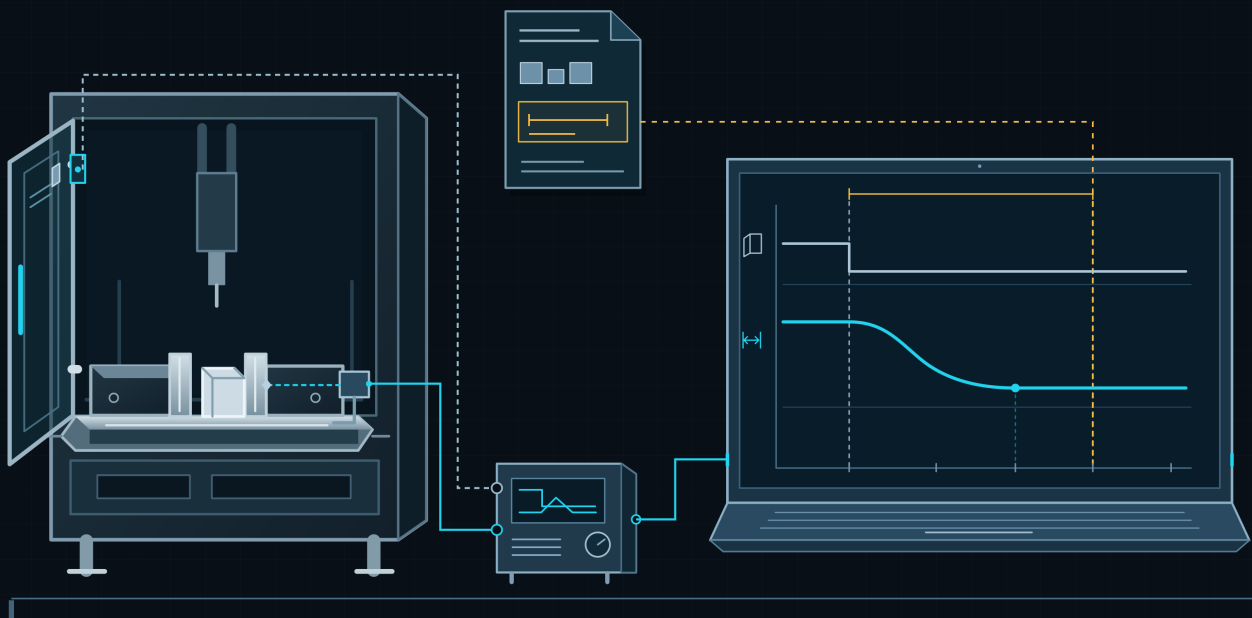




Safety Requirements Specification

From the operator task to a requirement you can design and test.



WORKED CASE + REUSABLE WORKSHEETS

A fictional clamping-access example, acceptance criteria and fillable project, function and evidence records.

Built around ISO 12100 and ISO 13849-1:2023. The example values are fictional project inputs. They do not establish a safe design, a required PLr for your machine or conformity with the whole standard.

01 / DEFINE THE APPLICATION

Start with the loading task

A specification begins with the work a person actually has to perform, including interventions outside the automatic cycle.

The operator has to locate a 12 kg workpiece before powered clamping. In the original arrangement, a hand supports the part next to the closing jaw. Blocking jaw motion with the guard open leaves the loading task unresolved.

The example design decision

For this worked variant, a mechanical nest supports and locates the part without powered jaw motion. The operator withdraws both hands, closes the guard and uses the separate start sequence. Open-guard powered clamping is excluded. A real task that still needs such movement requires a different assessed protective concept.

Actual task	Hazardous situation	Assessment and specification link
TASK-L01 / load	Fingers enter the closing-jaw area while positioning the part.	RA-L01 -> SF-01. Assess the supporting nest as a separate mechanical measure.
TASK-I01 / intervene	Jam clearing or a positioning problem can change access and exposure.	Reassess the task. Do not extend SF-01 by simply bypassing the guard.
TASK-M01 / maintain	Cleaning, fault finding and stored energy introduce additional situations.	Assess isolation and any necessary powered work separately; define the relevant protection.

