

Evidence Report

Falke-Werk · SIL Validation (CamFollow & WP4 Smoke)

ISO 13849 / ISO 13855:2024 · Sealed Runs

Deterministic Safety Validation · ViProve · for Notified Body Review

Document ID	VIP-NB-ROBOTIK-FALKE-WERK-20260830
Project	Robotik Falke-Werk (Falke-Werk)
Scope	CamFollow Smoke + WP4 Smoke · sealed runs 1–21
Standards	ISO 13849 / ISO 13855:2024 / ISO 10218
Version / date	VIP-NB-ROBOTIK-FALKE-WERK-20260830 · 30 August 2026
Issuer	ViProve · responsible person not assigned in the graph
JSON seal	evidence-report.json
Classification	Controlled — for Notified Body (working document, not a certificate)

This document is a **working document for assessment** (notified body / TÜV). It summarizes the state of the evidence chain from the project graph. It does not replace the Technical Documentation under the Machinery Regulation nor a Declaration of Conformity.

Counting rule: only edges with status **confirmed** or **inferred** count as evidence. Proposed candidates (O) are not counted. Application screenshots are not evidence. Sealed SIL test runs — run table, fail explanations, step images and the featured recording — are **Appendix C and D** (video as a sibling file).

0. Executive Summary

This Evidence Report documents the deterministic SIL validation runs of the scenarios **falke:CamFollow Smoke** and **falke:WP4 Smoke** (ViProve · Falke-Werk · Robotik Falke-Werk).

Scope

- Standards referenced: ISO 13849 and ISO 13855:2024
- Runs covered: Run 1–21 (as of 30.08.2026)
- Evidence format: sealed test runs including status (P/F/n), seal hash, and optional video/screenshot evidence

Result Overview

The runs are technically completed and reproducibly logged. Some runs passed fully (e.g. 3/0/3), while several show mixed results (P/F/n observed: 12/7/19, 7/3/10, 9/7/16, 14/7/21, 0/1/1). Existing seals and media evidence enable traceability of the successful executions. Fail cases include expected vs. actual zone/SSM-speed with references to the relevant criteria (R1 protective stop, R3 early detection) in Appendix D.

Key Open Points

- Open graph gaps remain (counts in §2): NORM_GAP 1.673, SYS_GAP 9, TEST_GAP 898, INTEGRITY_GAP 10 — SIL runs do not close requirement-level tests of every SYS.2 statement
- End-to-end chain Requirement → Test → Run → Seal is shown in §1; remaining work is closing the graph gaps, not documenting the chain

Release Recommendation

This report is released for **internal reviews and pilot customers**.

For formal submission to a Notified Body, remaining open graph gaps (see §2) must still be closed. Traceability (Requirement → Test → Run → Seal) and the compact gap summary are included in this document. Only after those gaps are closed is the report recommended as a standalone evidence package.

The machine-readable seal payload (`evidence-report.json`) and the gap-chain JSON (`gap-chain.json`) shall be attached to this PDF (ZIP).

1. Traceability (Requirement → Test → Run → Seal)

Intended evidence chain for this SIL package: **Requirement (SYS.2 / FSC) → Test → sealed Run → Seal** (and video where recorded). Graph TEST_GAP items are still open (18 SYS.2 without a test edge). The featured SIL run is **cell-level protocol evidence**, not a substitute for those edges.

1 · REQUIREMENT

18

SYS.2 in the project graph
FSC in §8

2 · TEST

0

SYS.2 with a graph test edge
open TEST_GAP 18

3 · RUN

Run 19

Patrouille (Template) · P/F/n
12/7/19
Appendix C / D

4 · SEAL

b17880921b434bb1...

Run seal · evidence-run-
19.mp4
graph: evidence-report.json

SYS.2	STATEMENT (EXCERPT)	GRAPH TEST	SIL RUN / SEAL / VIDEO
Dynamic Hazard Radius Calculation sysreq: falke:3ac30f5076	The system shall dynamically calculate the hazard radius Rh using the formula Rh = reach +	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
HW Bridge Raw Data Only sysreq: falke:16627a378a	The sensor_layer implementation (hwbridge) shall deliver only raw sensor data over TCP por	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
Independent Safe Monitor Architecture sysreq: falke:45e16a0a4a	The safe_monitor shall be implemented on hardware or software distinct from the performanc	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
LiDAR Primary Detection Role sysreq: falke:20d07d0b9c	The sensor_layer shall utilize the LD-360 LiDAR (PL e) as the primary detection source for	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
Patrouille Scenario Stop Events sysreq: falke:44be737d1a	The system shall correctly trigger 3 stop events during the 'Patrouille' scenario where a	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
Performance Layer Non-Safety Role sysreq: falke:f5c35d4e6c	The performance_layer (ROS 2) shall perform sensor fusion and zone evaluation for function	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
R1 Zone Stop Reaction sysreq: falke:bc88fc894a	The system shall initiate a Protective Stop (STO) for the associated robot arm when a huma	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
R2 Zone Speed Reduction sysreq: falke:4048095481	The system shall reduce the robot speed when a human enters the R2 zone defined by the for	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
R3 Zone Early Detection sysreq: falke:6d856c08b5	The system shall activate early detection monitoring when a human enters the R3 zone defin	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...

SYS.2	STATEMENT (EXCERPT)	GRAPH TEST	SIL RUN / SEAL / VIDEO
Radar Robustness Detection sysreq:falke:10f6311162	The sensor_layer shall utilize the RX-240 Radar (SIL 2) for long-range detection robust ag	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
Safe Monitor Autonomous STO Trigger sysreq:falke:72e28be838	The safe_monitor layer shall autonomously trigger a Safe Torque Off (STO) signal when the	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...
Static Object Masking sysreq:falke:6bce378db1	The system shall mask known static objects (e.g., GT-75) within the protective field using	No graph test edge (TEST_GAP)	Run 19 · Patrouille (Template) · twin protocol (not a SYS.2 unit test) b17880921b434bb1...

Featured recording file: evidence-run-19.mp4 · run JSON: evidence-run-19.json · graph seal payload: evidence-report.json.

2. Gap Summary

Compact overview for the notified body. Counts match `gap-chain.json`. Criticality is for **formal submission**, not for whether the twin currently runs. A Pass in Appendix C does not close TEST_GAP.

