



WORKED EXAMPLE / 1 OF 2

Subsystem category justification record

One worked example. One reusable record. Trace each design decision to evidence.

01 Define the task and the boundary

SF-01: stop hazardous conveyor movement before access through the guard and prevent restart during access.

OUT-01: disconnect the drive supply on a switch-off command. Scope: K1, K2, their coil control, interconnections and feedback monitoring.

OUT-01 / CATEGORY 3 EXAMPLE

Guard opens: switch-off command



02 Read the model result

CATEGORY	MTTF D / CHANNEL	DC AVG	PFH / HOUR	PL
3	30 years	90%	2.65×10^{-7}	d

MODEL ASSUMPTIONS - EVIDENCE TO BE COMPLETED

ISO 13849-1:2023, Table K.1: Category 3, medium diagnostic coverage, $MTTF_D = 30$ years for each channel. PL d is the output subsystem model result. The complete safety function includes the guard input and logic.

Pages 1-2: worked example. Pages 3-5: fillable project record.
Use document IDs and revisions to connect the record to your technical documentation.



Follow the fault to the evidence

All example test outcomes remain open until the design has been checked and tested.

03 Fault cases for OUT-01

Fault	Required behaviour	Evidence to obtain
F-01 K1 main contacts fail to open.	K2 interrupts the drive supply. K1 feedback does not confirm opening. The control system detects the fault and inhibits re-energisation.	T-01 Disconnection by K2; response time; detection; restart inhibition.
F-02 K2 main contacts fail to open.	K1 interrupts the drive supply. K2 feedback does not confirm opening. The control system detects the fault and inhibits re-energisation.	T-02 The same checks for the other channel.
F-03 K1 feedback is bridged and stays at "contactor open".	On energisation, feedback fails to change within the specified time. The control system switches off the outputs and inhibits re-energisation.	T-03 The short circuit, expected signal transitions, detection time and reaction.

04 Build the evidence set

Design: drawing and software revisions; full-load switching capability; mirror-contact data; response-time limits.

Reliability: component data, switching cycles, $MTTF_D$, diagnostic coverage and CCF assessment.

Verification: analysis, test configuration, measured results, reviewer and open actions.

CCF: assess shared wiring, supply, temperature, electromagnetic disturbances and short-circuit exposure. The Annex F scoring method requires at least 65 points, supported by implemented measures.

Basis: ISO 13849-1:2023, 6.1.3.2.5, 6.1.5-6.1.10, 6.2.2, Clause 10, Clause 12, Annex F and Table K.1. Mirror contacts: IEC 60947-4-1:2018, Annex F. Check applicable type-C standards.



YOUR PROJECT / 1 OF 3

Define your subsystem

Fill in the fields, then save a project copy of this PDF. Keep evidence references specific.

Project

Record ID / revision / date

Machine / asset ID

Safety function ID / SRS reference

Subsystem task and required behaviour

Subsystem boundary, components and interconnections

Drawing revision / software revision

Safety function PLr / target subsystem category

01

Parameters and source references

MTTFD of each channel / data source / switching cycles

DCavg / diagnostic measures / justification reference

CCF measures / score / evidence reference

Use the same record ID on pages 4 and 5. Link calculations and analyses by document ID and revision.



YOUR PROJECT / 2 OF 3

Record faults and reactions

Describe what fails, what still performs the task, and how the control system reacts.

Record ID / revision

F01

Fault assessment

Fault, affected part and effect on the subsystem task

Retained capability / response to the fault

Detection method / time / restart behaviour

Evidence ID / revision / result / open action

F02

Fault assessment

Fault, affected part and effect on the subsystem task

Retained capability / response to the fault

Detection method / time / restart behaviour

Evidence ID / revision / result / open action

Extend the analysis to the faults relevant to the selected category. For Category 4, address the accumulation of undetected faults. Record any fault exclusions with their justification.



YOUR PROJECT / 3 OF 3

Review the evidence and outcome

Identify the assessed configuration and record the limits of the decision.

Record ID / revision

Prepared by / date

Evidence index: drawings, calculations, analyses and test reports / revisions / results

Subsystem PFH / achieved PL / calculation reference

Required response time / verified response time / stopping and access conditions

Mission time / T10D / inspection, replacement and maintenance requirements

Environment, systematic failure measures, assumptions and integration conditions

Decision, assessed category, outstanding actions and scope of acceptance

Reviewed by / date

Approval / review record reference

Keep this record with the technical documentation. Combine subsystem results and verify the complete safety function against its PLr.
Reassess the record when the task, components, software or conditions change.