Project boundary: MC-01 is a hypothetical machining centre. SF-01 covers powered jaw motion for loading access. Spindle, axis, guard-release and feeder protections are related project functions, not silently covered by this one example card.

Keep the workpiece in the story

Removing energy is not automatically the safe reaction. First establish whether the part or a load can move, fall or be released, and how that risk is reduced.

02 / WORKED FUNCTION CARD

SF-01: define the required effect

Worked draft. PLr d, 200 ms, the 12 kg load and the duty profile are illustrative inputs, not project recommendations.

Field	Worked record	Clause link
SF-01 / identity and objective	SF-01 / MC-01. Stop and inhibit powered clamping motion during access to the loading fixture. The objective is to prevent finger crushing at the moving jaw.	5.1; 5.2.1.3 a)
APP-01 / task and risk	TASK-L01: load and locate a 12 kg workpiece in a supporting nest. HS-01: fingers enter the clamping area. Mock record RA-L01 supplies the function and protective concept. All identifiers and values in this example are fictional.	4.5; 5.1; 5.2.1.2
REQ-01 / trigger	An access request, or loss of the required closed/locked guard state while clamping motion is enabled, demands the function. The demand remains effective while loading access is open.	5.2.1.3 b)
REQ-02 / physical effect	Stop powered jaw movement and prevent further powered clamping motion during access. Do not issue an access-release permission before the specified clamp safe state is established. The supporting nest must retain the workpiece independently of clamping pressure.	5.2.1.3 c)
REQ-09 / PLr and basis	PLr d is an illustrative input assigned to SF-01 in the mock RA-L01 record. It is not a calculated or recommended PLr for machining centres. The real assessment and applicable type-C requirements must establish or confirm the project value before design release.	5.2.1.3 d); 5.3
REQ-03 / total time	EXAMPLE LIMIT: total time from the demand event at the protective device to cessation of the specified jaw movement ≤ 200 ms. Include sensing, logic, outputs and mechanics. Access remains locked until the required safe conditions of all relevant functions are established; 200 ms alone does not justify access safety.	5.2.1.3 e)
REQ-04 / modes	Active in automatic operation and manual loading. Powered jaw movement with the guard open is excluded from this example. If a real task needs it, reassess the task and specify the appropriate alternative protection before allowing that mode.	5.2.1.3 f); 5.2.2.9

OPEN-01 / justify the inputs

Before issuing a design baseline, replace or justify the fictional risk, PLr and time inputs for the actual machine and confirm all access conditions.

03 / WORKED FUNCTION CARD CONTINUED

SF-01: follow every machine state

Use the same function ID and revision. Interfaces, faults and energy behaviour belong to the requirement, not to undocumented commissioning decisions.

