

SIL VERIFICATION REPORT

Three-gate verification record for one Safety Instrumented Function

PROJECT	PROJECT NUMBER
SILProof Example Demonstration Plant	SP-EX-001
PLANT / UNIT	TARGET
Separator V-101	SIL 2

SAFETY INSTRUMENTED FUNCTION

SIF-Example-LSH

High-High Separator Level Shutdown

WORKED EXAMPLE

REVISION HISTORY

REV.	DATE	PURPOSE	PREPARED	STATUS
Rev. 0	2026-09-06	Draft	SILProof Reference Engineering	Draft

REVIEW AND APPROVAL

ROLE	NAME / FUNCTION	DATE	SIGNATURE
Prepared	SILProof Reference Engineering	2026-09-06	
Checked	Functional Safety Review		
Approved	Project Engineering		

1 Purpose and assessment boundary

This report follows SIF-Example-LSH, a low demand safety instrumented function, from its risk target to the reliability, architecture and systematic checks that support its SIL claim. The quantitative measure is the average probability of failure on demand (PFDavg); it is one of three gates, and the claimed SIL is the lowest of the three. The report also states the operating conditions that keep the result valid. Where the project record does not hold a value, the report says so rather than assuming one.

The function is defined in safety requirements specification SRS-SIF-101, Rev. 0. The calculation was made with SILProof, Engine 2026.10.1 · algebraic.

2 Risk basis and function definition

High-high separator level can cause liquid carryover into downstream equipment. Credible causes are inlet flow exceeds separation capacity and level control valve fails open. The consequence to be prevented is: potential mechanical damage and loss of containment downstream. The function's purpose is to prevent liquid carryover to the downstream flare/compression system by initiating an independent shutdown on high-high separator level.

Parameter	Basis
Risk assessment	LOPA; LOPA scenario L-101-HH; HAZOP Node V-101 — high level deviation; initiating event $2.5e-2$ /yr; independent protection layers: Independent high-level alarm with operator response (PFD $1e-1$), Second independent protection layer (PFD $1e-1$); tolerable frequency $1e-6$ /yr
Required risk reduction	SIL 2; RRF ≥ 250 ; allocated PFDavg $\leq 4.0 \times 10^{-3}$.
Demand	Low demand; 0.1 demands/year
Trip initiation	LT-101A/B/C, Separator level, setpoint HH level setpoint, 2oo3 voting
Safe state	Isolate the separator inlet by closing XV-101A and XV-101B.
Timing	Process safety time 10 s. Allocated response 1.5 s sensing + 0.5 s logic + 4 s final element + 0.5 s other delays = 6.5 s.
Reset and restart	Manual reset; Initiating condition cleared and process safe to restart; authorised by operator with approved procedure; Restart permitted only after field verification
Included boundary	LT-101A/B/C through safety PLC SPLC-101 to XV-101A/B including associated I/O, power and final-element interfaces.
Trip action	De-energize to trip
Functional description	High-high level in separator V-101 is detected by a 2oo3 level measurement system and initiates the safety PLC to close the inlet ESD valves.
Operating mode	Continuous process operation; SIF armed during normal production.
Independence	The SIS is independent of the BPCS level control loop.
Common cause controls	Diverse process connections and 5% beta assumed for redundant channels; confirm on the project.
Loss of energy	Instrument air and safety PLC power. Loss of required energy shall move final elements to the closed safe state.
Availability requirement	Less than 0.1 spurious trips per year as an operational constraint.
Mission time	20 years

Executive summary

SIL 2 TARGET ACHIEVED

Required SIL 2 | Overall design claim SIL 2 | IEC 61508 — Route 1H | Low demand

SIF-Example-LSH meets the SIL 2 target. The SILProof calculation gives PFDavg 9.509×10^{-5} (RRF 10,516) against an allocation of 4.0×10^{-3} . The sensor and logic solver architectural constraints govern the SIL 2 claim.

Assessment	Result	Disposition
Quantitative reliability	PFDavg 9.509×10^{-5}	Meets allocation $\leq 4.0 \times 10^{-3}$
Hardware architecture	IEC 61508 — Route 1H: maximum SIL 2	Meets required SIL 2
Systematic capability	Lowest subsystem SC 3	Supports a SIL 2 claim
Spurious trip rate	0.00882 trips/year	SRS: Less than 0.1 spurious trips per year as an operational constraint.