NORM_GAP	SYS_GAP	TEST_GAP	INTEGRITY_GAP	RESULT_GAP
1.673	9	898	10	0
Clause without SYS.2	SYS.2 without SWE.1	Requirement without test	PL/SIL vs layer	SIL protocol P/F/n

GAP	COUNT	CRITICALITY	STATUS / CLOSURE
NORM_GAP	1.673	Blocking for type examination completeness	Open — in-scope clauses without SYS.2; full list in gap-chain.json
SYS_GAP	9	Blocking where SYS.2 has no SWE.1	Open — see §10 excerpt
IMPL_GAP	890	Blocking where a requirement has no code evidence	Open — requirement without SWE.1 / implementation edge
TEST_GAP	898	Blocking for requirement-level validation	Open — SYS.2/SWE.1 without test evidence; SIL runs do not close this
INTEGRITY_GAP	10	Blocking for ISO 13849 allocation (PL/SIL vs layer)	Open — FSC findings in §8
RESULT_GAP	0	Not blocking if SIL protocols in Appendix C are complete	See P/F/n and Appendix D
OVER_FILL	57	Not blocking (extra SWE.1 without SYS.2 parent)	Documented; not counted as coverage · same count as §10

3. Scope and Acceptance Criteria

In scope. Robotik Falke-Werk (Falke-Werk, robotics hall / digital twin). SIL scenarios **Patrouille (Template) · Szenario 2**, sealed runs 1–21. Graph evidence for ISO 13849 and ISO 13855:2024 (protective separation / SSM zones) and the FSC allocated in the project graph.

Out of scope. Machinery Regulation technical file and Declaration of Conformity. Certification of the physical robot controller. Hardware SIL of sensors. Full clause-by-clause type examination. Application screenshots as evidence (only sealed runs and the graph count).

Pass criteria (SIL scenario)

CRITERION	RULE
Zone match	At each recorded waypoint, <code>actual_zone</code> equals <code>expected_zone</code> (JSON array Arm A / Arm B / VI-7: CLEAR, MONITOR, WARN, STOP) — ISO 13855 SSM radii, not a screenshot judgement.
Speed / SSM	<code>actual_speed</code> equals <code>expected_speed</code> (100 %, reduced, STOP).
Completed	Run has <code>status=completed</code> and <code>finished_at</code> set. Running or aborted runs are not evidence.
P/F/n	Passed steps / failed steps / total recorded steps. A run with <code>failed_steps > 0</code> is a protocol Fail (see Appendix D).
Seal	SHA-256 over the canonical run JSON (steps without images) plus the video digest. Valid only for that exact payload; a new recording is a new seal. Graph seal is a separate hash over project totals (evidence-report.json).

4. Seal

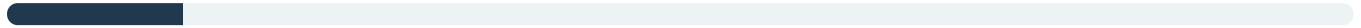
SHA-256 over the canonical JSON payload (project, totals, per standard, test cases), algorithm sha256. File in the ZIP: evidence-report.json.

```
535377291da04e1b15d540805265e80719fb4ee60a59ea79cdaa4650f7e78d45
```

Discrepant numbers between HTML and JSON indicate different generation runs were used.

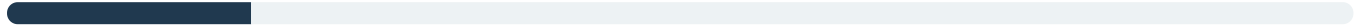
5. Coverage

Clauses with requirements



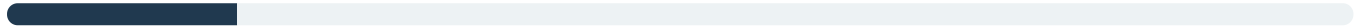
249 / 1.922 · 13.0 %

Requirements with code evidence



194 / 1.084 · 17.9 %

Requirements with test evidence



186 / 1.084 · 17.2 %

Test cases total: 6 · never run: 2 · with failures: 3

6. Per Standard

STANDARD	CLAUSES	NORM_GAP	REQ.	IMPL.	IMPL_GAP	TESTED	TEST_GAP
ISO 10218-2:2025	178/453	275	933	194	739	186	747
ISO 13849-1:2023 (Knowledge Summary)	30/38	8	58	0	58	0	58
ISO 13849-2:2012 (Knowledge Summary)	27/32	5	49	0	49	0	49
ISO 13855:2024 (Knowledge Summary)	14/20	6	44	0	44	0	44
EU AI Act	0/140	140	0	0	0	0	0
EU-Maschinenrichtlinie	0/76	76	0	0	0	0	0
IEC 61508-1:2010	0/254	254	0	0	0	0	0
IEC 61508-2:2010	0/180	180	0	0	0	0	0
IEC 61508-3:2010	0/202	202	0	0	0	0	0
IEC 61508-4:2010	0/121	121	0	0	0	0	0
IEC 61508-5:2010	0/42	42	0	0	0	0	0
IEC 61508-6:2010	0/13	13	0	0	0	0	0
IEC 61508-7:2010	0/67	67	0	0	0	0	0
ISO/SAE 21434:2021	0/284	284	0	0	0	0	0

7. V-Model Chain (Deterministic)

Graph query without LLM · Scene falke · Artifact 2026-08-20T18:45:52+00:00

1 · G1 STANDARD TARGET

392 / 1.084

in scope · SYS.2 coverage 15
out of scope 692 · pending 0

2 · SYS.2 SYSTEM

18

with SWE.1 9 · tested 0
Digital Twin

3 · SWE.1 SOFTWARE

66

with SYS.2 9 · tested 0
reconstructed from code

4 · FSC

12

Safety Functions
Integrity findings 10

LEVEL	STATUS	NOTE
G1 · Standard target	392 in scope / 1.084 · SYS.2 coverage 15	out of scope 692 · pending 0
SYS.2 · System	18 · with SWE.1 9 · tested 0	Digital Twin
SWE.1 · Software	66 · with SYS.2 9 · tested 0	Reconstructed from code
FSC · Safety Functions	12	Integrity findings 10

8. Functional Safety Concept (FSC)

Safety functions from the project graph (ISO 13849 / ISO 10218). PL/SIL is the required integrity level, not an issued certificate.