Field	Worked record	Clause link
REQ-05 / interfaces	Guard unlock requires the clamp safe-state permission AND the safe conditions for spindle, axes and any connected feeder. Those protections need their own specifications. SF-01 must not treat a normal PLC acknowledgement as proof that every connected hazard has ceased.	5.2.1.3 g)
REQ-06 / detected fault	A detected fault affecting the function inhibits new clamp motion and prevents an access-release permission until the required safe condition is established. Maintain the required safe state until the relevant fault is corrected. Fault acknowledgement does not replace repair.	5.2.1.3 h)
REQ-07 / energy	Loss or out-of-range electrical/fluid energy must not cause hazardous jaw motion or release the supported workpiece. Restoration must not initiate movement. The passive nest is a separate mechanical risk-reduction measure; its adequacy needs engineering evidence, not an automatic PLr label.	5.2.1.3 i); 5.2.2.8
APP-02 / duty profile	Illustrative use: 40 loading accesses/hour, 16 operating hours/day and 250 days/year = 160,000 demands/year. Record actual operations of each relevant element separately. The example profile is an input for design and lifetime assessment, not a reliability calculation.	5.2.1.3 j)
REQ-10 / priorities	A demand from SF-01 has priority over normal clamp-start commands. Emergency stopping and other safety demands must not defeat workpiece retention or permit an unsafe access release. Resolve conflicting reactions in the project safety concept.	5.2.1.3 k); 5.2.2.2
APP-03 / type-C input	Review the scope and applicable requirements of the machine's type-C standard, including clamping and access requirements. ISO 16090-1 is a relevant candidate for this hypothetical machining centre. The clause selection and any prescribed PLr remain OPEN-02 until recorded by the responsible engineer.	5.2.1.3 l)
REQ-08 / reset and restart	For this example, restoring the closed/locked guard state and required safety readiness permits a separate intentional reset, followed by a separate start command. Neither closing the guard, resetting nor restoring power starts clamp movement. If manual reset is itself a safety function, specify its PLr as required by the application.	5.2.1.3 m); 5.2.2.3
APP-04 / environment	Illustrative envelope: indoor use, 5 to 40 C, non-condensing, metal chips and coolant splash. Washdown and powered intervention with open access are excluded. Cleaning and maintenance tasks still require their own assessment and suitable isolation/protection arrangements.	5.2.1.2; 5.2.2.10

04 / ACCEPTANCE AND TRACEABILITY

Write the test before the signature

The records below are a test-planning example. No physical tests or analyses have been completed for this fictional machine.

Check	Required observation / acceptance basis	Link / status
VT-01 / trigger and stop	Apply the specified demand in controlled conditions at the relevant operating limits. Measure from the actual protective-device event to cessation of the specified jaw movement, including the mechanics. Compare with the example 200 ms limit.	REQ-01..03 / Not performed
VT-02 / access and inhibition	Confirm no powered clamp motion during open loading access. Verify access-release permission is withheld until the required safe conditions of SF-01 and the other relevant functions are established.	REQ-02, REQ-05 / Not performed
VT-03 / fault and energy	Use the planned analyses and prepared tests for applicable faults and energy variations/loss/return. Check the demanded safe reaction and prevention of unintended restart. Assess passive retention separately.	REQ-06, REQ-07 / Not performed
VT-04 / restart and modes	Check guard closing, reset, start and changes of mode as separate events. Confirm no loss of required protection during transitions and no powered open-guard clamping in the example operating concept.	REQ-04, REQ-08 / Not performed
VT-05 / integration	Check actual safe-state behaviour at spindle, axes and feeder interfaces, including loss of required signals. An acknowledgement bit alone is not the acceptance criterion.	REQ-05 / Not performed
VT-06 / use and envelope	Review the task, access frequency, loads, environment and any exclusions against the actual machine. Record test configuration, software/parameter versions, instruments, conditions and results.	APP-01, 02, 04 / Not performed

Add design/PL evidence for REQ-09 and priority checks for REQ-10. For timing, declare the protective-device event, physical endpoint, load, operating limits, method and uncertainty. State the acceptance rule before testing; an example conservative rule is measured time + stated uncertainty $\leq$ the specified time limit.

Do not close the SRS with an unexplained blank

Carry OPEN-01 (actual risk/PLr/time basis) and OPEN-02 (type-C applicability and requirements) into the project issue register. Record an owner, due point and disposition. A completed template alone is not a design release or full conformity evidence.

05 / FILLABLE WORKSHEET

Project and risk-assessment inputs

Fill these fields for the actual machine. Link the controlled risk assessment, task information and protective concept before drafting individual function cards.

Project / machine / physical boundary

SRS document ID / revision / status / date

Intended use, machine limits and affected zones

Operator, setup, cleaning and maintenance tasks / foreseeable misuse

Risk-assessment reference / hazardous situations / required risk reduction

Protective concept / non-control measures / related safety functions

Applicable type-C and other requirements / applicability decisions

Environment / loads / duty profile / assumptions and exclusions

06 / FILLABLE FUNCTION CARD A

Make the function testable

One controlled record per function. Use a function ID, revision and links that can be followed into design and validation. Continue on the next page.