3 Functional architecture

The trip is initiated by LT-101A/B/C voting 2oo3, through the SPLC-101 logic solver (1oo2D), to the final elements in 1oo2 voting between 2 legs (Isolation Path A: SOV-101A → XV-101A; Isolation Path B: SOV-101B → XV-101B). Components drawn in one leg act in series: each must work for that leg to act.

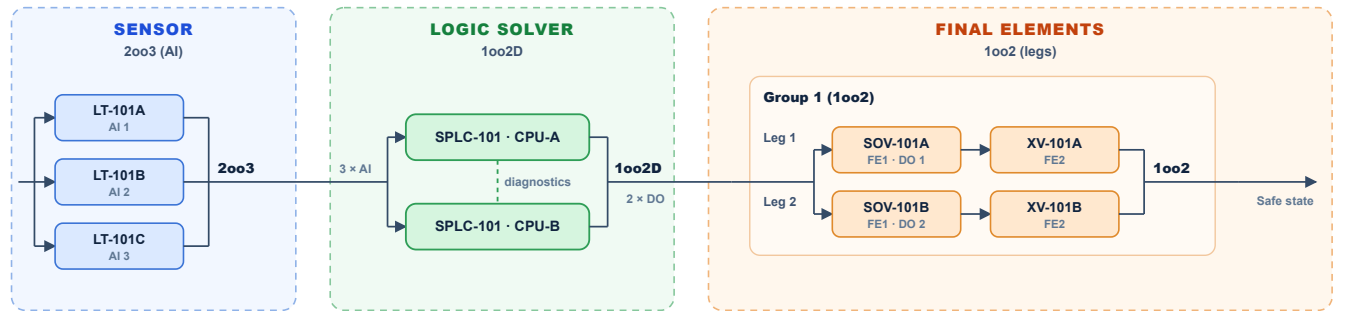


Figure 1. Trip path and voting of SIF-Example-LSH, as drawn by the SILProof workspace.

Final-element group	Voting	Leg	Series components
Group 1	1oo2	Isolation Path A	SOV-101A → XV-101A
Group 1	1oo2	Isolation Path B	SOV-101B → XV-101B

4 Input data and model assumptions

The SIF uses 6 recorded data sets, covering SILProof Reference Instruments SP-REF-LT-300, SILProof Reference Safety PLC SP-REF-SPLC-1oo2D, SILProof Reference Solenoid SP-REF-SOV-24 and SILProof Reference Valve SP-REF-ESD-150. Failure rates are per channel for the sensor and logic solver and per component for each final-element leg, in FIT ($1 \text{ FIT} = 10^{-9} \text{ failures/hour}$; 1 year = 8,760 hours).

Element	λ_{DU}	λ_{DD}	λ_{SU}	λ_{SD}	Reliability data source	Rate multiplier
LT-101A/B/C Sensor, per channel	60	160	20	10	Certificate	×1
SPLC-101 Logic solver, per channel	25	120	15	8	Certificate	×1
SOV-101A Final element, Isolation Path A	35	100	15	8	Certificate	×1
XV-101A Final element, Isolation Path A	60	180	25	10	Certificate	×1
SOV-101B Final element, Isolation Path B	35	100	15	8	Certificate	×1
XV-101B Final element, Isolation Path B	60	180	25	10	Certificate	×1

Every data set has a recorded source.

Element	Vote / type	PTC	Test interval	MTTR	Common cause
LT-101A/B/C	2oo3 / Type B	95%	1 year	6 h	5%
SPLC-101	1oo2D / Type B	99%	1 year	4 h	5%
SOV-101A	1oo2 legs, series in leg / Type A	90%	1 year	6 h	5%
XV-101A	1oo2 legs, series in leg / Type A	90%	1 year	6 h	5%
SOV-101B	1oo2 legs, series in leg / Type A	90%	1 year	6 h	5%
XV-101B	1oo2 legs, series in leg / Type A	90%	1 year	6 h	5%

4.1 Reliability model basis

Closed-form PFDavg: each channel's piecewise-linear unavailability $q(t)$ over the mission, the M-of-N vote taken at every instant and averaged exactly, β -factor common cause; final-element legs and groups are voted the same way. IEC 61508-6 Annex B is used only as the benchmark. Engineering support. Not a certification claim. 5% common-cause factor applied to redundant channels; independence/CCF basis documented for the reference case. The model uses a 20-year mission time.

