

E i g e n i a B . V .

Eigenia Cyber Digital Twin · Fail Fast, Fail Safe

CASE STUDY · OPEN-SOURCE INTELLIGENCE · REPRESENTATIONAL EXAMPLE

A representational drone ecosystem, built on the open-source Project Quiver to show how the Eigenia Cyber Digital Twin prepares a product for the CRA

An illustrative example of the Eigenia Cyber Digital Twin, built only from open-source information and general engineering knowledge. It is not a model of any manufacturer's product and is not to be read as high fidelity. Client engagements use controlled engineering data and produce very high-fidelity models.

Example

A representational multirotor ecosystem based on Arrow-air Project Quiver, with a Crazyflie 2.1 stack alongside

Built from

Open-source intelligence and engineering judgement only

Regime

Cyber Resilience Act, (EU) 2024/2847



Eigenia Cyber Digital Twin, 3D scene. X-ray view of the representational airframe built from the open-source Project Quiver bill of materials. Geometry is procedural; it illustrates the method and is not a CAD model.

01 Summary

A manufacturer placing a drone on the EU market has to prove, product by product, that it is secure by design, that it knows every component inside it, and that it can report an actively exploited vulnerability within 24 hours. This case study uses a representational drone ecosystem, built from open-source intelligence, to show how Eigenia builds a product as a Cyber Digital Twin first, so that those obligations become questions the model can answer rather than spreadsheets assembled before an audit.

The example is built on [Arrow-air Project Quiver](#), an open-source multirotor development kit whose bill of materials, PCB production files and harness guide are published. A Crazyflie 2.1 nano-drone stack, a ground segment, a maintenance bench and a twin platform sit alongside it, so the model covers a small system of systems rather than one airframe.

9

system records in the ecosystem

143

BOM items from the open-source repository

297

PCB components at KiCad positions

135

harness wires with pin, signal and gauge

34 · 58

interfaces · sub-interfaces

45

failure modes, 10 attacker-triggerable

REPRESENTATIONAL ONLY — OPEN-SOURCE INTELLIGENCE

Every figure in this document comes from public sources (the Project Quiver repository, Bitcraze datasheets, ArduPilot documentation and vendor manuals) or from engineering judgement where those sources are silent. Values the sources do not state are tagged *assumed* in the model. The example has limited information by design: firmware versions are unpinned, geometry is procedural and no hardware was tested. It shows how the platform works; it makes no claim about the security or compliance of Project Quiver or any product built from it.

CLIENT ENGAGEMENTS

On a client engagement the same platform is fed with controlled engineering data: CAD and DEXPI drawings, build manifests, firmware hashes, supplier certificates and test results. The resulting models are of very high fidelity and are held under the client's control.

02 The ecosystem

Project Quiver is a 25 kg maximum take-off weight multirotor with 5–8 kg of payload capacity, an aluminium plate frame with carbon-fibre arms, four Hobbywing X6 Plus motor-and-ESC units, a 14S 30 Ah smart battery and four custom PCBs. The twin models it, and the systems around it, as independent system records.

System record	Role	Core components (open-source BOM)
SYS-QVR-AIR	Air vehicle	Pix32 v6 flight controller with ArduPilot, Raspberry Pi 5, 2× GigaBlox Nano switches, CubeNode ETH, Here4 + M9N GNSS, NRA15, MR82, RPLidar S2L, db201 Remote ID, SIYI A8 mini, Main / BC / FC / Attachment PCBs
SYS-HM30-AIR	Airborne link	SIYI HM30 air unit and two antennas: RC, MAVLink telemetry and video over one radio
SYS-MK32-GCS	Ground controller	SIYI MK32 handheld ground station
SYS-QGC-WS	Operator workstation	QGroundControl workstation
SYS-CF21-AIR	Air vehicle	Crazyflie 2.1: STM32F405 + nRF51822, BMI088 / BMP388, expansion-deck bus
SYS-CRADIO	Radio gateway	Crazyradio 2.0 (nRF52840) USB dongle
SYS-CF-HOST	Operator workstation	cfclient / cflib host
SYS-DT-PLAT	Twin platform	DMZ broker and gateway, asset graph, model store, telemetry store
SYS-MAINT	Maintenance	Debug probe, provisioning laptop, charger, calibration turntable

Each system record carries its own bill-of-materials fragments, documentation, configuration and the buses and links that connect it to its neighbours, with every value marked *reported* (from a cited source) or *assumed*.



System-of-systems view in the Eigenia Cyber Digital Twin. Each system record is an independent node with its zone volume; conduits are drawn between them.