Function ID / title / revision

Actual task / risk-assessment and hazardous-situation references

Demand event / activation and persistence conditions

Required output reaction AND intended physical safe state

PLr for this function / risk or type-C basis / decision reference

Total response time / physical endpoint / timing justification

Modes in which protection is active / transitions / excluded tasks

Specify measurable behaviour. "Stop safely", a component list and a PL letter do not describe when the function acts or what the complete machine has to do.

07 / FILLABLE FUNCTION CARD B

Keep protection through the sequence

Continuation of the same function. Enter a justified N/A where a field does not apply; an empty field does not explain a design decision.

Function ID / revision - match card A

Interfaces with machine control / other functions / adjacent machines

Detected faults / required reaction / maintaining the safe state

Energy variation, loss and restoration / load or workpiece retention

Demand rate / element operations / intended duty and lifetime inputs

Priority and conflicts when functions are active together

Applicable type-C requirements / scope / clause and decision references

Conditions for reset and restart / visibility and presence considerations

08 / FILLABLE EVIDENCE RECORD

Leave a trail the next engineer can use

Connect each requirement to its risk basis, design and evaluation. Record the actual status; this worksheet contains no pre-approved results.

Requirement ID -> risk record -> design reference -> evidence reference

Assessed configuration / software and parameter versions / load and conditions

Acceptance criterion / method / instruments and uncertainty where relevant

Measured or analysed result / pass-fail decision / record location

Open issues / owner / due point / disposition

Change / affected tasks, functions and evidence / reassessment decision

Prepared by / reviewed by / dates / review and release status

Review is a recorded engineering decision

Review the SRS before design (5.4), address SRS validation (10.2), and plan the later verification and validation of the implementation. Document control is part of the technical record; it does not replace this engineering work.

09 / COMPLETION AND SOURCE MAP

Know what the form covers

The workbook is an original organisational aid. It paraphrases the requirements; it does not reproduce the standard or prescribe the only acceptable SRS format.

ISO 13849-1:2023	Where to make the decision visible	Worksheet
5.2.1.3 a)	Function identity and objective	Card A
5.2.1.3 b)	Demand / activation	Card A
5.2.1.3 c)	Output reaction and physical safe state	Card A
5.2.1.3 d)	PLr and decision basis	Card A
5.2.1.3 e)	Total response to the safe state	Card A
5.2.1.3 f)	Modes and transitions	Card A
5.2.1.3 g)	Control and function interfaces	Card B
5.2.1.3 h)	Detected-fault behaviour	Card B
5.2.1.3 i)	Energy loss and restoration	Card B
5.2.1.3 j)	Demands and operations	Card B
5.2.1.3 k)	Concurrent-function priorities	Card B
5.2.1.3 l)	Applicable machine-standard requirements	Card B
5.2.1.3 m)	Conditions for restarting	Card B

Application inputs: 4.5, 5.1 and 5.2.1.2. Additional function-specific requirements: 5.2.2. PLr determination: 5.3. SRS review: 5.4. SRS validation: 10.2. Technical documentation: 12 a). Annex M provides further information on typical functions.

Primary references

ISO 12100:2010 - risk assessment and risk reduction, particularly the machine limits, tasks, hazards and protective concept. ISO 13849-1:2023 - specification, design and evaluation of safety-related parts of control systems. Consult the applicable licensed editions and machine-specific standards.

[ISO 12100:2010 / official catalogue](#)

[ISO 13849-1:2023 / official catalogue](#)

SRS is the starting specification, not the whole conformity case

A project still needs the applicable design, integration, PL evaluation, software, verification, validation and documentation work. Review changes to tasks, tooling, loads, access and parameters against the original risk and requirement basis.