SAFETY FUNCTION	PL / SIL	LAYER	DESCRIPTION
Access Proximity Detection	—	—	Near-field detection at cell access points using Ultrasonic sensors.
Dynamic Hazard Radius Calculation	PL d	—	Real-time calculation of the hazard radius based on current robot reach, nominal TCP speed, and system reaction times to define dynamic zone boundaries.
Early Detection Monitoring	PL d	—	Monitoring of the outermost zone to provide early warning and prepare the system for potential speed reduction or stop.
Emergency Stop	PL e	—	Not-Halt nach ISO 13850
Monitored Speed	PL d	—	Überwachte Geschwindigkeitsbegrenzung
Monitored Standstill	PL d	—	Überwachtes Stillstehen mit sicherer Abschaltung
Primary Spatial Detection	PL e	—	360° spatial monitoring using LiDAR as the primary detection source for human presence.
Protective Stop	PL d	—	Schutzabschaltung bei Gefahr
Protective Stop (STO)	PL d	—	Autonomous triggering of Safe Torque Off to stop robot motion immediately upon detection of a human in the critical stop zone.
Raw Sensor Data Provision	—	—	Delivery of raw sensor data from all sensors to the processing layers via the hardware bridge.
Reduced Speed	PL d	—	Reduzierte Geschwindigkeit für sicheren Eingriff
Robust Long-Range Detection	SIL 2	—	Long-range detection using Radar, robust against dust and light interference, to complement LiDAR.
Software-based Limiting	SIL 2	—	Software-seitige Kraft-/Geschwindigkeitsbegrenzung
Speed Reduction	PL d	—	Reduction of robot speed to a safe level when a human enters the warning zone, allowing for a controlled stop if the human continues to approach.
Static Object Masking	PL d	—	Filtering of known static objects from the sensor data using an environment map to prevent false positive safety triggers.
Worst-Case Zone Aggregation	PL d	—	Evaluation of the overall system safety state by determining the worst-case zone state across all monitored entities (ARM A, ARM B, VI-7).
Zone Edge Depth Evaluation	PL d	—	Provision of 3D depth images for precise evaluation of zone edges using ToF sensors.
Zone State Hysteresis	PL d	—	Application of hysteresis to zone state transitions to prevent flickering of safety reactions due to sensor noise or boundary oscillations.

INTEGRITY_GAP

FUNCTION	DEMAND	LAYER	FINDING
Worst-Case Zone	PL d	safes_monitor	requires PL d, but is implemented via

FUNCTION	DEMAND	LAYER	FINDING
Protective Stop (STO) safetyfn:falke:08d382690f	PL d	safe_monitor	requires PL d, but is implemented via ['component:safety_logic'] (performance layer without safety capability); independent safe monitor (target architecture) is missing
Zone Edge Depth Evaluation safetyfn:falke:314556a533	PL d	sensor_layer	requires PL d, but has no implementation chain (SYS.2→SWE.1→component) — function not implemented
Robust Long-Range Detection safetyfn:falke:3776e61637	SIL 2	sensor_layer	requires SIL 2, but has no implementation chain (SYS.2→SWE.1→component) — function not implemented
Dynamic Hazard Radius Calculation safetyfn:falke:3ac30f5076	PL d	safe_monitor	requires PL d, but is implemented via ['component:ssm_node'] (performance layer without safety capability); independent safe monitor (target architecture) is missing
Primary Spatial Detection safetyfn:falke:4e907cc618	PL e	sensor_layer	requires PL e, but has no implementation chain (SYS.2→SWE.1→component) — function not implemented
Static Object Masking safetyfn:falke:6bce378db1	PL d	safe_monitor	requires PL d, but is implemented via ['component:lidar_sensor_node'] (performance layer without safety capability); independent safe monitor (target architecture) is missing
Zone State Hysteresis safetyfn:falke:ae1de4b226	PL d	safe_monitor	requires PL d, but is implemented via ['component:ssm_probe'] (performance layer without safety capability); independent safe monitor (target architecture) is missing
Speed Reduction safetyfn:falke:b033997fe6	PL d	safe_monitor	requires PL d, but is implemented via ['component:safety_logic'] (performance layer without safety capability); independent safe monitor (target architecture) is missing
Early Detection Monitoring safetyfn:falke:d968811a16	PL d	safe_monitor	requires PL d, but has no implementation chain (SYS.2→SWE.1→component) — function not implemented

9. Architecture (SYS.3) and System Requirements (SYS.2)

Not a screenshot copy of the interactive view — the notified body reads the components and statements. Graph layout is not evidence. The diagrams from the EA model (layered layout, deterministically generated) are in Appendix A and B.

COMPONENT	TYPE	LAYER	RATING	ROLE
ABB IRB 6700 (armA)	robot	plant	—	
ABB IRB 6700 (armB)	robot	plant	—	
HW-Bridge (Sensor-Gateway)	gateway	sensor_layer	—	raw sensor data, TCP :9999
LD-360 (LiDAR)	sensor	sensor_layer	PL e	360°-Raumüberwachung, Primärdetektion
ROS 2 Performance-Stack	software_stack	performance_layer	—	fusion + zones + speed control (nicht safe)
RX-240 (Radar)	sensor	sensor_layer	SIL 2	Weitbereich, robust gegen Staub/Licht
Safety Monitor (Target Architecture)	controller	safe_monitor	—	STO/SS1 autark (Classic/TDA4/STM32, simuliert)
TF-320 (ToF)	sensor	sensor_layer	PL d	3D-Tiefenbild der Zonenränder
US-80 (USS)	sensor	sensor_layer	—	Nahbereich an den Zugängen
Worker	human	environment	—	trigger

SYS.2 system requirements from the project graph (shall-statements).

SYS.2 REQUIREMENT	CATEGORY	PL / SIL	STATUS	STATEMENT
Dynamic Hazard Radius Calculation sysreq:falke:3ac30f5076	zone_model	PL d	proposed	The system shall dynamically calculate the hazard radius Rh using the formula $R_h = reach + M_ARM + v_nom * (T1+T2)$ at runtime based on current robot reach and nominal TCP speed.
HW Bridge Raw Data Only sysreq:falke:16627a378a	layer_separation	—	proposed	The sensor_layer implementation (hwbridge) shall deliver only raw sensor data over TCP port 9999, without performing safety logic or fusion.
Independent Safe Monitor Architecture sysreq:falke:45e16a0a4a	layer_separation	PL d	proposed	The safe_monitor shall be implemented on hardware or software distinct from the performance_layer (ROS 2) to ensure functional independence and safety integrity.