03 Why this matters now

CRA reporting obligations under Article 14 have applied since 11 September 2026, and the regulation applies in full from 11 December 2027, when CE marking requires demonstrated conformity. Every product in a portfolio needs its own risk assessment, SBOM, technical file and conformity route, and every new version reopens them.

WHY A REPRESENTATIONAL MODEL

Open-source hardware gives a public, inspectable example where every input can be checked. It lets Eigenia show the full method on a real bill of materials without exposing any client's data, and it shows honestly where public information runs out: those gaps are exactly what a client engagement fills with controlled data.

04 The same six-phase method

This example was built with the same six-phase Eigenia readiness method used for client engagements and for representational models such as LEO-RSAT-001. Phases 1 to 4 follow IEC 62443; for a product the emphasis shifts from the system view (62443-3-2 zones and conduits) to

the product security lifecycle and component requirements (62443-4-1 and 4-2), with the CRA obligations on top. Phases 5 and 6 are Eigenia additions: an ALARP review, so residual risk is argued rather than assumed, and a defined handover, so the bench starts with a known scope.

Phase	IEC 62443 activity	Applied to the example	Feeds the CRA evidence
1 · Scope and classify	Confirm CRA scope and exclusions, core functionality, class, conformity route and support period	Nine system records inventoried; scope and class left open for a representational product	Classification record with reasoning; product description for the technical file
2 · Risk assessment	Zones, conduits, threats and consequences in the intended use (62443-3-2)	Eight zones from flight control to maintenance, with SL-T per foundational requirement; 45 failure modes and five fault trees	The cybersecurity risk assessment the technical documentation must contain
3 · Requirements and design	Map Annex I Part I to 62443-3-3 / 4-2 requirements and security levels	34 interfaces and 58 sub-interfaces typed at signal, protocol, network and security level	RTM rows; non-applicable requirements justified
4 · Secure development and vulnerability handling	Lifecycle evidence, SBOM, HBOM, CBOM, CVD policy, update mechanism, Art. 14 readiness (62443-4-1)	CycloneDX 1.6 SBOM with 19 firmware and software components (versions unpinned); HBOM from 143 BOM items	Vulnerability handling evidence and the security update plan
5 · ALARP review	For each residual risk: further measures, their cost and effect, and why the remainder is as low as reasonably practicable	Estimated SL-C against SL-T per sub-interface; cascades simulated for every failure mode	Residual risk argument recorded in the technical file
6 · Handover to the test bench	Frozen dossier, RTM, focus areas, test scope and API access; bench confirms receipt and scope	Export package generated; gate decision recorded as no-go with listed gaps	RTM, test results, declaration readiness

Zones inside the product

Zones and conduits apply inside the airframe as much as across a facility. The twin draws each zone as a volume around the parts it contains, and every conduit between zones carries the interfaces that cross it.

Zone	Contains	Why it is separate
Z-AIR-FLIGHT	Pix32 v6, FC PCB, GNSS, LiDAR, radars	Integrity and availability of flight control dominate
Z-AIR-ACT	Battery, BC PCB, busbars, X6 Plus motors and ESCs, propellers	Prevent unsafe actuation and preserve a safe state
Z-AIR-COMMS	HM30 air unit, antennas, CubeNode ETH, switches, Remote ID	Terminates every externally exposed conduit
Z-PAYLOAD	Raspberry Pi 5, A8 mini camera, attachment interfaces	Potentially lower-trust applications
Z-GROUND-CTRL	MK32, QGroundControl, cfclient host, Crazyradio	Holds operator authority and credentials
Z-DMZ · Z-ENTERPRISE	Twin integration DMZ; twin services	Separate operational data from enterprise services
Z-MAINT	Debug probe, provisioning laptop	Privileged cross-zone capability

ONE METHOD, EVERY SCALE

The same workshops, zone and conduit reasoning and evidence discipline serve a representational satellite such as LEO-RSAT-001, this drone ecosystem, a substation or a hyperscale campus. A product twin can later sit inside a facility twin as one of its assets.

05 Inside the airframe

The twin models the airframe part by part and link by link: plates, arms, PCBs with their components at KiCad positions, every harness wire with its pins, and the buses that join them. That is what lets a single failure or a single unauthenticated bus be traced to everything that depends on it.

