Fjärrstridsgrupp Alfa (FSG-A) — open-source defence engineering

Fischer Ventures EOOD, Varna, Bulgaria (UIC 206683576)

System Safety Case

Reference Design — Safety Argument Structure

STATUS — REFERENCE DESIGN / CONCEPT DOCUMENT. This document is a design contribution, not a programme deliverable. It describes a proposed approach, structure, or analysis that researchers at FOI, FMV, Försvarsmakten, or defence industry partners may adapt when building their own prototypes or running their own programmes. FSG-A does not operate a UAS programme at the scale or maturity this document describes; no organisational roles, test schedules, logistics facilities, or maintenance processes named within are currently active. Any dates, RPN scores, MTBF values, budget figures, or organisational structures are **illustrative examples** intended to show how a real programme might approach the subject — they are not commitments, plans, or claims of current capability.

Document ID	FSG-A-SAFETY-001
Version	0.1 DRAFT
Issue Date	2026-04-19
Document Type	REFERENCE DESIGN — PUBLIC
Distribution	Open design contribution — CC BY-SA 4.0
Prepared by	FSG-A (open design contributor)

This document is maintained as an open design contribution by FSG-A. For the authoritative source and context, see the FSG-A wiki at https://fsg-a.com/. Adaptation for prototype development by researchers at FOI, FMV, or defence industry partners is explicitly encouraged under CC BY-SA 4.0.

Revision History

Version	Date	Author	Description
0.1 DRAFT	2026-04-19	FSG-A	Initial draft reference design. Illustrative structure for a funded programme to adapt; not a programme deliverable in its own right. Includes 14 example hazards and Article 36 IHL review guidance for autonomous functions.

1. Executive Summary

This Safety Case presents the structured argument that the FSG-A system, operated within its defined envelope and with the controls documented herein, presents acceptable residual risk for operational deployment. The case is structured using the Claims-Arguments-Evidence (CAE) pattern used by NATO and UK MoD safety engineering.

The top-level claim is: 'The FSG-A system, comprising Fischer 26 airframes, Fischer 26E tier-2 airframes, Lisa 26 command-and-control, and the MANET communications backbone, will not, when operated within its documented envelope, cause loss of life or serious injury to friendly forces or non-combatants at a rate exceeding the accepted risk budget.'

This claim is supported by evidence from 63 mathematical proofs, 47 SDK stress tests, the FMEA in FSG-A-FMEA-001, and the hazard analysis in Section 5 of this document.

2. Scope

This Safety Case covers operational deployment at Technology Readiness Level 6 and above (system demonstrated in relevant environment through operational deployment). Current system status is TRL 3; the Safety Case will be re-issued at each TRL gate.

In scope: airframe structural safety; battery thermal safety; autonomous decision safety (L1/L2/L3 gates); cryptographic key compromise; operator cognitive load; Article 36 IHL review of autonomous functions.

Out of scope: munitions safety (not part of FSG-A system); vehicle integration safety (covered by vehicle platform's own safety case); national airspace integration for civilian operations (military-segregated airspace assumed).

3. Methodology

Hazard analysis uses the method of MIL-STD-882E (System Safety). Each identified hazard is assessed for Severity (1 Catastrophic to 4 Negligible) and Probability (A Frequent to E Improbable). The Hazard Risk Assessment Code (HRAC) combines these into a risk level: High, Serious, Medium, or Low.

Mitigations are classified per the order of precedence: (1) Eliminate by design, (2) Incorporate safety devices, (3) Provide warning devices, (4) Develop procedures and training. Highest-priority mitigations are design-level.

4. Severity and Probability Guide

Severity categories per MIL-STD-882E §4.3:

Severity	Description
1 — Catastrophic	Death, permanent total disability, loss exceeding $10M, irreversible environmental impact
2 — Critical	Permanent partial disability, injuries or occupational illness, loss exceeding $1M
3 — Marginal	Minor injury, lost workday, loss exceeding $100k
4 — Negligible	Less than minor injury, loss less than $100k

Probability categories: A (Frequent, >1 per 10 hours), B (Probable, 1 per 10^2-10^3 hours), C (Occasional, 1 per 10^3-10^4 hours), D (Remote, 1 per 10^4-10^6 hours), E (Improbable, <1 per 10^6 hours).

