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

Fischer Ventures EOOD, Varna, Bulgaria (UIC 206683576)

Threat and Vulnerability Assessment

Reference Design — Threats Against a Deployed UAS

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-THREAT-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.

1. Purpose and Scope

This Threat and Vulnerability Assessment identifies threats AGAINST the FSG-A system and its operators. This is the complement to the Fischer 26 / Lisa 26 combat capability documentation, which covers threats the system is designed to DEFEAT (primarily enemy UAVs, armour, and supply nodes).

This assessment is scoped from the perspective of a sophisticated adversary attempting to neutralise, capture, exploit, or subvert the FSG-A system. Countermeasures are documented for each threat and traced to specific design features or procedures.

Methodology follows NIST SP 800-30 Rev 1 (Guide for Conducting Risk Assessments) and NATO STANAG 4795 (Cyber Resilience for Defence Systems) conventions.

2. Threat Actor Profile

The assessment considers five threat actor categories:

• Nation-state (peer adversary) — Russia, China — Advanced capability including cyber weapons, EW, SIGINT, HUMINT.

• Nation-state (near-peer) — Belarus, Iran — Intermediate capability; primarily cyber and SIGINT.

• Criminal — profit-motivated; ransomware, cryptocurrency theft; limited military capability.

• Research / competitor — academic or industrial; advanced ML and cryptanalysis capability, no combat effects.

• Insider — compromised or disaffected personnel within the FSG-A organisation or partner.

Peer-adversary threats are the primary planning case. If the system is resilient against peer threats, lesser threats are covered a fortiori.

3. Likelihood and Impact Scoring

Likelihood (L/M/H):

• L (Low) — Technically demonstrated but rare operational use; requires specific targeting decision.

• M (Medium) — Known operational use against similar systems; expect regular attempts.

• H (High) — Ubiquitous in operational environments; continuous attempt expected.

Impact (L/M/H):

• L — Mission degraded but continues; recoverable.

• M — Mission failure; loss of airframes/data; recoverable at cost.

• H — Multi-airframe loss; cryptographic compromise; fratricide; programme setback.

4. Supply Chain Threats

5 supply chain threats identified.

ID	Threat	Actor	Capability	L	I	Countermeasure
TS-01	Compromised firmware in Silvus radio module	Nation-state	Advanced	L	H	Reproducible firmware build verification; pre-flight hash check against known-good; alternative radio qualified (Bittium TAC WIN)

TS-02	Malicious Python package published as typo-squat	Criminal / Nation-state	Intermediate	M	M	Vendored dependencies in FSG-A infrastructure; SHA-256 verification; pip audit in CI
TS-03	u-blox GPS module with hidden spoofing backdoor	Nation-state	Advanced	L	H	Crossed-check with IMU/SLAM; anomaly detection on GPS vs dead-reckoning; CRPA beamforming rejects spoofing from known azimuths
TS-04	Counterfeit LiPo battery with different chemistry	Criminal	Basic	M	M	Sourcing only from qualified distributors; BMS monitors match manufacturer specs; initial capacity test on every new battery
TS-05	Raspberry Pi CM4 compromised during manufacture	Nation-state	Advanced	L	M	Secure boot with verified signature chain; runtime attestation; isolation of CM4 from critical flight-safety code paths

5. Cyber Threats

5 cyber threats identified.

ID	Threat	Actor	Capability	L	I	Countermeasure
TC-01	Lisa 26 server remote code execution via web interface	Criminal / Nation-state	Intermediate	M	H	TLS 1.3 only; mutual certificate authentication; WAF; regular pen-test; least-privilege service account; no outbound internet from operational instance
TC-02	SQL injection into Lisa 26 database	Criminal	Basic	L	M	Parameterised queries exclusively; ORM (SQLAlchemy) in all paths; static analysis in CI
TC-03	MAVLink command injection into airframe	Nation-state	Advanced	L	H	HMAC-SHA256 signing of all commands; per-airframe key; sequence number rejection of replay; daily key rotation
TC-04	Exfiltration of target data from captured drone	Nation-state	Advanced	M	M	DRAM scrubber on power loss; no persistent target data on airframe (telemetry streamed, not stored); destructive self-test
TC-05	DoS attack against Lisa 26 server	Criminal / Nation-state	Intermediate	M	M	Rate limiting; offline mode ('lisa26-offline-debrief') allows continued operations; redundant server deployment

6. EM Warfare Threats

4 em warfare threats identified.