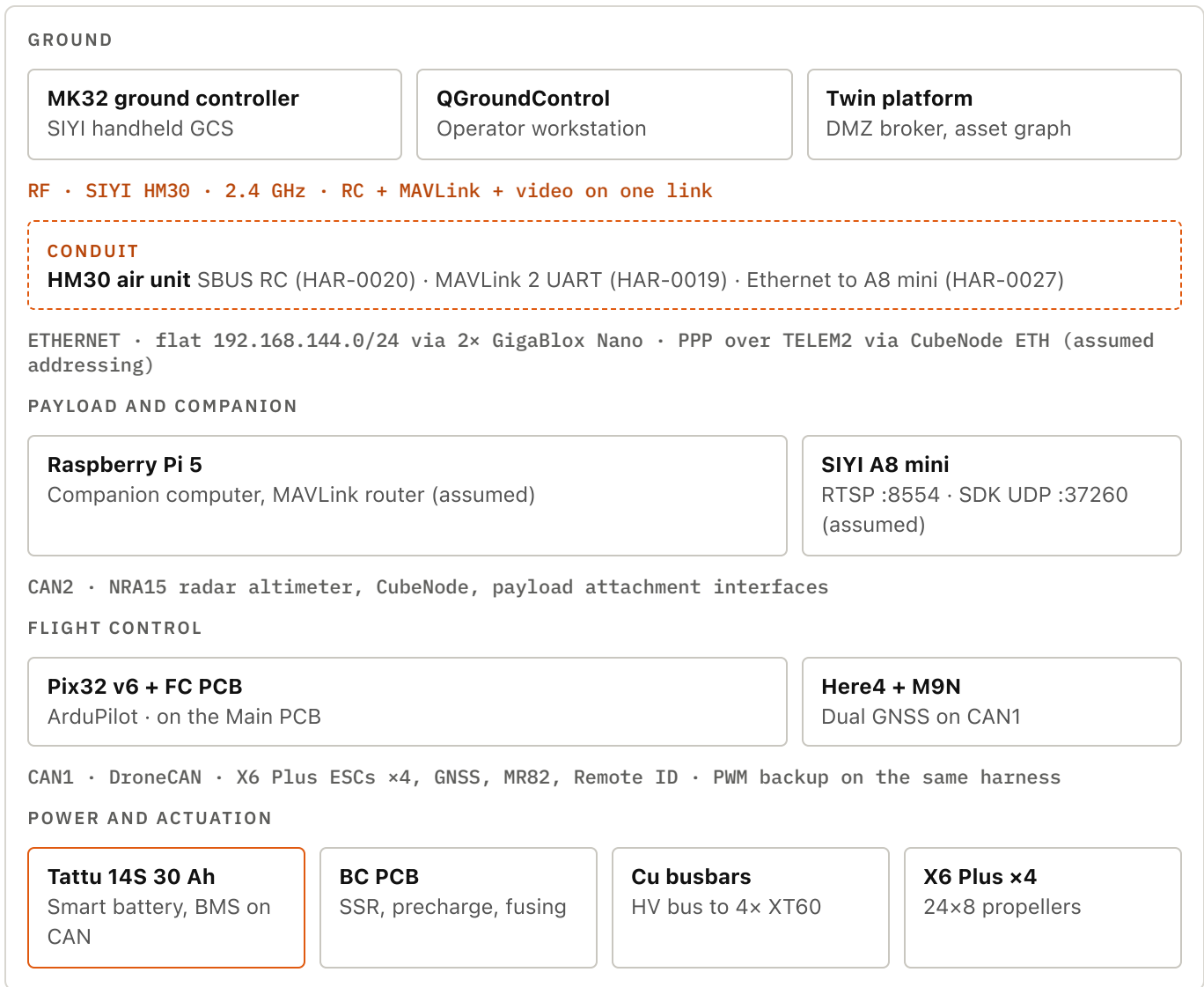


Figure 1. Avionics architecture of the representational airframe, drawn from the model. The dashed box is the single radio conduit leaving the aircraft. Addressing and rates marked assumed are typical defaults.