$q(t) = \lambda_{DU} \cdot [\text{PTC} \cdot (t \bmod \text{TI}) + (1 - \text{PTC}) \cdot t] + \lambda_{DU} \cdot \text{PTC} \cdot \text{MRT} + \lambda_{DD} \cdot \text{MTTR}$ (a partial stroke test adds its own sawtooth)

$q_i(t) = (1 - \beta) \cdot q(t)$, $q\beta = \beta \cdot \bar{q}$ ($\bar{q}$ = mission average of q)

$\text{PFD}_i = (1/\text{MT}) \cdot \int_0^{\text{MT}} \sum C(N, k) \cdot q_i(t)^k \cdot [1 - q_i(t)]^{N-k} dt$, summed over $k = N - M + 1 \dots N$ (exact between tests)

$\text{PFD}_{\text{avg}} = q\beta + (1 - q\beta) \cdot \text{PFD}_i$ $1\text{oo}2 = E[q_i^2]$, $2\text{oo}3 = 3E[q_i^2] - 2E[q_i^3]$

$1\text{oo}2\text{D}$: $\text{PFD}_i = E[u^2 + 2u \cdot d]$, $d = ((1 - \beta_D) \lambda_{DD} + \lambda_{SD}) \cdot \text{MTTR}$; plus $\beta \cdot \bar{u} + \beta_D \cdot \lambda_{DD} \cdot \text{MTTR}$

No uncertainty multiplier is applied: the calculation uses the stated failure rates.

4.2 λ DU sensitivity cases

Dangerous undetected rates carry the largest influence on the result. The table shows each λ DU as used in the calculation and the halved and doubled cases that the sensitivity check applies in Section 5.3. λ DD, λ SU and λ SD are unchanged in these cases; this is an engineering check, not a statistical confidence interval.

Element	λ DU used (FIT)	λ DU $\times 0.5$ case	λ DU $\times 2$ case
LT-101A/B/C	60	30	120
SPLC-101	25	12.5	50
SOV-101A	35	17.5	70
XV-101A	60	30	120
SOV-101B	35	17.5	70
XV-101B	60	30	120

5 Quantitative reliability and availability

5.1 Probability of failure on demand

The low-demand calculation produces the subsystem values below. For this independent subsystem model, loop $PFD_{avg} \approx \sum PFD_{avg,i} = 9.5092 \times 10^{-5}$, rounded to 9.509×10^{-5} . $RRF = 1/PFD_{avg} \approx 10,516$. The result is within the allocation of 4.0×10^{-3} . The final elements contribute the largest share, 65.2%.

Subsystem	Architecture	PFD_{avg}	Share
Sensor	2oo3	2.653×10^{-5}	27.9%
Logic Solver	1oo2D	6.563×10^{-6}	6.9%
Final elements	1oo2 legs	6.200×10^{-5}	65.2%
Loop total	Series of subsystems	9.509×10^{-5}	100%

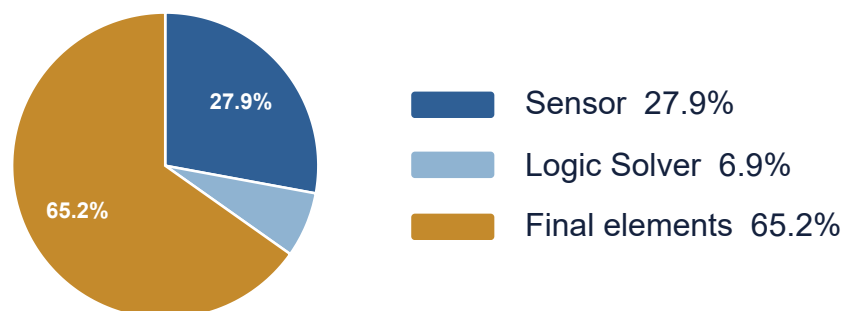


Figure 2. Share of calculated loop PFD_{avg} by subsystem.

5.2 Spurious trip rate

STR estimates how often hardware faults could cause an unintended shutdown. It is separate from PFD_{avg} and does not set the SIL claim. Conservative rate sum. Not a spurious-trip study.

