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

Fischer Ventures EOOD, Varna, Bulgaria (UIC 206683576)

# Software Bill of Materials

## Reference Design — Software Component Inventory

**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-SBOM-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

This Software Bill of Materials (SBOM) documents every software component in the FSG-A system, including its version, license, provenance, and current CVE (Common Vulnerabilities and Exposures) status. The SBOM is maintained per ISO/IEC 5962:2021 (SPDX) format guidance and CISA/NTIA SBOM minimum-element requirements.

This document is required for regulatory compliance under the EU Cyber Resilience Act (Article 13) for products with digital elements. It is also required input to the Safety Case (FSG-A-SAFETY-001) for cybersecurity arguments.

# 2. Minimum Elements (per CISA guidance)

Each component entry in this SBOM includes the seven minimum elements defined by NTIA:

• Supplier name (or 'first-party' if FSG-A)

• Component name

• Version of the component

• Other unique identifiers (e.g. SPDX licence code)

• Dependency relationship (via Deployment Matrix, Section 8)

• Author of the SBOM data (Cybersecurity Lead (programme role, not staffed by FSG-A))

• Timestamp (document issue date, see cover)

# 3. FSG-A SDK Components

The SDK is the core library shared across all FSG-A subsystems. It is intentionally dependency-light to minimise supply-chain attack surface.

| Name | Version | Purpose | Licence | Provenance | CVE Status |
|---|---|---|---|---|---|
| libfischer26e | 2.0.0 | FSG-A SDK — NATO/Swedish integration | CC BY-SA 4.0 | FSG-A (first-party) | N/A — first party |
| Python | 3.9+ | Runtime | PSF | python.org | Track upstream CVEs |
| cryptography (optional) | 41.0+ | HMAC, AES (if extending SDK) | Apache 2.0 / BSD-3-Clause | pypi.org/project/cryptography | CVE-2023-50782 patched in 42.0.2 |

# 4. Lisa 26 Server Components

Lisa 26 runs on a battalion-level server and provides the C2 web interface, AI detection pipeline, and fusion.

| Name | Version | Purpose | Licence | Provenance | CVE Status |
|---|---|---|---|---|---|
| Flask | 2.3.0 | Lisa 26 web server | BSD-3-Clause | pypi.org/project/Flask | Clean |
| Werkzeug | 2.3.x | Flask WSGI foundation | BSD-3-Clause | pypi.org/project/Werkzeug | CVE-2023-46136 patched in 3.0.1 |
| SQLite | 3.40+ | Local COP database | Public domain | sqlite.org | Clean |
| PyJWT | 2.8.0 | Session tokens | MIT | pypi.org/project/PyJWT | Clean |
| Jinja2 | 3.1.2 | Template rendering | BSD-3-Clause | pypi.org/project/Jinja2 | CVE-2024-34064 patched in 3.1.4 |

| Name | Version | Purpose | Licence | Provenance | CVE Status |
|---|---|---|---|---|---|
| NumPy | 1.24+ | Numerical processing for fusion | BSD-3-Clause | numpy.org | Clean |
| OpenCV | 4.8+ | Image processing pipeline | Apache 2.0 | opencv.org | Clean |
| PyTorch | 2.0+ | YOLOv8 inference | BSD-3-Clause | pytorch.org | Clean |
| ultralytics (YOLOv8) | 8.1.x | Object detection | AGPL-3.0 / commercial | github.com/ultralytics | Clean — licence review required for commercial use |

## 5. Fischer 26 / 26E Airframe Components

Airframe-side software — autopilot firmware, SDR, and tier-2-specific EW pipeline.

| Name | Version | Purpose | Licence | Provenance | CVE Status |
|---|---|---|---|---|---|
| ArduPilot / ArduPlane | 4.5.0+ | Autopilot firmware | GPL-3.0 | ardupilot.org | Clean |
| MAVLink | 2.0 protocol | Ground-station communication | LGPL-3.0 | mavlink.io | Clean |
| librtlsdr / SoapySDR | 3.0+ | SDR interface (Fischer 26E) | GPL-2.0 / LGPL | osmocom.org / github | Clean |
| GNU Radio | 3.10+ | SDR signal processing | GPL-3.0 | gnuradio.org | Clean |
| libfischer26e | 2.0.0 | FSG-A SDK (same as above) | CC BY-SA 4.0 | FSG-A (first-party) | N/A |

## 6. GCS and Delivery Toolkit

Ground Control Station and secure-delivery utilities. These run on operator laptops, not on airframes.

| Name | Version | Purpose | Licence | Provenance | CVE Status |
|---|---|---|---|---|---|
| GnuPG | 2.2+ | OpenPGP encryption (gpg-tools) | GPL-3.0 | gnupg.org | Clean |
| python-gnupg | 0.5.6 | Python wrapper for GnuPG | BSD-2-Clause (new) | pypi.org/project/python-gnupg | Clean |
| reportlab | 4.4+ | PDF generation (this document) | BSD-3-Clause | reportlab.com | Clean |

