FMEA study — a failure mode and effects analysis kept as one document

Menu: System ▸ FMEA Study... and System ▸ FMEA tab

Part 1 — What the function does

What it calculates. A failure mode and effects analysis (FMEA) lists, for each part of a system, how it can fail, what the failure causes and how bad it is. ReliaEn keeps an FMEA as a **study**: one document that holds the scope, the failure rows, their ranking, the corrective actions, the verification tests and the revision history. A study uses one of two templates:

Template	How ReliaEn ranks a row
Process FMEA (the default)	The risk priority number RPN = S × O × D from the severity, occurrence and detection scores (1 to 10); a row needs action when RPN ≥ 100 or S ≥ 9
ABS FMECA	A risk class Low, Medium or High read from the study's risk matrix at (severity, likelihood), and a verdict: does a single failure reach an effect you must prevent without an adequate safeguard?

For the ABS FMECA template ReliaEn calculates, for every row:

Result	How ReliaEn sets it
Risk	The matrix cell at the row's Severity and Likelihood
Verdict	COMPLIANT when the row reaches no effect of interest; COMPLIANT (safeguarded) when it reaches one with an adequate safeguard; NON-COMPLIANT when it reaches one without. A safeguard is adequate when the mitigation is not hidden-prone, or when a hidden-prone mitigation has Adequate detection
Residual risk	The class after an Implemented corrective action

The report adds the counts by class and by verdict, the worst-case failures (the NON-COMPLIANT rows of the highest class), whether the design philosophy is met (no row NON-COMPLIANT), the heat maps before and after actions, a Pareto, a cause-and-effect matrix and the revision log. You type the scores and the descriptions; you cannot type the RPN, the class, the verdict or the residual risk.

From which data. No worksheet: the study is typed on the FMEA tab, imported from an Excel workbook, or brought in from five worksheet columns with Import quick FMEA. It is saved in the project.

When an engineer uses it. When the FMEA is a document to keep - reviewed, issued, revised and linked to corrective actions and work orders.

When not to use it.

Situation	Use instead
A quick ranked list of failure modes from five worksheet columns, with a criticality chart	System ▸ FMEA / Criticality... (chapter 4.7); the same columns can later come into a study with Import quick FMEA
The probability that the system fails	System ▸ RBD Canvas (chapter 4.1) or System ▸ Fault Tree... (chapter 4.8): the verdict is not a probability

Part 2 — The example's input data

Setting. A fire-pump skid has a pump, a motor, a coupling, a starter, a pressure switch, a programmable logic controller (PLC), a motor control centre (MCC), a pump room and a suction pipe; a diesel backup pump stands by. The safety engineer opens an FMECA of the skid with the ABS FMECA template and wants to know which single failures can stop the firefighting without an adequate safeguard.

Input	Value
Title	Fire pump skid FMECA
Template	ABS FMECA
Operational modes	Standby, Running
Effects of interest	Injury, Pollution, Loss of firefighting, Facility damage
Risk matrix	the default 4 × 4: likelihood 1 Unlikely, 2 Seldom, 3 Occasional, 4 Frequent × consequence 1 Incidental, 2 Minor, 3 Serious, 4 Major

The twelve failure rows, typed on the Worksheet page (every row also has a Function, for example deliver flow, and a Global effect, loss of function, none for R4):