Subsystem	Architecture	STR per hour
Sensor	2oo3	1.887×10^{-7}
Logic Solver	1oo2D	1.427×10^{-7}
Final elements	1oo2 legs	6.760×10^{-7}
Loop total	Sum of subsystems	1.007×10^{-6}

STR is 1.007×10^{-6} /h, or 0.00882 trips/year; mean time to a modelled spurious trip is about 113 years. It is not a guaranteed operating interval. SRS requirement: Less than 0.1 spurious trips per year as an operational constraint.

5.3 Sensitivity and robustness

Each case changes one parameter family; all other inputs stay fixed. Coverage changes are percentage points, capped at 100%. Values are taken from the workspace sensitivity output.

Variation	Lower PFDavg	Higher PFDavg	Upper case as % of limit
Proof test coverage +10 pts / -10 pts	4.010×10^{-5}	1.755×10^{-4}	4.39%
λ DU (every device) $\times 1/2$ / $\times 2$	4.702×10^{-5}	1.948×10^{-4}	4.87%
Common cause $\beta \times 1/2$ / $\times 2$	4.889×10^{-5}	1.875×10^{-4}	4.69%
Proof test interval $\times 1/2$ / $\times 2$	7.600×10^{-5}	1.339×10^{-4}	3.35%
Repair time (MTTR) $\times 1/2$ / $\times 2$	9.499×10^{-5}	9.530×10^{-5}	2.38%

The highest individual result is the λ DU (every device) $\times 2$ case, 20.5 times below the limit. These checks are not a combined worst case or a statistical confidence bound, and they do not authorise changes to proof testing or other operating controls.

5.4 Quantitative acceptance and margin

Case	Loop PFDavg	RRF	Result
Base case (verified result)	9.509×10^{-5}	10,516	Pass: $\leq 4.0 \times 10^{-3}$

The verified result is the base case, as calculated by SILProof. Architecture limits the claim to SIL 2.

6 Hardware architectural constraints

The architectural route (IEC 61508 — Route 1H) combines element type, hardware fault tolerance and safe failure fraction. $SFF = (\lambda DD + \lambda SU + \lambda SD) / (\lambda DU + \lambda DD + \lambda SU + \lambda SD)$; $DC = \lambda DD / (\lambda DU + \lambda DD)$, which is different from proof-test coverage.

Subsystem	Type / HFT	SFF	DC	Route	Architectural limit
Sensor	B / 1	76.0%	72.7%	Route 1H	SIL 2

Subsystem	Type / HFT	SFF	DC	Route	Architectural limit
Logic Solver	B / 1	85.1%	82.8%	Route 1H	SIL 2
Final elements	A / 1	78.1%	74.7%	Route 1H	SIL 3
Overall	—	—	—	—	SIL 2

The sensor and logic solver limit the architecture to SIL 2, which meets the SIL 2 target. A lower PFDavg does not remove that limit.

7 Systematic capability and evidence register

Systematic capability concerns design and implementation faults; PFDavg and SFF do not establish it. The lowest recorded capability is SC 3, which supports the SIL 2 target. 6 of 6 devices have no certificate or safety-manual reference recorded.

Device	Manufacturer / model	SC	Basis	Certificate / safety manual
LT-101A/B/C	SILProof Reference Instruments SP-REF-LT-300	SC 3	Certified	<i>Reference not recorded</i>
SPLC-101	SILProof Reference Safety PLC SP-REF-SPLC-1002D	SC 3	Certified	<i>Reference not recorded</i>
SOV-101A	SILProof Reference Solenoid SP-REF-SOV-24	SC 3	Certified	<i>Reference not recorded</i>
XV-101A	SILProof Reference Valve SP-REF-ESD-150	SC 3	Certified	<i>Reference not recorded</i>
SOV-101B	SILProof Reference Solenoid SP-REF-SOV-24	SC 3	Certified	<i>Reference not recorded</i>
XV-101B	SILProof Reference Valve SP-REF-ESD-150	SC 3	Certified	<i>Reference not recorded</i>

Supporting document	Reference	Source and note
LOPA target SIL Risk assessment	LOPA L-101-HH	Reference engineering basis — Illustrative LOPA basis establishing SIL 2 and a precise required RRF of 250×.
SIF functional requirements SRS	SRS-SIF-101 Rev. 0	SILProof Example SIF — Defines trip, safe state, response time and reset requirements.
Failure-rate data Calculation input	REF-FR-001	SILProof reference dataset — Hypothetical FIT values used consistently by the calculation engine.
Architecture basis IEC 61508 basis	Route 1H / architecture check	SILProof verification engine — Voting, HFT, SFF and systematic capability are checked in the verification.
Proof-test strategy Proof test	PT-101-SIF-001	SILProof Example SIF — Annual full-loop proof test with final-element stroke testing.