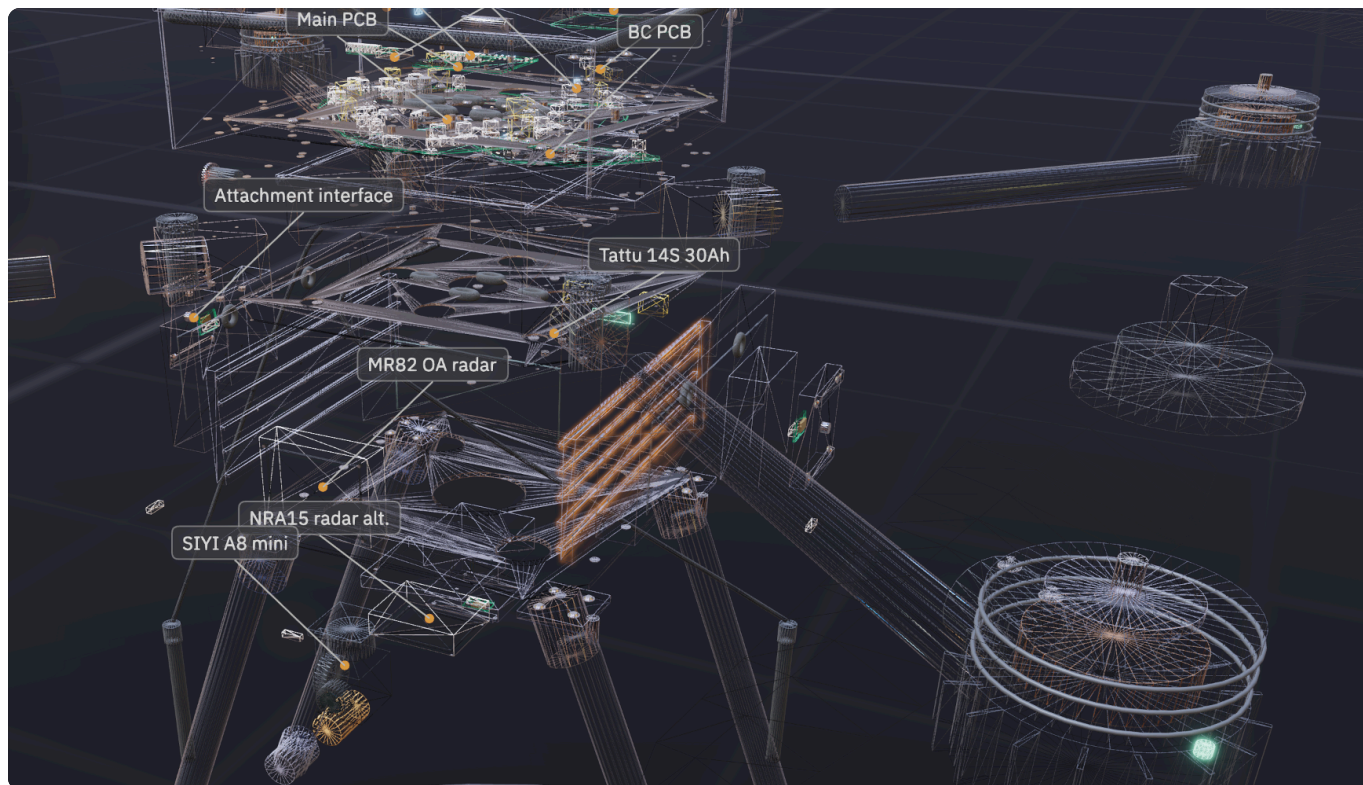


Figure 2. Exploded X-ray view in the Eigenia Cyber Digital Twin. Each labelled item (main PCB, battery-connector PCB, attachment interface, Tattu 14S 30 Ah battery, MR82 obstacle-avoidance radar, NRA15 radar altimeter, SIYI A8 mini) is a part with its own record, zone and links.

Every link, typed

The twin records each interface with its protocol, rate and the control that protects it, and estimates the security capability (SL-C) it achieves against the zone target (SL-T). A selection of the most security-relevant links:

Link	Protocol · rate	Control	Evidence
Flight controller → X6 Plus ESCs	DroneCAN on CAN1, 1 Mbit/s; RawCommand at 400 Hz (assumed)	CRC only; no node authentication	Reported pinout; rates assumed
HM30 ↔ flight controller	MAVLink 2 over UART, 115 200 baud (assumed)	Signing available, not configured	Assumed
HM30 → flight controller	SBUS, 100 000 baud 8E2, 16 channels	Physical access only	Reported
Flight controller ↔ CubeNode ETH	PPP over TELEM2 with RTS/CTS	Flat LAN; no VLAN or 802.1X	Assumed
A8 mini → HM30	RTSP / H.264 over Ethernet	None documented	Assumed
MK32 ↔ HM30	Vendor 2.4 GHz digital link	Pairing; encryption not evidenced	Unknown
Crazyradio ↔ Crazyflie	CRTP over Enhanced ShockBurst, default address 0xE7E7E7E7	No authentication or encryption	Reported
STM32F405 ↔ nRF51822	Syslink UART, 1 Mbaud	Checksum only	Reported

WHY THIS MATTERS FOR THE CRA

Because the twin holds every link with its protocol and exposure, it can answer "who can command the motors?" for this configuration: any node on CAN1, because DroneCAN frames carry no authentication. That is a specific, testable finding rather than a general statement about the protocol.

06 Bills of materials, one record

The model holds CycloneDX 1.6 bills of materials alongside a DEXPI-style structural export, all keyed to the same component identifiers. In this example the hardware side is rich, because the open-source repository publishes it; the software side is thin, because firmware versions are not published.