ID	Threat	Actor	Capability	L	I	Countermeasure

TE-01	GPS jamming across operational area	Nation-state	Common (RU)	H	M	SLAM-based dead-reckoning; CRPA null-steering; visual-inertial odometry; pre-loaded terrain reference waypoints for RTL
TE-02	Communications jamming across UHF tactical bands	Nation-state	Common (RU)	H	H	Design intent: FHSS frequency-agile; mesh re-routing; IR/optical fallback link; ADR (adaptive data rate) drops bandwidth rather than dropping link
TE-03	HPM (High-Power Microwave) weapon	Nation-state	Rare (emerging)	L	H	MIL-STD-461G EMC compliance provides partial protection; dispersed fleet (loss of one airframe tolerable); no single-point-of-failure in comms
TE-04	GPS spoofing to redirect drone	Nation-state	Intermediate	M	H	RAIM (Receiver Autonomous Integrity Monitoring); cross-check with IMU ground-speed; rejected if inconsistent; ADS-B consistency check (F26E)

7. Kinetic Threats

4 kinetic threats identified.

ID	Threat	Actor	Capability	L	I	Countermeasure
TK-01	Ground-launched anti-drone system (Pantsir, 9K33)	Nation-state	Common	H	M	Low radar cross-section design; thermal signature minimisation; altitude below 500m keeps below most radar coverage; cost asymmetry — our loss cost low vs their interceptor cost
TK-02	Interception by enemy fighter aircraft	Nation-state	Uncommon	L	M	Low speed + low thermal signature makes IR missile seeker acquisition difficult; dispersed swarm — one loss acceptable; altitude hugging terrain
TK-03	Enemy interceptor drone (air-to-air)	Nation-state	Emerging	M	M	Fischer 26E mesh-coordinated evasion; larger swarm → probabilistic survival; passive radar / SLAM-based threat detection
TK-04	Small-arms fire (opportunity shooting)	Any	Common	M	L	Operational altitude above small-arms effective ceiling (>500m during transit); low profile reduces visual acquisition

8. Adversarial ML Threats

3 adversarial ml threats identified.

ID	Threat	Actor	Capability	L	I	Countermeasure
TA-01	Adversarial patch to defeat YOLOv8 detection	Nation-state / Research	Advanced	M	M	Ensemble with thermal stream (IR harder to spoof); multi-sensor Dempster-Shafer requires 2+ agreement; model retraining with adversarial examples

TA-02	Model poisoning via compromised training data	Nation-state	Intermediate	L	H	Training data sourced only from vetted channels; hash-verified datasets; shadow evaluation against held-out reference set
TA-03	Model extraction via repeated query	Nation-state / Competitor	Intermediate	L	M	Model deployed air-gapped (no remote query surface); rate-limiting on any exposed inference interface

9. Insider Threats

2 insider threats identified.

ID	Threat	Actor	Capability	L	I	Countermeasure
TI-01	Compromised operator exfiltrates target data	Nation-state (HUMINT)	Intermediate	L	H	Two-person rule for L3 authorisation; audit logs immutable (append-only); classification controls; regular personnel security review
TI-02	Developer introduces backdoor in SDK	Nation-state (HUMINT)	Advanced	L	H	All commits reviewed by 2 reviewers; signed commits mandatory; CI-side static analysis; reproducible builds allow external verification

10. Summary

Total threats assessed: 23

High-likelihood threats (L=H): GPS jamming, comms jamming, ground-launched anti-drone systems — these are assumed-present in any operational deployment against a peer adversary.

High-impact threats (I=H): firmware compromise in Silvus radio, GPS spoofing, comms jamming, HPM weapons, L3 model poisoning, insider-introduced SDK backdoor, captured-drone data exfiltration.

The combined H×H combination is limited to: comms jamming. This is the dominant operational risk and drives much of the architectural resilience design (mesh networking, multi-band, IR/optical fallback).

11. Countermeasure Traceability

Every threat entry includes at least one countermeasure. Countermeasures trace to specific design features documented in:

• FSG-A wiki chapters (anti-jam-hardening, cybersecurity-mavlink, firmware-hardening, lisa26-captured-drone, crpa-antennas)

• SDK source code (cryptographic primitives, HMAC signing, Dempster-Shafer fusion, L3 gate invariants)

• Procedural controls (operator training, two-person rule, classification controls)

No threat is accepted without a documented countermeasure.

12. References

NIST SP 800-30 Rev 1 — Guide for Conducting Risk Assessments.

NATO STANAG 4795 — Cyber Resilience for Defence Systems.

MITRE ATT&CK; for ICS — tactics and techniques applicable to UAS operational technology.

FSG-A-SAFETY-001 — System Safety Case.

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

FSG-A wiki https://fsg-a.com/ — threat-specific countermeasures.