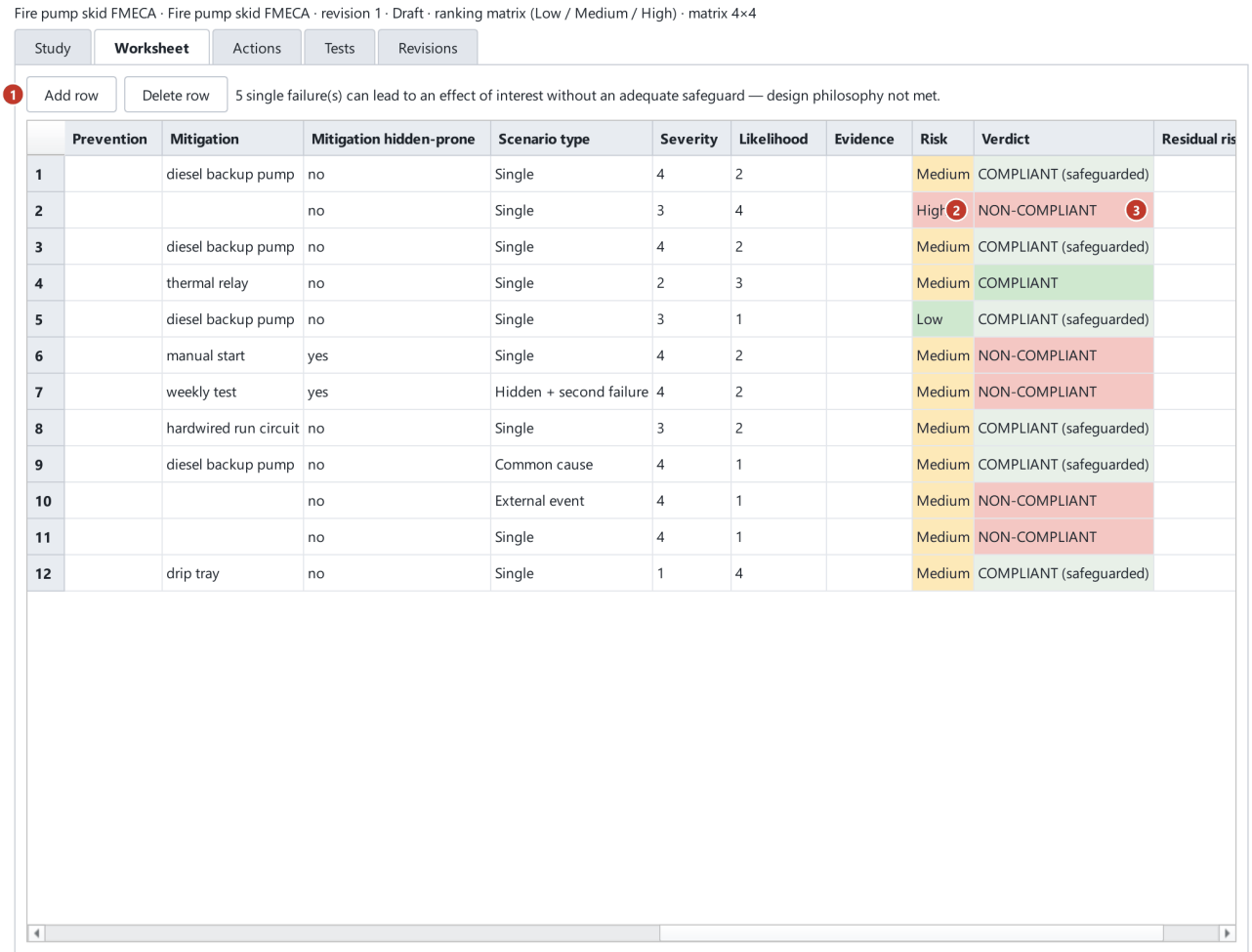
ID	Unit	Failure mode	Effects realised	Mitigation (hidden-prone)	Detection (adequacy)
R1	pump	fails to start	Loss of firefighting	diesel backup pump	pressure alarm (Adequate)
R2	pump	degraded output	Loss of firefighting	—	flow indication (Insufficient)
R3	motor	fails to start	Loss of firefighting	diesel backup pump	starter feedback (Adequate)
R4	motor	trips	—	thermal relay	— (None)
R5	coupling	shears	Loss of firefighting	diesel backup pump	— (None)
R6	starter	fails to close	Loss of firefighting	manual start (yes)	— (None)
R7	pressure switch	stuck	Loss of firefighting	weekly test (yes)	weekly test (Insufficient)
R8	PLC	spurious stop	Loss of firefighting	hardwired run circuit	— (None)
R9	MCC	loss of power	Loss of firefighting	diesel backup pump	— (None)
R10	pump room	fire in pump room	Loss of firefighting; Facility damage; Injury	—	— (None)
R11	suction pipe	rupture	Loss of firefighting; Pollution	—	— (None)
R12	pump	seal leak	Pollution	drip tray	— (None)

ID	Scenario type	Severity	Likelihood
R1	Single	4	2
R2	Single	3	4
R3	Single	4	2
R4	Single	2	3

R5	Single	3	1
R6	Single	4	2
R7	Hidden + second failure	4	2
R8	Single	3	2
R9	Common cause	4	1
R10	External event	4	1
R11	Single	4	1
R12	Single	1	4

No file: the study is typed on the FMEA tab as the steps of Part 3 show.

The twelve rows on the Worksheet page, as steps 11 and 12 of Part 3 type them:

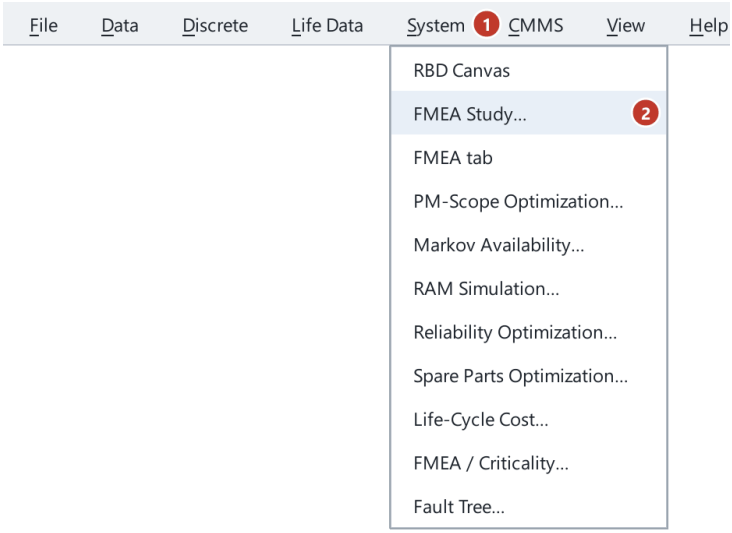


The example's rows on the Worksheet page

- ① Add row: one row per click.
- ② and ③ R2's Risk High and Verdict NON-COMPLIANT, filled by ReliaEn as the row is typed.