SYS.2 REQUIREMENT	CATEGORY	PL / SIL	STATUS	STATEMENT
LiDAR Primary Detection Role sysreq:falke:20d07d0b9c	sensor_architecture	PL e	proposed	The sensor_layer shall utilize the LD-360 LiDAR (PL e) as the primary detection source for 360° spatial monitoring.
Patrouille Scenario Stop Events sysreq:falke:44be737d1a	scenario_coverage	PL d	proposed	The system shall correctly trigger 3 stop events during the 'Patrouille' scenario where a worker walks from Arm A to Arm B to VI-7.
Performance Layer Non-Safety Role sysreq:falke:f5c35d4e6c	layer_separation	PL d	proposed	The performance_layer (ROS 2) shall perform sensor fusion and zone evaluation for functionality only, and shall not be relied upon as the sole safety mechanism.
R1 Zone Stop Reaction sysreq:falke:bc88fc894a	reaction	PL d	proposed	The system shall initiate a Protective Stop (STO) for the associated robot arm when a human enters the R1 zone defined by the formula $R_h + C$.
R2 Zone Speed Reduction sysreq:falke:4048095481	reaction	PL d	proposed	The system shall reduce the robot speed when a human enters the R2 zone defined by the formula $R1 + K_HAND * (T1+T2)$.
R3 Zone Early Detection sysreq:falke:6d856c08b5	reaction	PL d	proposed	The system shall activate early detection monitoring when a human enters the R3 zone defined by the formula $R2 + K_WALK * (T1+T2)$.
Radar Robustness Detection sysreq:falke:10f6311162	sensor_architecture	SIL 2	proposed	The sensor_layer shall utilize the RX-240 Radar (SIL 2) for long-range detection robust against dust and light interference.
Safe Monitor Autonomous STO Trigger sysreq:falke:72e28be838	safety_architecture	PL d	proposed	The safe_monitor layer shall autonomously trigger a Safe Torque Off (STO) signal when the worst-case zone state is 'stop' (R1), independent of the performance_layer.
Static Object Masking sysreq:falke:6bce378db1	detection	PL d	proposed	The system shall mask known static objects (e.g., GT-75) within the protective field using an environment map to prevent false positive safety triggers.
System Reaction Time Parameters sysreq:falke:7cd5da973b	zone_model	PL d	proposed	The zone distance calculations shall use system reaction time parameters $T1 = 0.08\text{ s}$ and $T2 = 0.4\text{ s}$.

SYS.2 REQUIREMENT	CATEGORY	PL / SIL	STATUS	STATEMENT
ToF Zone Edge Depth sysreq:falke:74b2badd 9a	sensor_architecture	PL d	proposed	The sensor_layer shall utilize the TF-320 ToF sensor (PL d) to provide 3D depth images for precise zone edge evaluation.
USS Access Proximity Detection sysreq:falke:b7595674 74	sensor_architecture	—	proposed	The sensor_layer shall utilize the US-80 USS sensor for near-field detection at cell access points.
Worker Walking Speed Parameter sysreq:falke:b75c8cdd a9	human_interaction	PL d	proposed	The zone calculation shall use a human walking speed of 1.2 m/s for the worker role in dynamic distance calculations.
Worst-Case Zone Aggregation sysreq:falke:088e43e8 f2	zone_model	PL d	proposed	The system shall determine the overall system reaction based on the worst-case zone state across all monitored entities (ARM A, ARM B, VI-7).
Zone State Hysteresis sysreq:falke:ae1de4b2 26	zone_model	PL d	proposed	The system shall apply hysteresis to zone state transitions to prevent flickering of safety reactions due to sensor noise or boundary oscillations.

10. Requirement Gaps (Excerpt)

Complete lists are in the gap chain (JSON). Showing the first 18 per type — not the full requirement catalog.

NORM_GAP — in-scope without SYS.2 (378)

ID / NAME	NORM
Perform risk assessment per ISO 12100 REQ-10218-2-4.1-01	ISO102182
Include high-energy movement in risk assessment REQ-10218-2-4.2-01	ISO102182
Include unpredictable movement in risk assessment REQ-10218-2-4.2-02	ISO102182
Include overlapping operating space in risk assessment REQ-10218-2-4.2-03	ISO102182
Include diverse tasks in risk assessment REQ-10218-2-4.2-05	ISO102182
Include operator travel paths in risk assessment REQ-10218-2-4.2-06	ISO102182
Include operator presence near powered robot in risk assessment REQ-10218-2-4.3.1-01	ISO102182
Include safety functions in risk assessment REQ-10218-2-4.3.1-02	ISO102182
Include contact potential in risk assessment REQ-10218-2-4.3.1-03	ISO102182
Design per ISO 12100 for non-significant hazards REQ-10218-2-5.1-01	ISO102182
Robots conform with ISO 10218-1:2025 REQ-10218-2-5.1-02	ISO102182
Prevent robot entry into occupied hazard zone REQ-10218-2-5.12.2.1-07	ISO102182
Detection zone includes hazard zone REQ-10218-2-5.12.2.3-01	ISO102182
SPE initiates protective stop REQ-10218-2-5.12.2.3-02	ISO102182
Protect operators from moving parts REQ-10218-2-5.14.1-01	ISO102182
Protect or stop before contact REQ-10218-2-5.14.1-02	ISO102182
Address quasi-static and transient hazards REQ-10218-2-5.14.1-03	ISO102182
All safeguards active during auto operation REQ-10218-2-5.14.1-06	ISO102182

182 more entries in the JSON appendix (gap chain).

SYS_GAP — SYS.2 without SWE.1 (9)

ID / NAME
Radar Robustness Detection sysreq: falke:10f6311162
LiDAR Primary Detection Role sysreq: falke:20d07d0b9c
Patrouille Scenario Stop Events sysreq: falke:44be737d1a
Independent Safe Monitor Architecture sysreq: falke:45e16a0a4a
R3 Zone Early Detection sysreq: falke:6d856c08b5
ToF Zone Edge Depth sysreq: falke:74b2badd9a
System Reaction Time Parameters sysreq: falke:7cd5da973b
USS Access Proximity Detection sysreq: falke:b759567474
Worker Walking Speed Parameter sysreq: falke:b75c8cdda9

TEST_GAP — SYS.2 untested

ID / NAME
Worst-Case Zone Aggregation sysreq: falke:088e43e8f2
Radar Robustness Detection sysreq: falke:10f6311162
HW Bridge Raw Data Only sysreq: falke:16627a378a
LiDAR Primary Detection Role sysreq: falke:20d07d0b9c
Dynamic Hazard Radius Calculation sysreq: falke:3ac30f5076
R2 Zone Speed Reduction sysreq: falke:4048095481
Patrouille Scenario Stop Events sysreq: falke:44be737d1a
Independent Safe Monitor Architecture sysreq: falke:45e16a0a4a
Static Object Masking sysreq: falke:6bce378db1

ID / NAME
R3 Zone Early Detection sysreq:falke:6d856c08b5
Safe Monitor Autonomous STO Trigger sysreq:falke:72e28be838
ToF Zone Edge Depth sysreq:falke:74b2badd9a
System Reaction Time Parameters sysreq:falke:7cd5da973b
Zone State Hysteresis sysreq:falke:ae1de4b226
USS Access Proximity Detection sysreq:falke:b759567474
Worker Walking Speed Parameter sysreq:falke:b75c8cdda9
R1 Zone Stop Reaction sysreq:falke:bc88fc894a
Performance Layer Non-Safety Role sysreq:falke:f5c35d4e6c

