, occurrence and detectability; the real project method must be defined.

Before substituting numbers, write the unit of every term, state whether the relationship is a physical law, approximation or project indicator, and check dimensional consistency. This is especially important here because “Requirements, hazards and FMEA: designing failures before they happen” combines quantities that do not all have the same evidence status. For “Requirements, hazards and FMEA: designing failures before they happen”, this relationship is chosen because of the phenomenon under study; a different dominant quantity would require a different equation or model.

5 — Worked calculations and interpretation

$8 \times 3 \times 4 = 96$

detectability 4 → 2:  $8 \times 3 \times 2 = 48$

27 modes analyzed out of 30 identified = 90%

- 1. 1. Teaching index  $8 \times 3 \times 4 = 96$  Interpretation: this result is used only after comparison with units, margin and the scenario boundary for “Requirements, hazards and FMEA: designing failures before they happen”.
- 2. 2. Reduction detectability 4 → 2:  $8 \times 3 \times 2 = 48$  Interpretation: this result is used only after comparison with units, margin and the scenario boundary for “Requirements, hazards and FMEA: designing failures before they happen”.
- 3. 3. Coverage 27 modes analyzed out of 30 identified = 90% Interpretation: this result is used only after comparison with units, margin and the scenario boundary for “Requirements, hazards and FMEA: designing failures before they happen”.

Operational table

|                          |                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Phenomena / sections:    | 3 — Course-specific system view ; 4 — Mathematical relationship and reading the symbols ; 5 — Worked calculations and interpretation |
| Relationship to revisit: | $RPN = S \times O \times D$                                                                                                          |
| Expected decision:       | measure → compare with margin → choose nominal, degraded or stop                                                                     |

Check before continuing

Explain without rereading: 3 — Course-specific system view ; 4 — Mathematical relationship and reading the symbols ; 5 — Worked calculations and interpretation. State one measured quantity, one margin and one possible decision.

Requirements, hazards and FMEA: designing failures before they happen

6 — What the formula does not contain

The relationship “ $RPN = S \times O \times D$ ” does not by itself contain all of “Requirements, hazards and FMEA: designing failures before they happen”. It does not automatically tell us whether a sensor is valid, a structure is aging, a resource is accessible, a command arrives in time or a secondary failure removes margin. The example  $8 \times 3 \times 4 = 96$  therefore remains a local calculation rather than a complete architecture.

To make the model useful, explicitly add the quantities that dominate this subject: failure rate, operating hours, margins, cycles, temperature, leaks, repair time and availability. We can then ask which variation truly changes the result, which is negligible and which forces an architectural change. For “Requirements, hazards and FMEA: designing failures before they happen”, this model limitation states exactly what a correct calculation still cannot establish about the real system.

7 — Instrumentation, observability and data quality

For “Requirements, hazards and FMEA: designing failures before they happen”, observability relies on failure rate, operating hours, margins, cycles, temperature, leaks, repair time and availability. Each datum has a unit, acquisition rate, uncertainty, timestamp and validity domain. A value arriving without context can be more dangerous than no measurement because it creates unjustified confidence.

Consistency is checked with at least one independent piece of information when the function is critical. A trend, physical balance or second measurement principle helps distinguish a real system change from a drifting sensor. For “Requirements, hazards and FMEA: designing failures before they happen”, the selected instrumentation must distinguish a real physical change from sensor drift or a bad state estimate.

8 — Phenomenon-specific failures and recovery

The reference failure is not a vague “broken component.” For “Requirements, hazards and FMEA: designing failures before they happen”, test in particular common cause, slow drift, uncovered fatigue, consumed margin or a repair introducing a new defect. Diagnosis asks which symptoms appear first, which are only consequences and which action preserves the most options.

The degraded mode must be defined before failure: minimum function, allowable duration, consumed stock, crew action, abort condition and return-to-nominal criterion. That sequence is topic-specific and cannot be replaced by one universal paragraph about redundancy. For “Requirements, hazards and FMEA: designing failures before they happen”, the degraded mode is defined around the minimum function specific to this subject, with an abort threshold and a return-to-nominal condition.

Operational table

|                          |                                                                                                                                             |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Phenomena / sections:    | 6 — What the formula does not contain ; 7 — Instrumentation, observability and data quality ; 8 — Phenomenon-specific failures and recovery |
| Relationship to revisit: | $RPN = S \times O \times D$                                                                                                                 |
| Expected decision:       | measure → compare with margin → choose nominal, degraded or stop                                                                            |

Check before continuing

Explain without rereading: 6 — What the formula does not contain ; 7 — Instrumentation, observability and data quality ; 8 — Phenomenon-specific failures and recovery. State one measured quantity, one margin and one possible decision.