Part 3 — How to use it, step by step

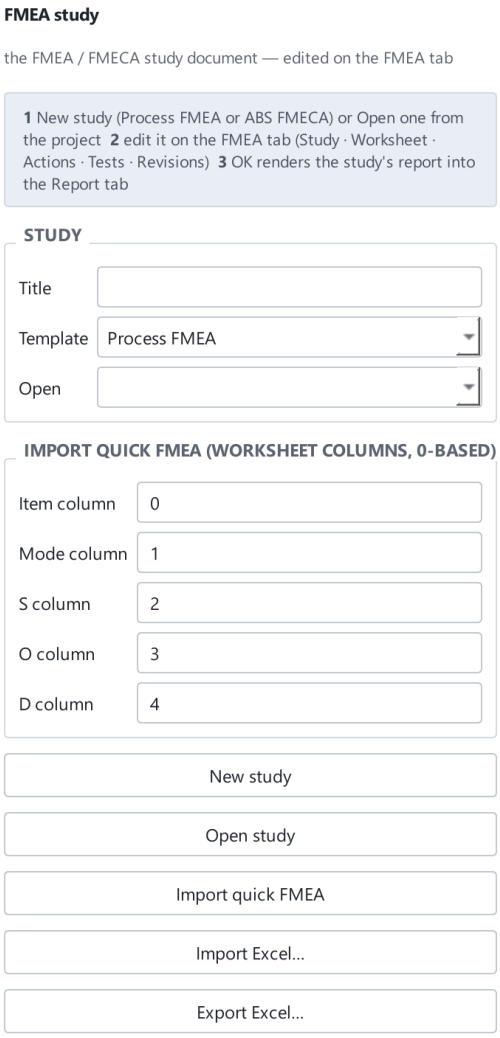
1. **Choose System ▸ FMEA Study…** in the menu bar. The form FMEA study opens in the left panel.



Step 1 — the menu path

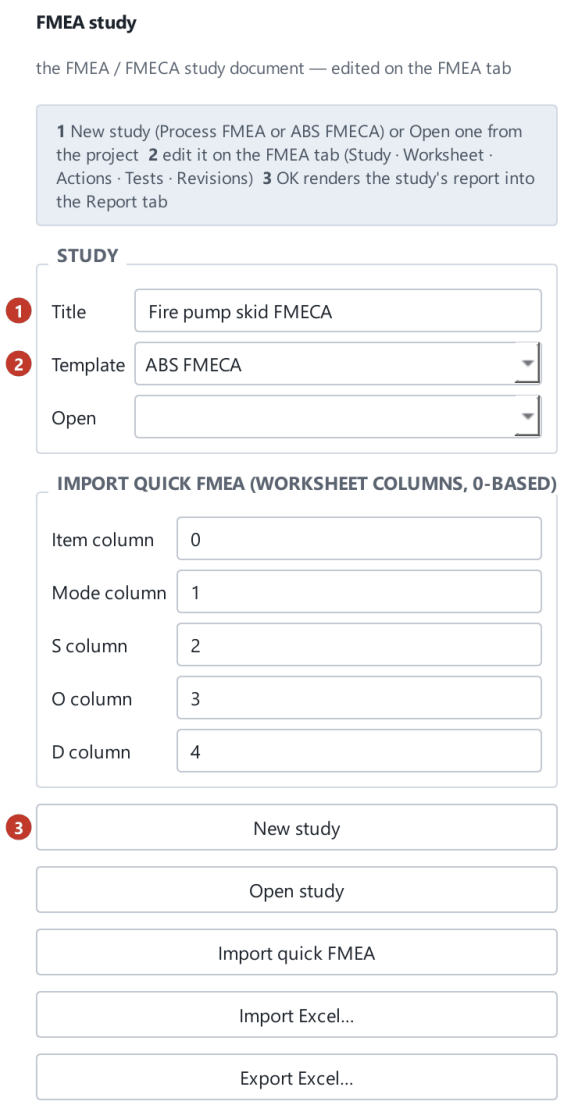
- ① System: the menu.
- ② FMEA Study…: the entry to click.