TEST_GAP — SWE.1 untested

ID / NAME
Publish point cloud data req_swe1:lidar_sensor_node:8ed7702bd8
Load entities from JSON file req_swe1:lidar_sensor_node:902fef4e6b
Update entity positions from entity update req_swe1:lidar_sensor_node:a2bf784002
Update sensor origin from entity update req_swe1:lidar_sensor_node:b81e35a0fd
Update sensor origin from robot pose req_swe1:lidar_sensor_node:e43cf7b093
Publish LiDAR scan data req_swe1:lidar_sensor_node:e62372d6e9
Trigger sequences via ROS topic req_swe1:mock_data_publisher:4c276be56c
Stop active sequence on request req_swe1:mock_data_publisher:55dc9a8c2c
Publish safety zone status messages req_swe1:mock_data_publisher:5d1ed57ae2
Publish human detection messages req_swe1:mock_data_publisher:6e2cc34675

ID / NAME
Execute sequence steps at interval req_swe1:mock_data_publisher:d2e74125e7
Load sequences from YAML config req_swe1:mock_data_publisher:fa97e1c55b
Reject goals during emergency stop req_swe1:neurapy_mock:64bcb45f34
Publish periodic movement feedback req_swe1:neurapy_mock:70b8668fac
Report successful action completion req_swe1:neurapy_mock:77857dc09a
Accept cancellation requests req_swe1:neurapy_mock:9c518082d9
Publish robot pose updates req_swe1:neurapy_mock:ad490da9fe
Scale execution time by speed req_swe1:neurapy_mock:c3d867e06a

48 more entries in the JSON appendix (gap chain).

OVER_FILL — SWE.1 without SYS.2 (57)

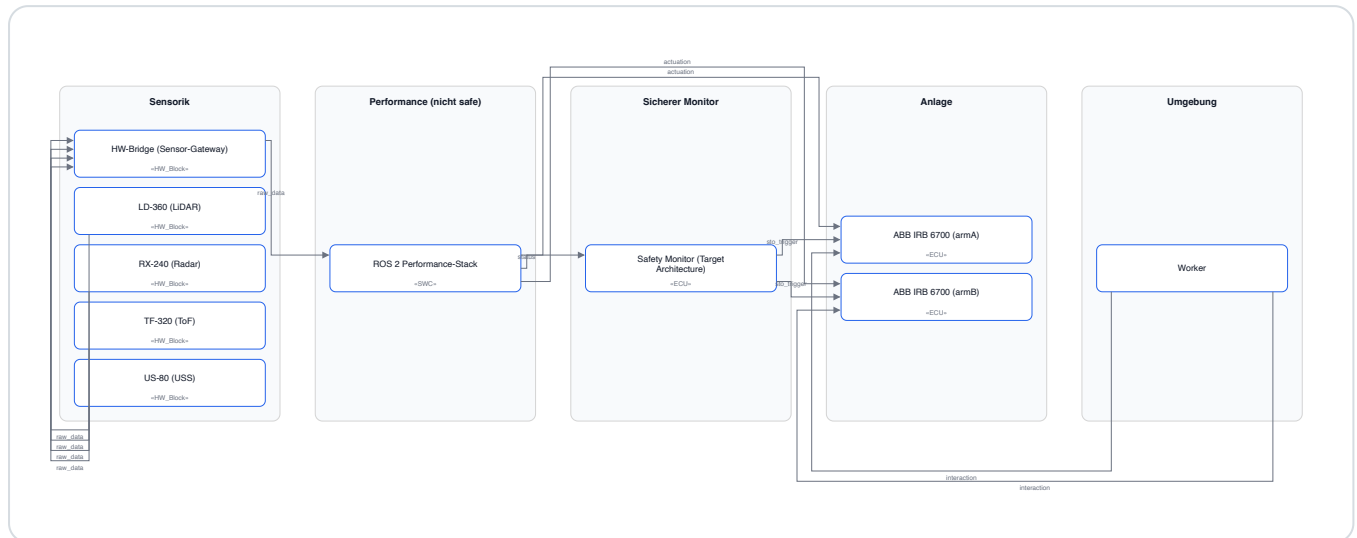
ID / NAME	COMPONENT
Publish point cloud data req_swe1:lidar_sensor_node:8ed7702bd8	lidar_sensor_node
Update entity positions from entity update req_swe1:lidar_sensor_node:a2bf784002	lidar_sensor_node
Update sensor origin from entity update req_swe1:lidar_sensor_node:b81e35a0fd	lidar_sensor_node
Update sensor origin from robot pose req_swe1:lidar_sensor_node:e43cf7b093	lidar_sensor_node
Publish LiDAR scan data req_swe1:lidar_sensor_node:e62372d6e9	lidar_sensor_node
Trigger sequences via ROS topic req_swe1:mock_data_publisher:4c276be56c	mock_data_publisher
Stop active sequence on request req_swe1:mock_data_publisher:55dc9a8c2c	mock_data_publisher
Publish safety zone status messages req_swe1:mock_data_publisher:5d1ed57ae2	mock_data_publisher
Publish human detection messages req_swe1:mock_data_publisher:6e2cc34675	mock_data_publisher
Execute sequence steps at interval req_swe1:mock_data_publisher:d2e74125e7	mock_data_publisher

ID / NAME	COMPONENT
Load sequences from YAML config req_swe1:mock_data_publisher:fa97e1c55b	mock_data_publisher
Reject goals during emergency stop req_swe1:neurapy_mock:64bcb45f34	neurapy_mock
Publish periodic movement feedback req_swe1:neurapy_mock:70b8668fac	neurapy_mock
Report successful action completion req_swe1:neurapy_mock:77857dc09a	neurapy_mock
Accept cancellation requests req_swe1:neurapy_mock:9c518082d9	neurapy_mock
Publish robot pose updates req_swe1:neurapy_mock:ad490da9fe	neurapy_mock
Scale execution time by speed req_swe1:neurapy_mock:c3d867e06a	neurapy_mock
Detection History Buffering req_swe1:omnisensor_sim:48c3ed76db	omnisensor_sim

39 more entries in the JSON appendix (gap chain).