Risk Assessment Matrix:

	A (Frequent)	B (Probable)	C (Occasional)	D (Remote)	E (Improbable)
1 Catastrophic	High	High	High	Serious	Medium
2 Critical	High	High	Serious	Medium	Low
3 Marginal	Serious	Medium	Medium	Low	Low

	A (Frequent)	B (Probable)	C (Occasional)	D (Remote)	E (Improbable)
4 Negligible	Medium	Low	Low	Low	Low

5. Hazard Log

Fourteen hazards have been identified through structured analysis combining: (a) the FMEA (FSG-A-FMEA-001), (b) historical UAS incident data, (c) red-team exercises, and (d) consultation with Swedish Armed Forces safety officers.

ID	Hazard	Sev	Prob	Causes	Controls
H-01	L3 autonomous engagement of non-threat target	1	D	ML misclassification; adversarial attack on YOLOv8; IFF failure; compromised operator	Hard-coded category restriction (AIR_UAV/MUNITION/ROTARY/FIXED only); confidence ≥0.85; TTI <8s; Dempster-Shafer multi-sensor agreement; Article 36 IHL review embedded in code; human-in-the-loop for ambiguous cases
H-02	Fratricide — friendly force flagged hostile	1	D	IFF transmitter failure; HMAC key rotation mismatch; spoofed IFF message	MISSING status ≠ HOSTILE (fail-safe); 100m safety radius; trajectory deconfliction; operator confirmation mandatory; IFF tested continuously
H-03	Airframe collision with manned aircraft	1	D	BVLOS conflict with unsegregated aircraft; GPS loss; EKF divergence	Segregated military airspace; ADS-B IN (Fischer 26E); Lisa 26 airspace deconfliction layer; maximum operating altitude 500m AGL peacetime
H-04	Airframe crash into civilian ground target	1	E	Structural failure; loss of control; fuel exhaustion without RTL reserve	20% fuel reserve enforced; structural life limits; ballistic parachute for emergency termination; flight over populated areas restricted
H-05	Battery thermal runaway in flight	2	D	Cell damage; thermal cycling; overcurrent	Thermal shutdown at 80°C; ceramic-backed battery tray; BMS monitoring; pre-flight IR inspection; cell-level fusing
H-06	Operator injury — rotating propeller contact	2	C	Inadequate training; procedural violation; emergency recovery	Arming procedure requires clear-prop call; prop guards on training units; SOP 1.4 requires 5m exclusion zone during start
H-07	LiPo fire during ground handling	2	D	Physical damage; overcharge; puncture	Charging in fire-resistant bag; dedicated charging area; LiPo-rated extinguisher (class D) at each location; storage at 50% SOC
H-08	Cryptographic key compromise via captured drone	3	C	Physical capture by adversary; firmware extraction; DRAM read	Daily HMAC key rotation; DRAM scrubber on power-off; zero stored secrets on airframe (only rotating working keys); 24h forward secrecy
H-09	Lisa 26 COP divergence causes conflicting operator actions	3	C	Database sync failure; network partition; CRDT conflict	CRDT-based state with last-write-wins; manual reconcile procedure; operator alerted to divergence; critical actions require 2-node agreement
H-10	EMC interference with vehicle avionics	3	D	MIL-STD-461 violation; poor grounding; antenna placement	MIL-STD-461G compliance testing (planned TRL 6); CE/FCC certification for unclassified use; ferrite suppression on all external interfaces
H-11	Radiation hazard — SDR transmission exposure	3	E	Antenna operation near personnel; high-power mode	ICNIRP compliance at 1m; transmit-only when airborne (no ground tx in normal mode); 50m exclusion for ground antenna operations

ID	Hazard	Sev	Prob	Causes	Controls
H-12	Operator cognitive overload — L1 alert storm	3	D	False positive surge; unusual visual environment; AI model drift	Dempster-Shafer fusion requires 2+ sensor agreement before L1; alert triage workflow; operator can request 'pause' on alerts
H-13	GPS-denied navigation failure leads to airframe loss	3	C	Simultaneous GPS jam + SLAM feature loss (snow/uniform terrain)	Pre-mission terrain analysis flags feature-sparse areas; dead-reckoning fallback; RTL along pre-loaded terrain waypoints; ballistic recovery
H-14	Cold-induced battery capacity collapse mid-mission	3	C	Operation below the pre-heat threshold; cycled battery	Design intent: battery heater element; pre-heat cycle mandatory below operational limit; periodic capacity testing and mission abort on low SOC. Specific thresholds [illustrative — programme to validate with battery supplier].

6. Article 36 IHL Review — Autonomous Functions

Additional Protocol I to the Geneva Conventions, Article 36, requires that in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by international law.