The form as it opens, before any box is set:



Step 1 — the form as it opens

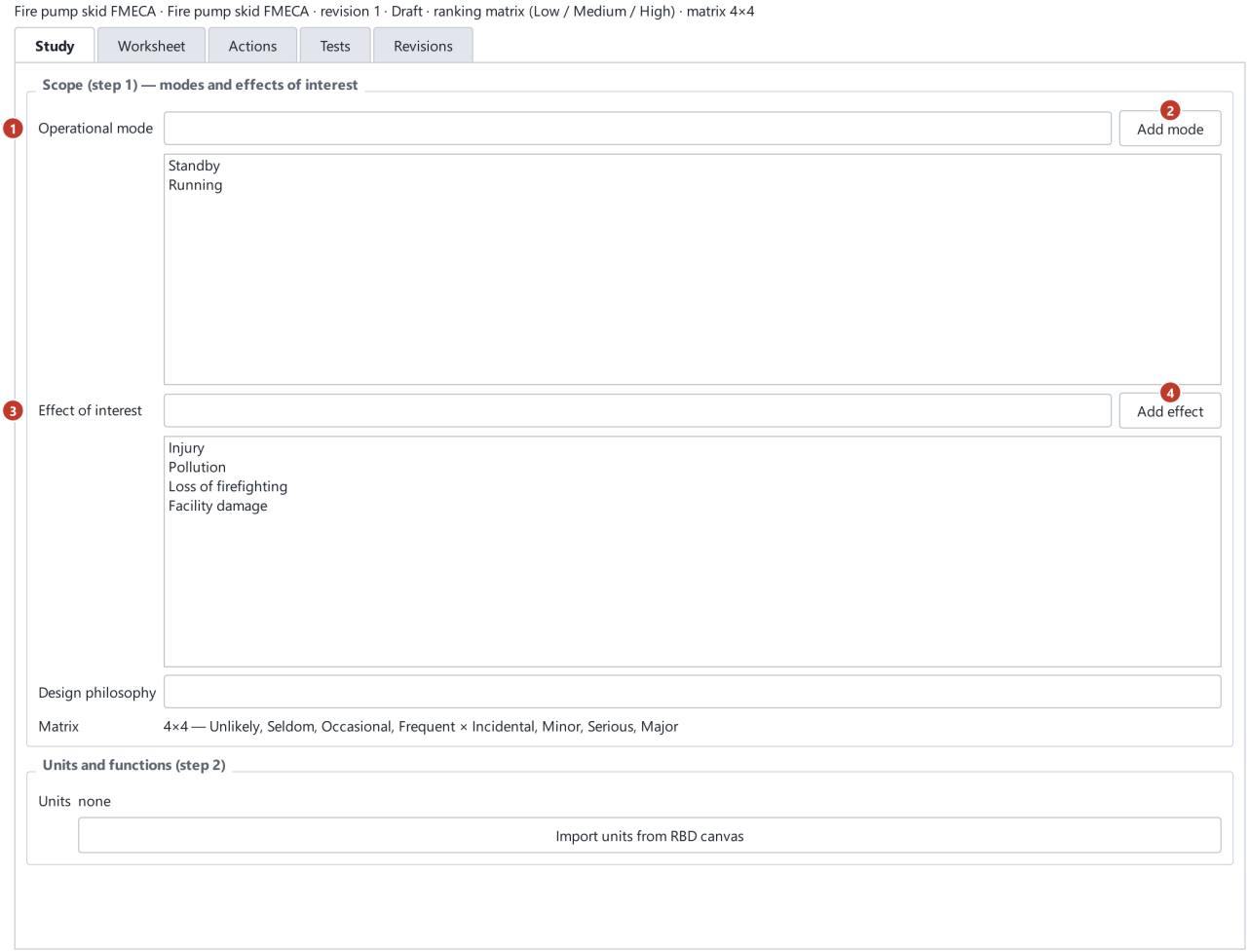
Steps 2 to 4 start the study, marked ① to ③:



Steps 2 to 4 — the form set for the new study

2. ① **In Title, type Fire pump skid FMECA.**
3. ② **In Template, choose ABS FMECA.**
4. ③ **Click New study.** The study opens on the main tab FMEA, on its Study page.