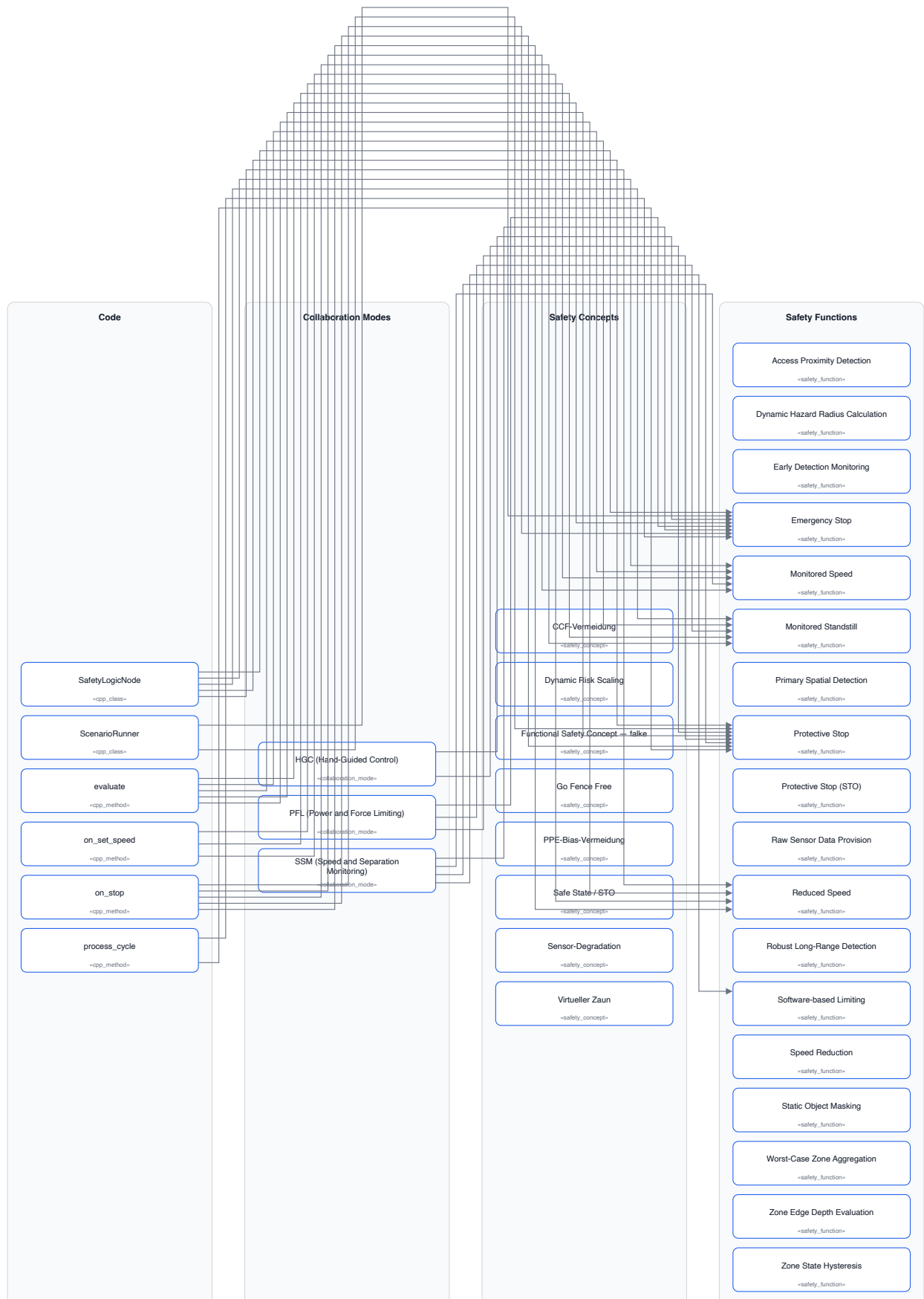
Appendix A — System Architecture SYS.3 (from EA model)

Deterministically generated from the project graph (ea_generator) — layered layout, no manual post-processing.



Appendix B — SW Safety Concept (from EA model)

Deterministically generated from the project graph (ea_generator) — layered layout, no manual post-processing.