Requirements, hazards and FMEA: designing failures before they happen

9 — NASA / reference case

NASA material is used as an evidence dossier: requirements, reliability, maintainability, testing and configuration. The lesson never turns a generic failure rate into a universal truth; it shows how evidence is bounded to defined hardware, environment and duration.

The case is used only within what it actually demonstrates. Flight measurement, human-system standard, component test and architecture study are different kinds of evidence; the text therefore states what is observed, calculated, simulated or still prospective. For “Requirements, hazards and FMEA: designing failures before they happen”, the cited NASA case is used as targeted evidence for this phenomenon and is never turned into one universal Mars architecture.

10 — Architecture trade

A good solution for “Requirements, hazards and FMEA: designing failures before they happen” does not maximize one metric. Compare nominal performance, mass, energy, simplicity, maintenance, crew time, common dependencies and recoverability. An option that improves detectability  $4 \rightarrow 2: 8 \times 3 \times 2 = 48$  can still be rejected if it makes failure detection or repair much harder.

The trade is recorded together with its assumptions. If environment data, mass or mission cadence changes, we know which conclusions must be recomputed instead of silently preserving an obsolete choice. For “Requirements, hazards and FMEA: designing failures before they happen”, the trade is evaluated against the interfaces actually touched by this subject rather than a generic list of desirable qualities.

11 — Demonstration, testing and success criteria

The evidence strategy for “Requirements, hazards and FMEA: designing failures before they happen” combines duration tests, reasoned accelerated cycling, FMEA/FMECA, injected faults and configuration tracking. Every test records exact hardware, software, configuration, environment, tolerances and success criterion. A successful demonstration outside the mission domain does not replace qualification inside it.

Evidence grows by levels: analytical relationship, simulation, component, subsystem, integrated system, duration and failure. This hierarchy prevents one spectacular test from being presented as validation of the whole mission. For “Requirements, hazards and FMEA: designing failures before they happen”, demonstration must reproduce the constraints that make this phenomenon difficult; a spectacular test outside the mission domain is insufficient.

Operational table

|                          |                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------|
| Phenomena / sections:    | 9 — NASA / reference case ; 10 — Architecture trade ; 11 — Demonstration, testing and success criteria |
| Relationship to revisit: | $RPN = S \times O \times D$                                                                            |
| Expected decision:       | measure → compare with margin → choose nominal, degraded or stop                                       |

Check before continuing

Explain without rereading: 9 — NASA / reference case ; 10 — Architecture trade ; 11 — Demonstration, testing and success criteria. State one measured quantity, one margin and one possible decision.

Requirements, hazards and FMEA: designing failures before they happen

12 — Decision exercise

Situation: revisit “Requirements, hazards and FMEA: designing failures before they happen” with a 20% increase in the most penalizing quantity from the first worked example while one measurement or backup path is unavailable.

Situation: revisit “Requirements, hazards and FMEA: designing failures before they happen” with a 20% increase in the most penalizing quantity from the first worked example while one measurement or backup path is unavailable. Expected answer: recompute the relationship, identify remaining margin, check whether observability is still adequate, and decide whether degraded operation remains acceptable. Multiplying by 1.2 is not enough if the variation also changes interfaces or limits.

13 — What to retain without over-generalizing

14 — Topic-specific primary sources

These references directly document the phenomenon, technology or human constraint addressed in this lesson. They do not by themselves define an official Mars architecture. For “Requirements, hazards and FMEA: designing failures before they happen”, the bibliography is deliberately targeted to this page so that readers can trace each claim back to the relevant primary document.

Topic-specific primary sources

NASA NTRS — Failure Modes and Effects Analysis (FMEA) - <https://ntrs.nasa.gov/citations/20000070720>

NASA NTRS — Reliability Analysis of Complex NASA Systems with Model-Based Engineering - <https://ntrs.nasa.gov/citations/20200000582>

NASA-STD-8729.1A — Reliability and Maintainability Standard - <https://standards.nasa.gov/standard/NASA/NASA-STD-87291>

Operational table

|                          |                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------|
| Phenomena / sections:    | 12 — Decision exercise ; 13 — What to retain without over-generalizing ; 14 — Topic-specific primary sources |
| Relationship to revisit: | $RPN = S \times O \times D$                                                                                  |
| Expected decision:       | measure → compare with margin → choose nominal, degraded or stop                                             |

Check before continuing

Explain without rereading: 12 — Decision exercise ; 13 — What to retain without over-generalizing ; 14 — Topic-specific primary sources. State one measured quantity, one margin and one possible decision.