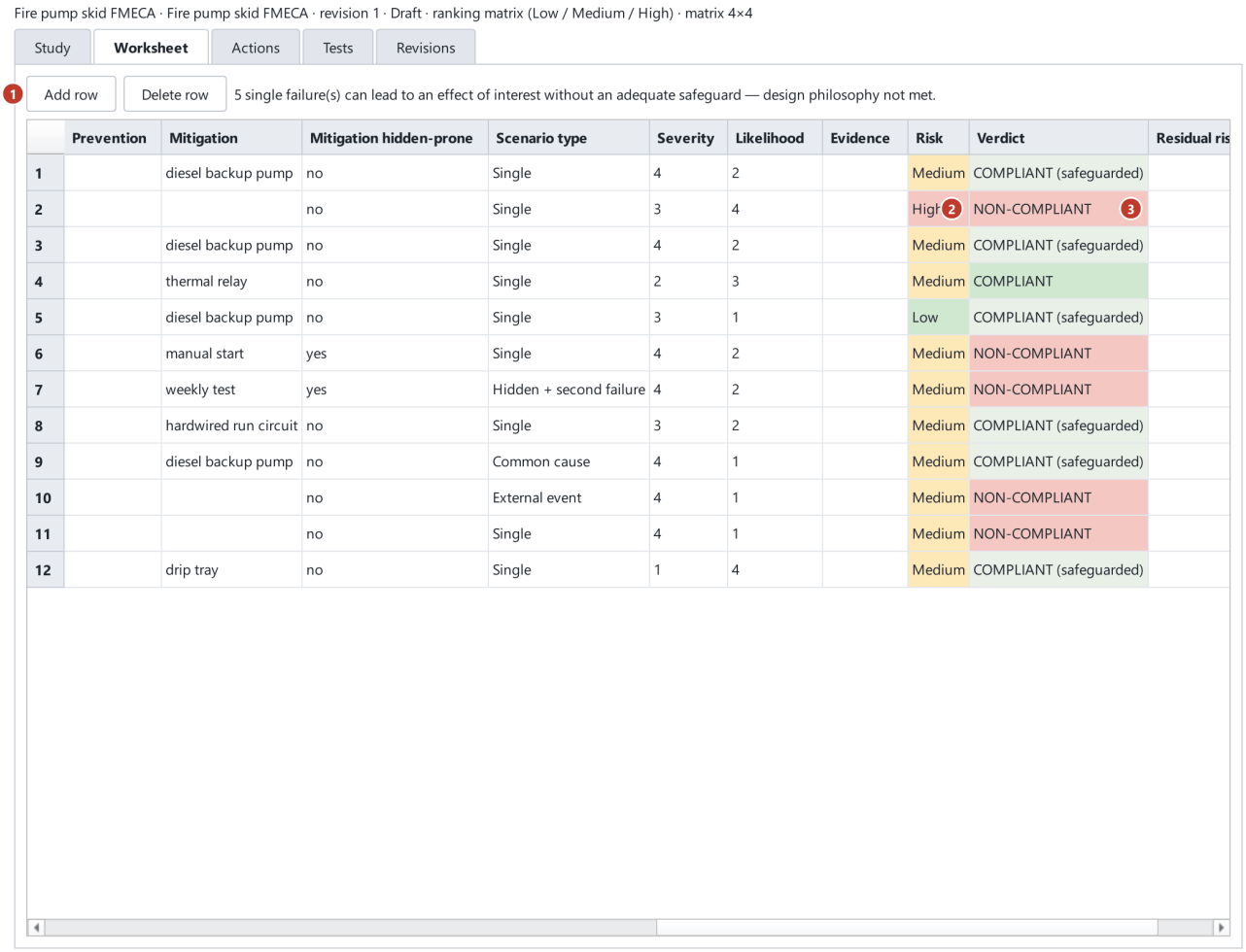
5. **On the Study page of the main tab FMEA, set the scope** - steps 6 to 9 set the boxes the picture below marks.



Steps 6 to 9 — the Study page with the scope set

6. ① **In the operational mode box, type Standby**,
7. ② **and click Add mode.** Repeat both for Running.
8. ③ **In the effect box, type Injury**,
9. ④ **and click Add effect.** Repeat both for Pollution, Loss of firefighting and Facility damage.

10. **Click the page Worksheet** of the FMEA tab - steps 11 and 12 type the failure rows on it.



	Prevention	Mitigation	Mitigation hidden-prone	Scenario type	Severity	Likelihood	Evidence	Risk	Verdict	Residual ris
1		diesel backup pump	no	Single	4	2		Medium	COMPLIANT (safeguarded)	
2			no	Single	3	4		High 2	NON-COMPLIANT 3	
3		diesel backup pump	no	Single	4	2		Medium	COMPLIANT (safeguarded)	
4		thermal relay	no	Single	2	3		Medium	COMPLIANT	
5		diesel backup pump	no	Single	3	1		Low	COMPLIANT (safeguarded)	
6		manual start	yes	Single	4	2		Medium	NON-COMPLIANT	
7		weekly test	yes	Hidden + second failure	4	2		Medium	NON-COMPLIANT	
8		hardwired run circuit	no	Single	3	2		Medium	COMPLIANT (safeguarded)	
9		diesel backup pump	no	Common cause	4	1		Medium	COMPLIANT (safeguarded)	
10			no	External event	4	1		Medium	NON-COMPLIANT	
11			no	Single	4	1		Medium	NON-COMPLIANT	
12		drip tray	no	Single	1	4		Medium	COMPLIANT (safeguarded)	

Steps 11 and 12 — the Worksheet page with the twelve rows

11. ① **Click Add row and type one row of Part 2's table** - ID, Unit, Function, Failure mode, Global effect, Effects realised, Mitigation and whether it is hidden-prone, Detection and its adequacy, Scenario type, Severity, Likelihood. Repeat for the twelve rows. ReliaEn fills Risk, Verdict and Residual risk as each row is typed.
12. **Check R2's row:** ② Risk High and ③ Verdict NON-COMPLIANT.