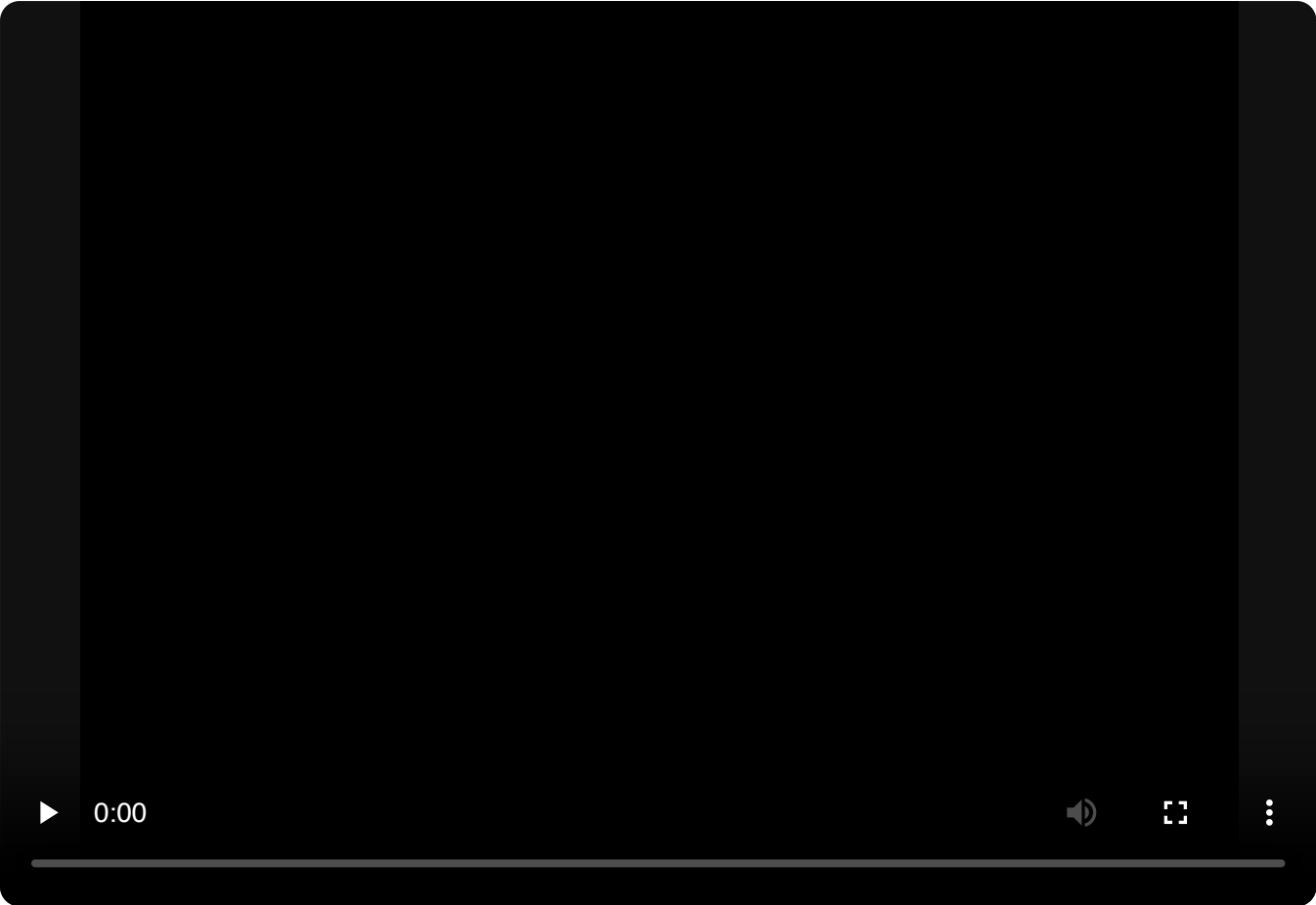


Appendix C — SIL test runs

Sealed SIL protocols from the local results store. The cover names this appendix as evidence: HTML/ZIP remains available from the API; this document carries the run table, step images, and the featured recording as a sibling file (not inlined).

Featured protocol: run **19** · falke:Patrouille (Template) · status completed · seal

b17880921b434bb17c2efe9356dbae994a2d74697f06c6200bcc0982122d353f. Newer runs with a roof-only camera (close-up of the hall ceiling) are listed below but not used as stills or video here.

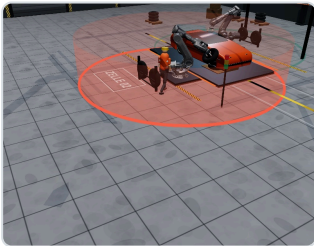


Recording evidence-run-19.webm · 62018 kB — sibling of this HTML (also in the ZIP export).

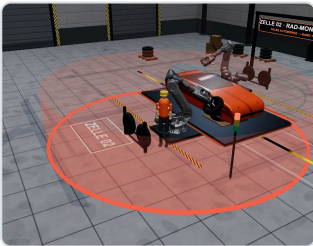
Step images (featured run)



t=0.0 · pass



t=5.19 · fail



t=6.39 · pass



t=10.93 · fail

RUN	SCENARIO	STARTED	STATUS	P/F/N	SEAL	VIDEO	FAIL EXPLANATION
21	falke:Patrouille (Template)	2026-08-06 13:51 UTC	abort...	12/7/19	a38dda3ff614...	66619...	t=16.37: zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)
20	falke:Patrouille (Template)	2026-08-06 13:50 UTC	abort...	7/3/10	705f5a100a43...	3407...	t=16.37: zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)

RUN	SCENARIO	STARTED	STATUS	P/F/N	SEAL	VIDEO	FAIL EXPLANATION
19 · ...	falke:Patrouille (Template)	2026-08-05 23:04 UTC	comp...	12/7/19	b17880 921b4 3...	6201...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
18	falke:Patrouille (Template)	2026-08-05 23:03 UTC	abort...	9/7/16	c5cef5 19dcf 2...	5565...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
17	falke:Patrouille (Template)	2026-08-05 22:59 UTC	comp...	14/7/21	2f1f81 f279b 1...	78641...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
16	falke:Szenario 2	2026-08-05 22:24 UTC	comp...	0/1/1	e52699 ea1f8 8...	—	t=0.0: zone expected ["CLEAR","CLEAR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — Waypoint zone/speed match (CamFollow / WP4 Smoke)
15	falke:Patrouille (Template)	2026-08-05 22:23 UTC	abort...	11/7/18	db3e71 a17ee 4...	—	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
14	falke:Szenario 2	2026-08-05 14:22 UTC	comp...	1/0/1	—	—	—
13	falke:Patrouille (Template)	2026-08-05 14:04 UTC	abort...	4/4/8	270c81 059ad 7...	2336...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)

RUN	SCENARIO	STARTED	STATUS	P/F/N	SEAL	VIDEO	FAIL EXPLANATION
12	falke:Patrouille (Template)	2026-08-05 13:14 UTC	abort...	6/6/12	bb6e74 8066b 8...	4170...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
11	falke:Patrouille (Template)	2026-08-05 13:12 UTC	abort...	7/7/14	dcc003 55a77 d...	4538...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
10	falke:Patrouille (Template)	2026-08-05 12:45 UTC	abort...	11/7/18	cab152 556c2 b...	—	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
9	falke:Patrouille (Template)	2026-08-05 12:42 UTC	abort...	9/7/16	2cbbf8 20dc5 b...	5440...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
8	falke:Patrouille (Template)	2026-08-05 12:33 UTC	abort...	1/1/2	964751 5b49e 7...	5508 ...	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
7	falke:Patrouille (Template)	2026-08-05 12:21 UTC	abort...	1/1/2	bf3ee7 7b502 2...	—	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
6	falke:Patrouille (Template)	2026-08-05 12:14 UTC	abort...	1/0/1	—	—	—

RUN	SCENARIO	STARTED	STATUS	P/F/N	SEAL	VIDEO	FAIL EXPLANATION
5	falke:Patrouille (Template)	2026-08-05 10:56 UTC	abort...	1/1/2	9ab4db ac49f d...	—	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
4	falke:Patrouille (Template)	2026-08-05 10:36 UTC	abort...	4/4/8	3e0551 17faa b...	—	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
3	falke:Patrouille (Template)	2026-08-05 10:35 UTC	abort...	1/0/1	—	—	—
2	falke:Patrouille (Template)	2026-08-05 10:35 UTC	abort...	3/3/6	ef9979 78ab7 3...	—	t=5.19: zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)
1	falke:Patrouille (Template)	2026-08-04 23:21 UTC	abort...	1/1/2	426577 e6a6b e...	—	1 failed step(s)

Appendix D — Fail-case details

Each row is a recorded waypoint that failed the zone/speed criterion. Screenshots stay in this HTML when present; the ZIP run JSON omits images. Video of the featured run is the sibling `evidence-run-*.mp4`.