8 Conditions for maintaining the verified design

The conclusion of this report applies to the configuration described above and holds only while the following conditions are kept. Proof tests are credited at 1-year intervals, with the coverage and repair times shown. Changes to the function, devices, intervals or assumptions require a documented impact review and re-verification.

Device	Test interval	PTC	Partial stroke test	MTTR	MRT	Mission time
LT-101A/B/C Sensor	1 year	95%	—	6 h	As MTTR	20 years
SPLC-101 Logic solver	1 year	99%	—	4 h	As MTTR	20 years
SOV-101A Final element	1 year	90%	Not used	6 h	As MTTR	20 years
XV-101A Final element	1 year	90%	Not used	6 h	As MTTR	20 years
SOV-101B Final element	1 year	90%	Not used	6 h	As MTTR	20 years
XV-101B Final element	1 year	90%	Not used	6 h	As MTTR	20 years

Requirement from the SRS	Recorded value
Assumed SIF response time	6.5 s (sensor 1.5 s + logic 0.5 s + final element 4.0 s + other 0.5 s)
Process safety time	10 s
Bypass / override basis	Permitted; authorisation: Permit and operations authorization; maximum duration: Maximum 4 h; compensating measures: Compensating measures and attended operation required; indication: Dedicated bypass indication in operator interface

8.1 Proof test and restoration basis

Item	SRS requirement
Proof-test interval	12 months
Method and scope	Full loop proof test including sensor simulation, voting verification, logic trip test and final-element stroke test.
Required coverage	90% assumed for final elements; sensor and logic coverage per example data.
Procedure	PT-101-SIF-001
Acceptance criteria	Trip occurs at specified setpoint; all channels and final elements respond within allocated time.
Maximum restoration time	24 h

Item	SRS requirement
Process safety during test	Partial stroke testing may be used where justified by procedure.
Calibration	Annual calibration per instrument procedure.

9 Engineering recommendations

No design corrective action is identified. Complete the following before issue, and continue the periodic reviews:

- Record the certificate or safety-manual reference for each device (Section 7).
- Review demand, failure and nuisance-trip records against the SRS assumptions at least annually.
- Reassess the model after device, logic, proof-test or fault-response changes; retain the revision history.

Conclusion

SIF-Example-LSH meets the SIL 2 target under the stated assumptions. The loop PFD_{avg} is 9.509×10^{-5} . The operating conditions in Section 8 and the reviews in Section 9 preserve the assessment basis.

Review and sign-off

Role	Name / function	Date	Signature
Prepared	SILProof Reference Engineering	2026-09-06	
Checked	Functional Safety Review		
Approved	Project Engineering		

Method references

Framework: IEC 61508-2:2010, IEC 61508-6:2010 and IEC 61511-1:2016+A1:2017. Calculation: Engine 2026.10.1 · algebraic. SILProof is engineering-support software; this report is not a certificate, an independent functional safety assessment or a validation record, and the responsible organisation remains accountable for the data and decisions it records.

Abbreviations and symbols

Term	Meaning	Term	Meaning
SIL	Safety integrity level	SIF	Safety instrumented function
SRS	Safety requirements specification	LOPA	Layer of protection analysis
PFD _{avg}	Average probability of dangerous failure on demand	PFH	Average frequency of dangerous failure per hour
RRF	Risk reduction factor	SC	Systematic capability
HFT	Hardware fault tolerance	SFF	Safe failure fraction
DC	Diagnostic coverage	PTC	Proof-test coverage
MTTR / MRT	Mean time to restoration / mean repair time	STR	Spurious trip rate
FMEDA	Failure modes, effects and diagnostic analysis	FIT	Failures in time: 1 FIT = 10 ⁻⁹ /h
MooN	M out of N voting; 2oo3 means two out of three	CCF / β	Common cause failure / common cause fraction
λ_{DU} / λ_{DD}	Dangerous undetected / detected failure rate	λ_{SU} / λ_{SD}	Safe undetected / detected failure rate