ReliaEn keeps the study as it is typed: Risk and Verdict stand on the Worksheet for every row. The report of Part 4 is rendered by the form's OK — Calculate button, which the FMEA study form of 1.0.0 does not show: in 1.0.0 the report cannot be opened from the form; the update that adds the button opens it as Part 4 shows.

Part 4 — The report, card by card

	INPUT DATA	
1	Study	Fire pump skid FMECA
2	Template	ABS FMECA
3	Revision / status	1 / Draft
4	Rows	12

Input data

- ① Study Fire pump skid FMECA.
- ② Template ABS FMECA.
- ③ Revision / status 1 / Draft.
- ④ Rows 12.

	RESULTS	
1	Rows by risk class	High 1 · Medium 10 · Low 1
2	Rows by verdict	COMPLIANT 1 · COMPLIANT (safeguarded) 6 · NON-COMPLIANT 5
3	Worst-case failure(s)	R2
4	Design philosophy	not met — 5 rows
5	Actions	actions: none
6	Issue	1 High-risk row(s) have no corrective action — the study can be saved, not Issued.

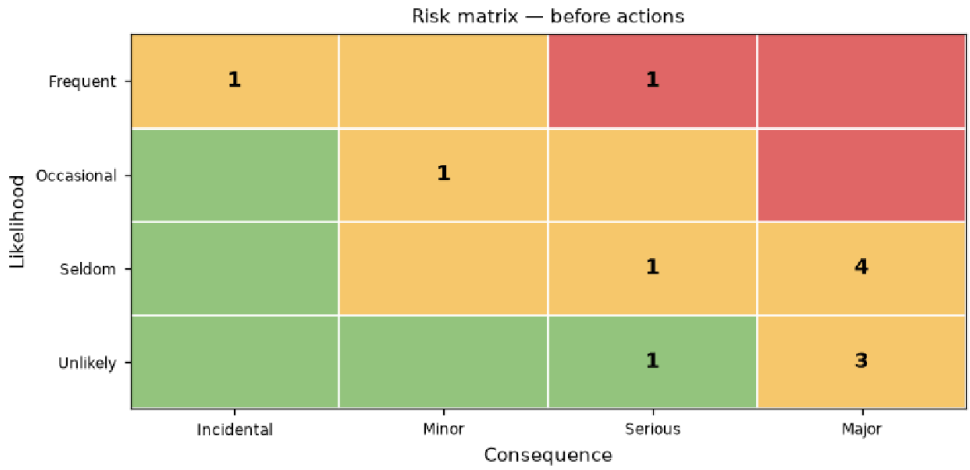
Results

- ① Rows by risk class High 1 · Medium 10 · Low 1. One row in the matrix's high band.
- ② Rows by verdict COMPLIANT 1 · COMPLIANT (safeguarded) 6 · NON-COMPLIANT 5. Five rows can reach an effect of interest without an adequate safeguard.
- ③ Worst-case failure(s) R2. The degraded pump output.
- ④ Design philosophy not met — 5 rows.
- ⑤ Actions actions: none.
- ⑥ Issue 1 High-risk row(s) have no corrective action — the study can be saved, not Issued..

	INTERPRETATION
1	5 single failure(s) can lead to an effect of interest without an adequate safeguard — design philosophy not met. Nothing in the verdict is a probability: it is Boolean algebra on what the analyst recorded.

Interpretation

- ① 5 single failure(s) can lead to an effect of interest without an adequate safeguard — design philosophy not met. Nothing in the verdict is a probability: it is Boolean algebra on what the analyst recorded.



Interactive Plot

Plot

- The heat map of the rows before actions, by consequence and likelihood.

EXECUTIVE SUMMARY

	Item	Value
1	Rows by risk class	High 1 · Medium 10 · Low 1
2	Rows by verdict	COMPLIANT 1 · COMPLIANT (safeguarded) 6 · NON-COMPLIANT 5
3	Worst-case failure(s)	R2
4	Design philosophy	not met — 5 rows
5	Actions	actions: none
6	Issue	1 High-risk row(s) have no corrective action — the study can be saved, not Issued.

Executive summary

- ① Rows by risk class · High 1 · Medium 10 · Low 1
- ② Rows by verdict · COMPLIANT 1 · COMPLIANT (safeguarded) 6 · NON-COMPLIANT 5
- ③ Worst-case failure(s) · R2
- ④ Design philosophy · not met — 5 rows
- ⑤ Actions · actions: none
- ⑥ Issue · 1 High-risk row(s) have no corrective action — the study can be saved, not Issued.