BOM	What it records here	What is missing in open-source data
HBOM	143 BOM items with quantities, materials, suppliers, part numbers and STEP references; 297 PCB components with footprint, value and position	Batch, lot and certificate-of-origin data
SBOM	19 firmware, OS and application components across both stacks, with package URLs where they exist	Every version is unpinned, so no CVE match can be claimed
Harness	28 harnesses and 135 wires with pins at both ends, signal, colour and gauge	Route lengths are taken from the guide; 3D routing is procedural
CBOM	Placeholders for link encryption and signing per sub-interface	No cryptographic material is documented in the sources

07 Suppliers in the open-source BOM

The Project Quiver bill of materials names the supplier of each part. The twin records them so provenance and export questions can be asked of the model; locations are the suppliers' publicly stated headquarters and are not batch-level provenance.

Supplier	Parts in the example	Public location
Hobbywing	X6 Plus motor + ESC, MFP 24×8 propellers	China
Holybro	Pix32 v6 flight controller	China
SIYI	HM30 link, MK32 controller, A8 mini camera	China
Tattu	14S 30 Ah smart battery	China
CubePilot	Here4 GNSS, CubeNode ETH	Australia
Raspberry Pi	Raspberry Pi 5	United Kingdom
BotBlox	GigaBlox Nano Ethernet switches	United Kingdom
Nanoradar · Slamtec · Mateksys	NRA15, MR82, RPLidar S2L, M9N	China
Bitcraze	Crazyflie 2.1, Crazyradio 2.0	Sweden

Locations are as publicly stated by each company and are given for illustration only.

08 From vulnerability to report

The twin links each component to the links that would expose it, so a disclosure becomes a question with an answer: are we affected, how exposed are we, and what have we done about it. In this example the first question cannot yet be answered, and the model says so: with firmware versions unpinned, no CVE can be matched to the build.

Signal	State in the example
CVE / CWE	Not matched: SBOM versions unpinned
EPSS / KEV	Not scored until CVEs are matched
Reachability	Available now: every component is placed on its zones, conduits and sub-interfaces, so a future CVE can be ranked by exposure on arrival

The 24-hour clock

Under Article 14 of the CRA, which applies from 11 September 2026, a manufacturer that becomes aware of an actively exploited vulnerability or a severe incident must send an early warning within 24 hours, a fuller notification within 72 hours, and a final report afterwards, through the single reporting platform to ENISA and the national CSIRT.



Once versions and serial ranges are recorded, the affected component, its exposure and its mitigation status sit in the model, and the early-warning payload can be assembled from it. The hard part of meeting 24 hours is knowing what you shipped, and that is what the twin is built to hold.

09 How an adversary would attack it

The twin carries a dependency model of 80 functional nodes. Any part, wire or bus can be failed, and the cascade, the redundancy that holds and the failsafes that respond are replayed on a timeline. Ten of the 45 failure modes can be triggered by an attacker through a security gap. Two of them:

Uncommanded motor start via CAN1

FM-10 · IF-QVR-CAN1-ESC

1. A rogue node is attached to CAN1, for example through a payload or service connector.
2. It publishes DroneCAN ESC RawCommand frames; the ESCs cannot tell them from the flight controller's.
3. Motors spin up or change thrust without operator command.

MITIGATIONS TO EVIDENCE

- Physical access control on CAN connectors
- Segment the ESC bus from GNSS, radar and payload nodes

Malicious firmware through the service port

FM-38 · IF-MAINT-QVR-FW

1. A provisioning laptop is compromised.
2. An unsigned image is flashed to the flight controller over USB or SWD.
3. The aircraft behaves as the attacker chooses: flyaway or uncommanded motor start.

MITIGATIONS TO EVIDENCE

- Signed bootloader enabled and recorded
- Controlled provisioning with firmware hash checks

Both scenarios end in a top event in the fault trees: loss of control, flyaway or uncommanded motor start. Scores and capability estimates are engineering judgement for a representational model, not a certified analysis.

10 Annex I requirements, mapped to evidence

The CRA sets essential cybersecurity requirements in Annex I. For each one the twin records what the open-source design shows today and what evidence a bench would need. In a representational example many rows are gaps, and showing them is the point.