## 7. Web Publication Components

Static site generator and interactive tools. These components affect only the public wiki and do not deploy to operational systems.

| Name | Version | Purpose | Licence | Provenance | CVE Status |
|---|---|---|---|---|---|
| FSG-A build system | 1.0 | Static site generator | CC BY-SA 4.0 | FSG-A (first-party) | N/A |
| Markdown (commonmark) | 0.9.1+ | Content processing | BSD-3-Clause | pypi.org/project/commonmark | Clean |
| React | 18.2+ | Interactive tool rendering | MIT | react.dev | Clean |
| Tailwind CSS (via classes) | 3.x | Styling (pre-compiled) | MIT | tailwindcss.com | Clean |
| Recharts | 2.10+ | Data visualisation in tools | MIT | recharts.org | Clean |

# 8. Deployment Matrix

✓ = required dependency; ■ = not installed; — = optional.

| Component | SDK | Lisa 26 Svr | F26E EW | GCS | Web |
|---|---|---|---|---|---|
| Python 3.9+ | ✓ | ✓ | ✓ | ■ | ✓ |
| libfischer26e v2 | ✓ | ✓ | ✓ | ■ | ■ |
| Flask | ■ | ✓ | ■ | ■ | ■ |
| PyTorch | ■ | ✓ | ■ | ■ | ■ |
| ultralytics / YOLOv8 | ■ | ✓ | ■ | ■ | ■ |
| ArduPilot / ArduPlane | ■ | ■ | ✓ | ■ | ■ |
| MAVLink 2.0 | ■ | ✓ | ✓ | ✓ | ■ |
| GnuPG | ■ | ■ | ■ | ✓ | ■ |
| React + Recharts | ■ | ■ | ■ | ■ | ✓ |

# 9. Licence Compatibility Analysis

The FSG-A first-party codebase is published under CC BY-SA 4.0. Dependencies use BSD/MIT/Apache (permissive, fully compatible with CC BY-SA redistribution), LGPL (compatible with dynamic linking), and GPL (compatible for internal use and derivative CC BY-SA publication).

One component requires specific attention: ultralytics (YOLOv8) is licensed AGPL-3.0 with a commercial license alternative. For FSG-A's current CC BY-SA 4.0 distribution model, AGPL-3.0 requires source disclosure of any network-accessible service using the model — which FSG-A satisfies by publishing the Lisa 26 server code. For end-users deploying in closed networks (Försvarsmakten operational use), AGPL-3.0 imposes no additional obligation. For commercial integrators wishing to restrict source disclosure, the Ultralytics commercial licence is required.

# 10. Supply Chain Security Controls

A programme adopting this architecture should download all components from official upstream sources (pypi.org, github.com/ardupilot, etc.) and verified against published SHA-256 hashes where available. A local mirror of all critical dependencies is maintained at FSG-A infrastructure to insulate against upstream outages or deliberate typo-squatting attacks.

Build artefacts are reproducible — a given git commit produces byte-identical build output given the same dependency lock file. This allows independent verification by evaluators and defends against build-system compromise.

Cryptographic dependencies (cryptography, GnuPG, OpenSSL transitively) should be updated promptly after any published High-severity CVE. Specific SLA [illustrative — programme to set based on its own security policy].

# 11. CVE Monitoring Process

Programmes adopting this architecture should run monthly automated scans against the NIST NVD database using pip-audit and equivalent tools for non-Python components. Quarterly manual review by Cybersecurity Lead. Any High-severity or Critical CVE triggers out-of-band assessment with patch or mitigation applied within the programme's security SLA [illustrative].

Scan results are recorded in the FSG-A wiki technical changelog. No High-severity CVEs are outstanding at time of this SBOM release.

## 12. Cryptographic Module Inventory

Software implementing cryptographic functions (as defined in FIPS 140-3):

• HMAC-SHA256 (MAVLink signing) — implemented in libfischer26e

• AES-256-GCM (at-rest encryption) — via cryptography library

• Ed25519 (signatures) — via cryptography library

• RSA-4096 / Curve25519 (OpenPGP) — via GnuPG

• HKDF (daily key rotation) — via cryptography library

All cryptographic implementations use well-reviewed, mainstream libraries. No custom cryptography is implemented.

## 13. References

ISO/IEC 5962:2021 — SPDX specification (Software Package Data Exchange).

CISA SBOM — minimum elements for a Software Bill of Materials (US Cybersecurity and Infrastructure Security Agency, 2021).

NTIA SBOM — Framing Software Component Transparency.

EU Cyber Resilience Act (Regulation 2024/2847) Article 13.

FIPS 140-3 — Security Requirements for Cryptographic Modules.

NIST NVD — National Vulnerability Database.

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