INTRODUCTION AND BACKGROUND

1 Card	2 Content
Purpose	—
Standards	ABS GN 2015; IEC 60812; MIL-STD-1629A
Scope and intent	—
Revision / date	1 / —
Design changes since last revision	none (first revision)
Participants and reviewers	—
Key design concepts	—
Operational modes	Standby, Running
Effects of interest	Injury, Pollution, Loss of firefighting, Facility damage
Failure criteria	single failure (the handbook's default)
Approach	4×4 matrix — likelihood 1 Unlikely, 2 Seldom, 3 Occasional, 4 Frequent; consequence 1 Incidental, 2 Minor, 3 Serious, 4 Major
Design philosophy	no single failure leads to an effect of interest

Introduction and background

- ① Card
- ② Content

PHYSICAL BOUNDARIES (THE UNIT HIERARCHY)

1 Unit	2 Kind
Fire pump skid FMECA	system
pump	component
motor	component
coupling	component
starter	component
pressure switch	component
PLC	component
MCC	component
pump room	component
suction pipe	component

Physical boundaries (the unit hierarchy)

- ① Unit
- ② Kind

DESCRIPTION OF SYSTEMS — WORKSHEET (HANDBOOK TABLE 2 ORDER)

① ID	② Mode	③ Unit	④ Function	⑤ Failure mode	⑥ Causes	⑦ Detection	⑧ Local effect	⑨ Global effect	⑩ Effects realised	⑪ Prevention	⑫ Mitigation	⑬ Scenario	⑭ Sev	⑮ Lik	⑯ Risk	⑰ Verdict	⑱ Residual
R1	Standby	pump	deliver flow	fails to start	–	pressure alarm (Adequate)	–	loss of function	Loss of firefighting	–	diesel backup pump	Single	4	2	Medium	COMPLIANT (safeguarded)	–
R2	Running	pump	deliver flow	degraded output	–	flow indication (Insufficient)	–	loss of function	Loss of firefighting	–	–	Single	3	4	High	NON-COMPLIANT	–
R3	Standby	motor	drive pump	fails to start	–	starter feedback (Adequate)	–	loss of function	Loss of firefighting	–	diesel backup pump	Single	4	2	Medium	COMPLIANT (safeguarded)	–
R4	Running	motor	drive pump	trips	–	– (None)	–	none	–	–	thermal relay	Single	2	3	Medium	COMPLIANT	–
R5	Running	coupling	transmit torque	shears	–	– (None)	–	loss of function	Loss of firefighting	–	diesel backup pump	Single	3	1	Low	COMPLIANT (safeguarded)	–
R6	Standby	starter	close on demand	fails to close	–	– (None)	–	loss of function	Loss of firefighting	–	manual start (hidden-prone)	Single	4	2	Medium	NON-COMPLIANT	–
R7	Standby	pressure switch	sense pressure	stuck	–	weekly test (Insufficient)	–	loss of function	Loss of firefighting	–	weekly test (hidden-prone)	Hidden + second failure	4	2	Medium	NON-COMPLIANT	–
R8	Running	PLC	run logic	spurious stop	–	– (None)	–	loss of function	Loss of firefighting	–	hardwired run circuit	Single	3	2	Medium	COMPLIANT (safeguarded)	–
R9	Standby	MCC	supply power	loss of power	–	– (None)	–	loss of function	Loss of firefighting	–	diesel backup pump	Common cause	4	1	Medium	COMPLIANT (safeguarded)	–
R10	Standby	pump room	house the skid	fire in pump room	–	– (None)	–	loss of function	Injury; Loss of firefighting; Facility damage	–	–	External event	4	1	Medium	NON-COMPLIANT	–
R11	Standby	suction pipe	supply water	rupture	–	– (None)	–	loss of function	Pollution; Loss of firefighting	–	–	Single	4	1	Medium	NON-COMPLIANT	–
R12	Running	pump	deliver flow	seal leak	–	– (None)	–	loss of function	Pollution	–	drip tray	Single	1	4	Medium	COMPLIANT (safeguarded)	–

Description of systems — worksheet (handbook Table 2 order)

- ① ID
- ② Mode
- ③ Unit
- ④ Function
- ⑤ Failure mode
- ⑥ Causes
- ⑦ Detection
- ⑧ Local effect
- ⑨ Global effect
- ⑩ Effects realised
- ⑪ Prevention
- ⑫ Mitigation
- ⑬ Scenario
- ⑭ Sev
- ⑮ Lik
- ⑯ Risk
- ⑰ Verdict
- ⑱ Residual

RISK MATRIX HEAT MAP (BEFORE ACTIONS)

1 every cell echoed: (consequence, likelihood): rows

2 Likelihood ↓ / Consequence →	3 1 Incidental	4 2 Minor	5 3 Serious	6 4 Major
7 4 Frequent	(1,4): 1	(2,4): 0	(3,4): 1	(4,4): 0
8 3 Occasional	(1,3): 0	(2,3): 1	(3,3): 0	(4,3): 0
9 2 Seldom	(1,2): 0	(2,2): 0	(3,2): 1	(4,2): 4
10 1 Unlikely	(1,1): 0	(2,1): 0	(3,1): 1	(4,1): 3

Risk matrix heat map (before actions)