Requirement	What the model shows	Evidence state
No known exploitable vulnerabilities	19 SBOM components placed on their links	Gap: versions unpinned
Secure by default	ArduPilot defaults leave GCS and battery failsafes disabled; Crazyradio uses a default address	Gap
Protection against unauthorised access	DroneCAN, CRTP and unsigned MAVLink accept unauthenticated commands	Gap: SL-C 0 vs SL-T 2
Confidentiality	Unencrypted links listed per sub-interface	Gap
Integrity	CRC on buses; firmware signing not evidenced	Gap
Minimal attack surface	34 interfaces enumerated, including USB-C and SWD service ports	Partial
Resilience to denial of service	A single CAN1 fault drops ESC CAN, both GNSS, radar and Remote ID; PWM backup shares the ESC signal harness	Partial: cascade simulated
Secure updates	Update paths modelled for flight controller, ESCs and peripherals	Gap: signing not evidenced

11 The CRA evidence pack

Conformity is shown with evidence, not assertions. The platform produces the digital files that describe the product, the bench tests that would reproduce its claims, and a Requirements Traceability Matrix that ties every requirement to its evidence.

Digital files

Every file is machine-readable and generated from the same model, so they agree with each other by construction. This example exports them as one package.

File	Format	What it is for
models/drone-twin-sos.glb	glTF 2.0	Full scene with per-part metadata; one GLB per system
sbom/cyclonedx-1.6.json	CycloneDX 1.6	Hardware, firmware, applications, interfaces as services, dependencies
dexpi/drone-twin.dexpi.xml	DEXPI-style XML	Equipment, signal lines, cables and conductors
data/icd.csv · icd.json	CSV / JSON	Interfaces and sub-interfaces with parameters, messages and pinouts
data/harness_wires.csv	CSV	135 wires with pins, signal, colour and gauge
fmeca/failure_modes.json	JSON	45 failure modes with cascade, failsafes and top events
fmeca/dependency_graph.graphml	GraphML	80 functional nodes and their dependencies
db/neo4j/drone_twin.cypher	Neo4j Cypher	Assets, zones, interfaces and failure modes as a queryable graph

Test bench readiness

A test bench reproduces the product's security claims on real hardware. The twin defines what the bench must test and tracks whether each test is ready. For this representational example none has been run.

Bench test	Exercises	Status
Port and service scan of every interface	Minimal attack surface	Defined
Signed and unsigned firmware on the flight controller	Secure updates	Blocked: signing not evidenced
Injected DroneCAN ESC commands on CAN1	Protection against unauthorised access	Defined
Unsigned and replayed MAVLink frames	Protection against unauthorised access	Defined
CAN1 short with PWM backup check	Denial-of-service resilience	Defined
SBOM against firmware manifest	No known exploitable vulnerabilities	Blocked: versions unpinned
Early-warning drill inside 24 hours	Vulnerability reporting	Defined

Requirements Traceability Matrix

The RTM is the backbone of the pack. Each row traces a requirement through the design element, the components, the test and the evidence it produces. Read top to bottom it shows coverage; read along a row it shows the pathway from obligation to proof.

Req.	Requirement	Components	Test	Evidence
R-01	No known exploitable vulnerabilities	ArduPilot, AP_Periph, HM30, A8 mini firmware	SBOM vs manifest, CVE scan	SBOM + VEX record
R-03	Unauthorised access	Pix32 v6, X6 Plus ESCs, HM30	Injected and replayed frames	Bench log
R-05	Integrity	Bootloader, CAN1, UART links	Tampered firmware, command injection	Bench log
R-07	Denial-of-service resilience	CAN1, ESC signal harnesses, HM30	Bus short, link jamming	Cascade + bench log
R-08	Secure updates	Flight controller, ESCs, peripherals	Signed and unsigned bundles	Update test report
R-09	Vulnerability reporting	Whole ecosystem	24-hour drill	Drill record

WHY THE RTM MATTERS

An assessor's first question is "show me how you know". The RTM answers it for every requirement at once, and because it is generated from the model, a design change that breaks a trace shows up as a gap immediately rather than at the next audit.

12 Ready for the test bench

Most delays in conformity assessment are not failed tests. They are waiting: for a file, a configuration, a firmware build, an answer from engineering. The Eigenia Cyber Digital Twin removes the wait by holding everything a test bench needs in one unified format, and by checking the product is ready before it reaches the bench.

One unified data model

DEXPI Engineering data from CAD Full DEXPI import of the design drawings, so the physical and logical design comes from the engineering source rather than a redrawn diagram.	CYCLONEDX Extended bills of materials SBOM for software, HBOM for hardware, CBOM for cryptography and a machine BOM, all in CycloneDX and linked to the same components.	THREAT DATA Vulnerability intelligence Every component checked for CVEs and their CWE weakness classes, scored for exploit likelihood with EPSS, and matched against the CISA Known Exploited Vulnerabilities catalogue.	MODEL The twin itself Architecture, zones, conduits, links, threat trees and the RTM, joining the files above into one queryable record.
---	--	--	--

Vulnerabilities, prioritised the way a bench needs them

A CVE list on its own does not tell a manufacturer what to fix first. The twin layers four signals on each finding, then adds the one thing a public database cannot know: whether the vulnerable code is actually reachable in this product.