RUN	SCENARIO	T	CAUSE / REQUIREMENT	STILL
21	Patrouille (Template)	t=16.37	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
21	Patrouille (Template)	t=28.31	zone expected ["CLEAR","MONITOR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, MONITOR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
21	Patrouille (Template)	t=31.95	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["CLEAR","MONITOR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [CLEAR, MONITOR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
21	Patrouille (Template)	t=40.57	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["WARN","CLEAR","CLEAR"]; SSM speed expected 100%, actual 25%; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [WARN, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet 25% — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
21	Patrouille (Template)	t=47.76	zone expected ["CLEAR","CLEAR","MONITOR"], actual ["CLEAR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, MONITOR] ≠ beobachtet [CLEAR, CLEAR, CLEAR] — R3 early detection (ISO 13855 SSM)	yes
21	Patrouille (Template)	t=49.16	zone expected ["CLEAR","CLEAR","STOP"], actual ["CLEAR","CLEAR","CLEAR"]; SSM speed expected STOP, actual 100%; Zonen erwartet [CLEAR, CLEAR, STOP] ≠ beobachtet [CLEAR, CLEAR, CLEAR] · SSM erwartet STOP ≠ beobachtet 100% — R1 / protective stop (ISO 13855 SSM, SYS.2 R1 Zone Stop)	yes
21	Patrouille (Template)	t=54.9	zone expected ["CLEAR","CLEAR","MONITOR"], actual ["CLEAR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, MONITOR] ≠ beobachtet [CLEAR, CLEAR, CLEAR] — R3 early detection (ISO 13855 SSM)	yes

RUN	SCENARIO	T	CAUSE / REQUIREMENT	STILL
20	Patrouille (Template)	t=16.37	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
20	Patrouille (Template)	t=28.31	zone expected ["CLEAR","MONITOR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, MONITOR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
20	Patrouille (Template)	t=31.95	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["CLEAR","MONITOR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [CLEAR, MONITOR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
19	Patrouille (Template)	t=5.19	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
19	Patrouille (Template)	t=10.93	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
19	Patrouille (Template)	t=14.65	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["WARN","CLEAR","CLEAR"]; SSM speed expected 100%, actual 25%; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [WARN, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet 25% — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
19	Patrouille (Template)	t=26.59	zone expected ["CLEAR","MONITOR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, MONITOR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
19	Patrouille (Template)	t=34.52	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes

RUN	SCENARIO	T	CAUSE / REQUIREMENT	STILL
19	Patrouille (Template)	t=38.85	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["WARN","CLEAR","CLEAR"]; SSM speed expected 100%, actual 25%; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [WARN, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet 25% — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
19	Patrouille (Template)	t=46.03	zone expected ["CLEAR","CLEAR","MONITOR"], actual ["CLEAR","CLEAR","WARN"]; SSM speed expected 100%, actual 25%; Zonen erwartet [CLEAR, CLEAR, MONITOR] ≠ beobachtet [CLEAR, CLEAR, WARN] · SSM erwartet 100% ≠ beobachtet 25% — R3 early detection (ISO 13855 SSM)	yes
18	Patrouille (Template)	t=5.19	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
18	Patrouille (Template)	t=10.93	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["WARN","CLEAR","CLEAR"]; SSM speed expected 100%, actual 25%; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [WARN, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet 25% — R3 early detection (ISO 13855 SSM)	yes
18	Patrouille (Template)	t=14.65	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
18	Patrouille (Template)	t=26.59	zone expected ["CLEAR","MONITOR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, MONITOR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
18	Patrouille (Template)	t=34.52	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
18	Patrouille (Template)	t=38.85	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes

RUN	SCENARIO	T	CAUSE / REQUIREMENT	STILL
18	Patrouille (Template)	t=46.03	zone expected ["CLEAR","CLEAR","MONITOR"], actual ["CLEAR","CLEAR","WARN"]; SSM speed expected 100%, actual 25%; Zonen erwartet [CLEAR, CLEAR, MONITOR] ≠ beobachtet [CLEAR, CLEAR, WARN] · SSM erwartet 100% ≠ beobachtet 25% — R3 early detection (ISO 13855 SSM)	yes
17	Patrouille (Template)	t=5.19	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
17	Patrouille (Template)	t=10.93	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["WARN","CLEAR","CLEAR"]; SSM speed expected 100%, actual 25%; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [WARN, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet 25% — R3 early detection (ISO 13855 SSM)	yes
17	Patrouille (Template)	t=14.65	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
17	Patrouille (Template)	t=26.59	zone expected ["CLEAR","MONITOR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, MONITOR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
17	Patrouille (Template)	t=34.52	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
17	Patrouille (Template)	t=38.85	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
17	Patrouille (Template)	t=46.03	zone expected ["CLEAR","CLEAR","MONITOR"], actual ["CLEAR","CLEAR","WARN"]; SSM speed expected 100%, actual 25%; Zonen erwartet [CLEAR, CLEAR, MONITOR] ≠ beobachtet [CLEAR, CLEAR, WARN] · SSM erwartet 100% ≠ beobachtet 25% — R3 early detection (ISO 13855 SSM)	yes

RUN	SCENARIO	T	CAUSE / REQUIREMENT	STILL
16	Szenario 2	t=0.0	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
15	Patrouille (Template)	t=5.19	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
15	Patrouille (Template)	t=10.93	zone expected ["MONITOR","CLEAR","CLEAR"], actual ["STOP","CLEAR","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [MONITOR, CLEAR, CLEAR] ≠ beobachtet [STOP, CLEAR, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes
15	Patrouille (Template)	t=14.65	zone expected ["CLEAR","CLEAR","CLEAR"], actual ["MONITOR","CLEAR","CLEAR"]; Zonen erwartet [CLEAR, CLEAR, CLEAR] ≠ beobachtet [MONITOR, CLEAR, CLEAR] — Waypoint zone/speed match (CamFollow / WP4 Smoke)	yes
15	Patrouille (Template)	t=26.59	zone expected ["CLEAR","MONITOR","CLEAR"], actual ["CLEAR","STOP","CLEAR"]; SSM speed expected 100%, actual STOP; Zonen erwartet [CLEAR, MONITOR, CLEAR] ≠ beobachtet [CLEAR, STOP, CLEAR] · SSM erwartet 100% ≠ beobachtet STOP — R3 early detection (ISO 13855 SSM)	yes

11. Use with the Notified Body

1. This HTML (print to PDF) is the readable overview.
2. `evidence-report.json` — machine-readable seal payload (same hash as §4).
3. `gap-chain.json` — NORM_GAP / SYS_GAP / TEST_GAP / INTEGRITY_GAP item lists.
4. Appendix C — sealed SIL runs (table, fail explanation, images, featured video).
5. Appendix D — fail-case details (criterion and requirement hint per waypoint).