- ① every cell echoed: (consequence, likelihood): rows
- ② Likelihood ↓ / Consequence →
- ③ 1 Incidental
- ④ 2 Minor
- ⑤ 3 Serious
- ⑥ 4 Major
- ⑦ 4 Frequent · (1,4): 1 · (2,4): 0 · (3,4): 1 · (4,4): 0
- ⑧ 3 Occasional · (1,3): 0 · (2,3): 1 · (3,3): 0 · (4,3): 0
- ⑨ 2 Seldom · (1,2): 0 · (2,2): 0 · (3,2): 1 · (4,2): 4
- ⑩ 1 Unlikely · (1,1): 0 · (2,1): 0 · (3,1): 1 · (4,1): 3

PARETO BY RISK CLASS, THEN BY MATRIX CELL

Class	Rows
1 High	1
2 Medium	10
3 Low	1

4 Cell (C,L)	5 Rows
(4,2)	4
(4,1)	3
(3,4)	1
(2,3)	1
(3,1)	1
(3,2)	1
(1,4)	1

Pareto by risk class, then by matrix cell

- ① High · 1
- ② Medium · 10
- ③ Low · 1
- ④ Cell (C,L)
- ⑤ Rows

CAUSE-AND-EFFECT MATRIX

1 ● realised without an adequate safeguard · ◐ realised and safeguarded · — not realised

2 Effect of interest	3 R1	4 R2	5 R3	6 R4	7 R5	8 R6	9 R7	10 R8	11 R9	12 R10	13 R11	14 R12
15 Injury	–	–	–	–	–	–	–	–	–	●	–	–
16 Pollution	–	–	–	–	–	–	–	–	–	–	●	◐
17 Loss of firefighting	◐	●	◐	–	◐	●	●	◐	◐	●	●	–
18 Facility damage	–	–	–	–	–	–	–	–	–	●	–	–

Cause-and-effect matrix

- ① ● realised without an adequate safeguard · ◐ realised and safeguarded · — not realised
- ② Effect of interest
- ③ R1
- ④ R2
- ⑤ R3
- ⑥ R4
- ⑦ R5
- ⑧ R6
- ⑨ R7
- ⑩ R8
- ⑪ R9
- ⑫ R10
- ⑬ R11
- ⑭ R12
- ⑮ Injury · — · — · — · — · — · — · — · — · — · ● · — · —
- ⑯ Pollution · — · — · — · — · — · — · — · — · — · — · ● · ◐
- ⑰ Loss of firefighting · ◐ · ● · ◐ · — · ◐ · ● · ● · ◐ · ◐ · ● · ● · —
- ⑱ Facility damage · — · — · — · — · — · — · — · — · — · — · ● · — · —

CONCLUSIONS AND CORRECTIVE ACTIONS

1 ID	2 Action	3 Category	4 Type	5 Rows	6 Status	7 Work order	8 Residual
9 –	–	–	–	–	–	–	–

Conclusions and corrective actions

- ① ID: No action yet.
- ② Action
- ③ Category
- ④ Type
- ⑤ Rows
- ⑥ Status
- ⑦ Work order
- ⑧ Residual
- ⑨ — · — · — · — · — · — · — · —

VERIFICATION PLAN

1 none generated

Verification plan

- ① none generated

REFERENCES

1 ABS Guidance Notes on FMEA for Classification (2015); IEC 60812; MIL-STD-1629A

References

- ① ABS Guidance Notes on FMEA for Classification (2015); IEC 60812; MIL-STD-1629A

REVISION LOG

1 no entries — revision 1 (the first)

Revision log

- ① no entries — revision 1 (the first)

Part 5 — How to interpret the results

What the skid's study says. Five of the twelve single failures can stop the firefighting without an adequate safeguard: R2 (degraded output), R6 (starter fails to close), R7 (pressure switch stuck), R10 (fire in the pump room) and R11 (suction pipe rupture). The design philosophy is therefore not met. Six rows reach an effect of interest but are safeguarded - R1, R3, R5, R8 and R9 by a safeguard that cannot fail unseen, R12 by its drip tray - and R4 reaches none.

Read the verdict before the class. Only R2 is High; R5 is Low; the other ten are Medium. Yet five rows are NON-COMPLIANT. The class says how likely and how bad a row is; the verdict says whether one failure reaches an effect you must prevent. A Medium row such as R6 can fail the design philosophy.

A safeguard that can fail unseen needs a test. R6 (manual start) and R7 (weekly test) rest on hidden-prone safeguards with no adequate detection: the backup itself can be failed when it is needed. Generate their verification sheets on the Tests page.

What comes first. R2, the worst-case failure: as long as a High row has no corrective action, the study can be saved but not issued. Then the cell (4,2) of the heat map, which holds the most rows (R1, R3, R6, R7) - two of them, R6 and R7, are NON-COMPLIANT. R10 alone reaches three effects of interest: Injury, Loss of firefighting and Facility damage.

What changes the result. Only an Implemented corrective action changes a row's risk; an Open action leaves the row as it was. After Issue this revision the study is locked, and any change needs New revision with a reason.

What the verdict is not. It is not a probability: it is Boolean algebra on what the analyst recorded. For the chance that the skid fails, model it on the RBD canvas or as a fault tree.