SIGNAL	QUESTION IT ANSWERS	SOURCE
CVE	Is there a known vulnerability in this component version?	National Vulnerability Database, matched from the SBOM
CWE	What kind of weakness is it, and where else does that weakness class appear?	Common Weakness Enumeration
EPSS	How likely is it to be exploited in the next 30 days?	Exploit Prediction Scoring System
KEV	Is it already being exploited in the wild?	CISA Known Exploited Vulnerabilities catalogue
Reachability	Can it be reached through this product's links and zones?	The twin: the link table, zones and conduits

A finding on the KEV list that is reachable through a product link is a reportable, fix-now item. One with a low EPSS score behind a zone boundary can be scheduled. That ordering is what turns a vulnerability feed into a work plan, and it is the same evidence the 24-hour reporting obligation depends on.

A checklist for both assessment routes

Depending on its classification, a product is assessed either by the manufacturer itself or by a third-party notified body. The twin keeps one checklist that serves both, with every item tied to a file, a test or an RTM row.

EVIDENCE ITEM	SELF-ASSESSMENT	NOTIFIED BODY	PULLED FROM
Product description and architecture	Required	Required	System records, DEXPI
Cybersecurity risk assessment	Required	Required	Zones, threat trees, CVE analysis
SBOM, HBOM, CBOM, machine BOM	Required	Required	CycloneDX files
Vulnerability analysis with CWE, EPSS and KEV	Required	Required	Threat data layer
Test procedures and bench results	Recorded internally	Witnessed or reviewed	Test bench records
Requirements Traceability Matrix	Required	Required	RTM
Vulnerability handling and reporting process	Required	Required	Reporting drill records
Security update plan for the support period	Required	Required	Firmware and key records

This table summarises what the model is set up to evidence. The exact requirements for a product depend on its classification and the applicable harmonised standards, which must be confirmed for each product.

Pull, not push: 5S for the test bench

Bench testers work best when everything they need is where they expect it, labelled and current. The twin applies that discipline to evidence.

5S APPLIED TO BENCH EVIDENCE

Sort	Only the files, builds and configurations that apply to the product variant under test are in scope.
Set in order	Every item has one place in the unified model and one identifier, so a tester finds it without asking.
Shine	Integrity checks flag missing, stale or contradictory evidence before the bench sees it.
Standardise	The same structure for every product and every lab, so a tester who knows one pack knows them all.
Sustain	Evidence regenerates from the model whenever the product changes, so the pack never drifts out of date.

Testers pull the data they need when they need it, rather than raising a request and waiting. For a lab that runs a tight schedule, that is the difference between a test slot used and a test slot lost.

The preparedness service and the go / no-go decision

Before a product goes to the bench, Eigenia runs a readiness review against the checklist and the RTM. Every gap is shown with its owner and the work needed to close it, and the review ends in a clear decision.

GO

Every RTM row traces to evidence, no reachable KEV items remain open, and the bench tests are ready. The product goes to the lab on schedule.

NO-GO

Gaps are listed with owners and effort. Eigenia engineers work with the manufacturer to close them, so the lab slot is moved once rather than wasted.

WHAT THE MANUFACTURER GAINS

Fewer failed or abandoned test slots, less engineering time spent answering evidence requests, and a schedule the lab can rely on. The same unified record then carries forward into the technical file and the post-market support period, so the effort spent preparing for the bench is not spent again.

13 For bench testers: a guide

This section is written for the people who run the tests: in-house security teams preparing a self-assessment, and laboratories or notified bodies carrying out a third-party conformity assessment. It describes what arrives with an Eigenia-prepared product, how to use it, and why it shortens the work.

What you can expect

YOU RECEIVE	WHAT IT CONTAINS	HOW YOU USE IT
Readiness report	The go / no-go decision, open gaps with owners, and the scope of the product variant under test	Confirm the product is ready before booking or starting a slot
Requirements Traceability Matrix	Every requirement traced to design element, components, test and evidence file	Your test plan: work down the rows, and every row tells you where its evidence lives
Unified evidence pack	DEXPI engineering data and CycloneDX SBOM, HBOM, CBOM and machine BOM, all keyed to the same component identifiers	Look up any component once and see its software, hardware, cryptography and drawings together
Vulnerability analysis	CVE and CWE per component, EPSS likelihood, KEV status and reachability through the product's links	Focus test effort on findings that are both exploitable and reachable
Bench test definitions	Procedure, configuration and expected result for each test, linked to its RTM row	Run tests to a defined procedure and record results against the right requirement
Architecture and interface model	Zones, conduits and every link with protocol, direction, rate and control	Know which ports, buses and services exist before you scan, so findings can be explained

How to use it

STEP 1 · CONFIRM SCOPE

Check the readiness report: product variant, firmware build and hardware revision. If the decision is no-go, the gap list tells you what is outstanding, so the slot can be moved once rather than lost.