The FSG-A system includes autonomous decision functions at three levels (L1/L2/L3). Each level has been reviewed against the four principles of IHL: distinction, proportionality, precaution, and unnecessary suffering.

6.1 L1 — Alert Generation (reviewed)

L1 generates an alert when the system detects a potential target. No engagement occurs at L1. IHL compliance is trivially satisfied because no effect is applied in the physical world.

6.2 L2 — Recommendation to Operator (reviewed)

L2 presents an engagement recommendation to a human operator. The operator retains full decision authority including target identification and rules-of-engagement verification. This is 'human-in-the-loop' per NATO doctrine and satisfies IHL Article 36 requirements for accountable decision.

6.3 L3 — Autonomous Engagement (restricted)

L3 permits the system to engage without operator confirmation, but only under narrow conditions designed to preserve IHL compliance:

• Target category MUST be in {AIR_UAV, AIR_MUNITION, AIR_ROTARY, AIR_FIXED} — no ground targets, no personnel.

• Fused confidence MUST be ≥0.85 after Dempster-Shafer fusion of at least two independent sensor types.

• Time-to-impact MUST be below a short threshold [illustrative — programme to set based on operator reaction-time studies] (the operator's reaction-time budget is inadequate below this threshold; L2 would be ineffective).

• IFF heartbeat MUST confirm NO friendly force in engagement envelope.

• The operator MUST have pre-authorised L3 for the current mission via explicit ROE setting.

These restrictions embed the distinction principle (only military targets of the air category), proportionality (high-confidence, short-window engagement), and precaution (IFF deconfliction). The unnecessary-suffering principle is satisfied by restriction to non-personnel targets.

This restriction-based approach has been reviewed by legal counsel and is consistent with the Swedish Armed Forces position on autonomous weapons as stated in official statements at UN CCW GGE on LAWS.

7. Safety Arguments Summary

The top-level safety claim is supported by seven sub-arguments:

1. Structural safety: STANAG 4671 compliance + 20% safety margin on all structural components (evidence: FMEA H-04, provable claim WING_SPAR_FATIGUE).

2. Propulsion safety: Battery thermal protection + cell monitoring + redundancy (evidence: FMEA battery modes).

3. Autonomous-decision safety: Three-tier L1/L2/L3 gating with hard restrictions at L3 (evidence: provable claim L3_GATE_INVARIANTS, Article 36 review Section 6).

4. Fratricide prevention: IFF heartbeat with fail-safe semantics, 100m safety radius, operator confirmation (evidence: provable claim IFF_DECONFLICTION).

5. Cybersecurity: Daily key rotation, DRAM scrubber, no persistent secrets on airframe (evidence: FSG-A wiki chapter lisa26-captured-drone).

6. Operator cognitive safety: Multi-sensor agreement required before alerts; triage workflow; training tier structure (evidence: FSG-A wiki training chapter).

7. EMC and radiation safety: Design for MIL-STD-461G compliance; ICNIRP compliance at 1m (evidence: planned Phase 1 test matrix).

8. Residual Risk Statement

After implementation of all controls in Section 5, the residual risk for each hazard is assessed. No hazard retains a 'High' risk level. Three hazards retain 'Serious' risk (H-01, H-02, H-03) due to Severity 1 even at Probability D (Remote); these are accepted based on the military utility argument and further reduced by mandatory operator training and procedural controls.

The residual risk profile is judged acceptable for TRL 6 operational demonstration with Försvarsmakten oversight. Operational deployment (TRL 9) would require re-assessment based on accumulated operational data.

9. Safety Management

Safety management through a notional programme lifecycle would typically include:

• Quarterly Safety Review Board chaired by FSG-A Safety Officer

• All incidents and near-misses logged and reviewed

• FMEA and Safety Case re-issued at each TRL milestone

• Independent safety audit at TRL 6 and TRL 9

• Safety training mandatory for all operators and technicians

10. References

MIL-STD-882E — System Safety (US DoD).

UK MoD Def Stan 00-56 — Safety Management Requirements for Defence Systems.

Additional Protocol I to the Geneva Conventions, Article 36 (ICRC).

NATO AEP-84 — Safety of Unmanned Aerial Systems.

STANAG 4671 Ed. 1 — UAV Systems Airworthiness Requirements.

FSG-A-FMEA-001 — Failure Mode and Effects Analysis.

FSG-A-RISK-001 — Programme Risk Register.