STEP 2 · PLAN FROM THE RTM

Use the matrix as the test plan. Each row names the requirement, the design element and the test, so coverage is visible before testing starts.

STEP 3 · PULL WHAT YOU NEED

Query the evidence pack by component, requirement or test. SBOM entries, crypto keys, drawings and interface details come from one place, with no request to engineering and no wait.

STEP 4 · TEST AND RECORD

Run each bench test to its procedure and record the result against its RTM row. A failed or partial result is a gap with an owner, not an email thread.

STEP 5 · CONFIRM THE TRACE

When every row traces to evidence, the matrix is the summary of your assessment. For self-assessment it supports the manufacturer's declaration; for a notified body it is the record you review or witness.

What you will not have to do

WITHOUT A UNIFIED MODEL	WITH Eigenia
Chase engineering for the right SBOM version or firmware build	The variant under test is fixed in the readiness report and the files match it
Reconcile BOMs, drawings and test reports that disagree	All files are generated from one model, so they agree by construction
Triage a raw CVE list with no product context	Findings arrive ranked by EPSS, KEV status and reachability
Discover missing evidence half-way through a slot	Gaps are found and assigned before the product reaches the bench
Rebuild the evidence pack for the next product revision	The pack regenerates from the model when the product changes

Why use Eigenia

A test bench runs on schedule, and its most expensive failure is an idle slot. Eigenia addresses the causes directly: products that arrive unready, evidence that has to be requested, and files that do not agree. The readiness review catches the first, the pull model removes the second, and the unified DEXPI and CycloneDX record removes the third.

FOR LABORATORIES AND NOTIFIED BODIES

A consistent pack structure across every Eigenia-prepared product means your team learns it once. Evidence is labelled, current and traceable, so assessor time goes on testing and judgement rather than on finding and reconciling documents.

FOR MANUFACTURERS

Fewer failed or rescheduled slots, a clear go / no-go before money is committed to a lab, and an evidence record that carries forward into the technical file and post-market support.

14 The technical file, compiled

Before CE marking, the manufacturer must hold technical documentation: a description of the product and its architecture, the cybersecurity risk assessment, the bills of materials, test results, and the vulnerability-handling arrangements for the support period. In most organisations these live in different places and are reconciled by hand before an audit.

In the twin they are views of the same record. The architecture comes from the system records, the risk assessment from the threat trees and CVE cross-reference, the test results from the bench and the RTM, the BOMs from the CycloneDX layer, and the update plan from the firmware and key-management records. When a component changes, every document that mentions it changes with it.

WHY THIS MATTERS

The CRA applies in full from 11 December 2027. A manufacturer that can regenerate its technical file from one model on demand is in a different position from one that rebuilds it by hand for each audit and each product revision.

15 What this gives the manufacturer

TEAM	WHAT THEY GET
Executives and compliance	A defensible position on CRA obligations, with evidence for each requirement and a clear view of where the gaps are
Engineering	Their own architecture, buses and firmware, modelled closely enough to trust the conclusions
Product security (PSIRT)	A disclosure answered in minutes: affected or not, exposed or not, and a pre-filled early warning
Procurement and supply chain	Provenance and choke points by tier, and the evidence export control needs
Notified bodies and auditors	A technical file that is current, machine-readable and traceable to the product

Beyond drones

The same structure applies to any product with digital elements: satellites such as LEO-RSAT-001, industrial controllers, robots, medical devices, connected vehicles. The components and the rules change; the method of holding product, supply chain and evidence in one model does not.

NEXT STEP

A product's design documents and existing bills of materials are enough to begin. On a client engagement Eigenia builds the twin from controlled engineering data, and the result is a very high-fidelity model held under the client's control.

NO WARRANTY

This case study and the model it describes are representational, built only from open-source intelligence and engineering judgement, and provided for illustration and education without warranty. They make no declaration that any figure, component, configuration or finding is correct for Project Quiver, the Crazyflie, or any product built from them. Product and project names describe publicly documented equipment and imply no endorsement by or of their owners. Regulatory summaries are not legal advice; CRA classification must be confirmed for each product.