

E I G E N I A B . V .

Cyber Digital Twin · Fail Fast, Fail Safe

Product security and compliance, built on a Cyber Digital Twin

Shown on Project Quiver, an open-source drone ecosystem: the CRA and compliance in other markets, the chain of trust, and preparation for the test bench.

FOR Manufacturers Test benches Distributors and resellers

Integrators Buyers

01

The platform

Eight layers, one model

02

The example

Nine system records, eight zones

03

Compliance

CRA, RED, PSTI, IEC 62443

04

Chain of trust

Suppliers to buyers

Electronics

Platform

61%

Wire

Zone

Wire

Interface

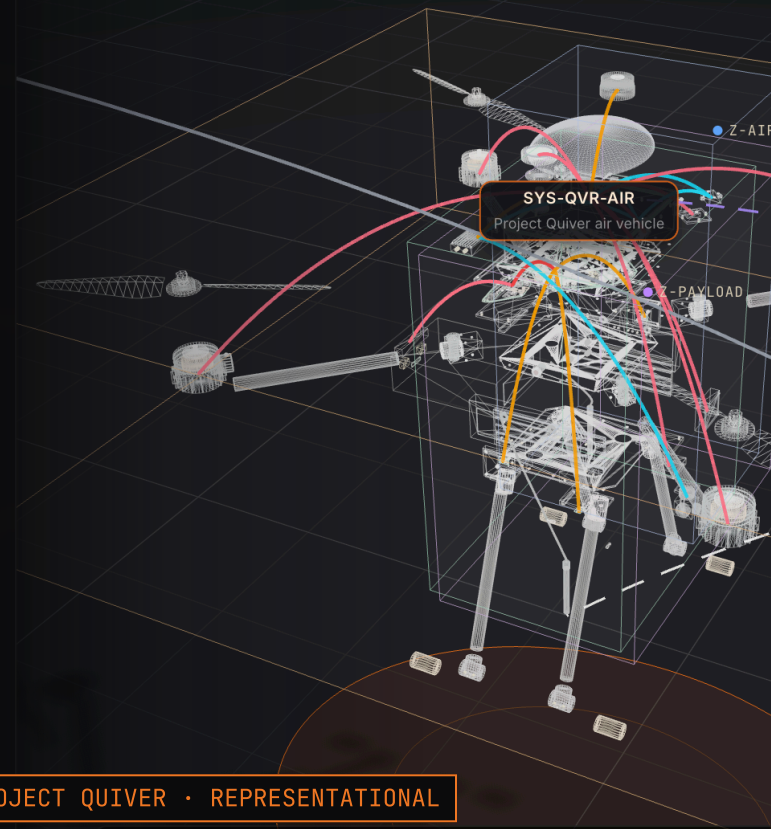
is

action

et

PROJECT QUIVER · REPRESENTATIONAL

○ Z-AIR-ACT ○ Z-AIR-COMMS ○ Z-AIR-FLIGHT ○ Z-DMZ ○ Z-ENTERPRISE



THE CYBER DIGITAL TWIN · ONE MODEL, EIGHT LAYERS

One Model. Eight layers, each answering a question about the Product

LAYER		THE QUESTION IT ANSWERS	IN THE DRONE SYSTEM	CHANGES
L1	Equipment catalogue	What should exist, by design and reference model?	Project Quiver BOM: 143 items, 297 PCB parts	Rarely
L2	Customer equipment	What actually exists, where, in what condition?	As-built airframe, ground segment, maintenance bench	Months
L3	Bills of materials	What software, hardware and crypto is inside?	ArduPilot, Pi 5 OS, CubeNode and HM30 firmware	Hours
L4	Threat intelligence	Who is attacking configurations of this kind?	Actors targeting drones and their ground links	Days
L5	Psychology	How will the people who run it behave?	Pilot, maintainer and provisioning practices	Months
L6	Information streams	What is happening now that changes the risk?	Export controls, sanctions, supplier disclosures	Hours
L7	Economic and actuarial	What would a failure cost; what is rational to spend?	Recall, field fixes, market access, liability	Quarterly
L8	Predictions	What happens next, how likely, what to do?	Breach likelihood, remediation priorities	On re-run

L1 vs L2 · drawn versus as-is. The gap is computed, not assumed.

ATQ · scores likely actors and capability from L4 to L6.

TACAM · traverses L1 to L4, writes cost and outcome into L7 and L8.

THE PRODUCT TWIN • FULL ENROLMENT DEPTH

The drone system: how far down the model goes

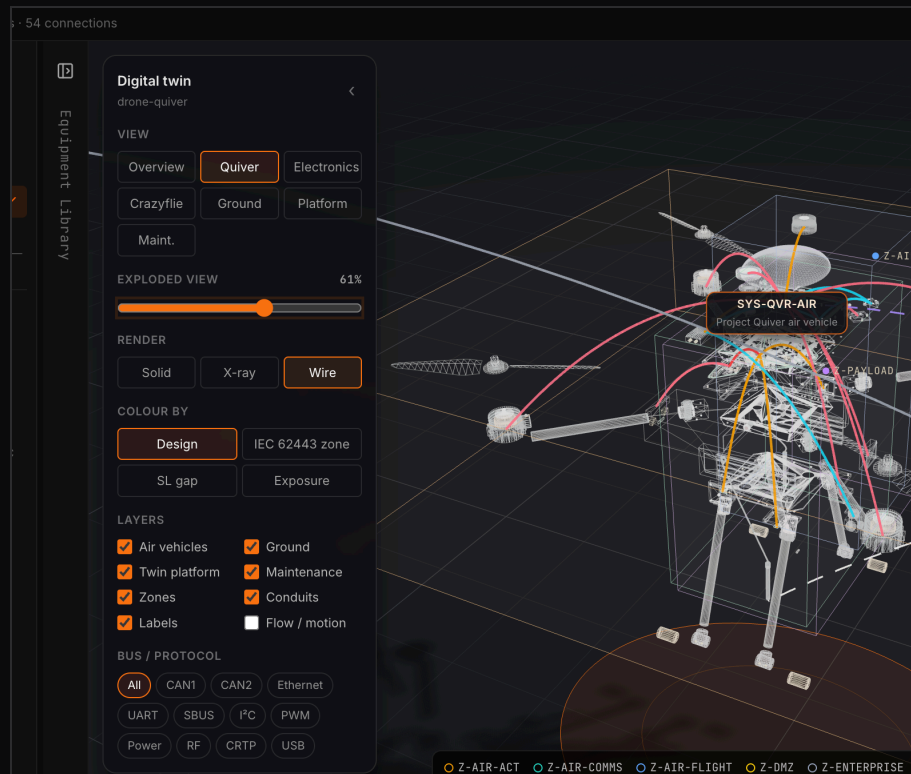
L1 System and mission

L2 Subsystems and interfaces

L3 Components and suppliers

L4 Firmware, SBOM, crypto

L5 Failure modes and test evidence



163

assets

54

connections

165

CVEs traced

Asset register

SBOM and HBOM basis

Connection register

Interface control evidence

Zones and conduits

Where an attack can enter

Security level rationale

SL-T per zone, for the technical file

Envelope map

Supplier and chain-of-trust map

Threat pathways

Attack scenarios for the test bench

Cascading failures

Failure cascades in the intended use

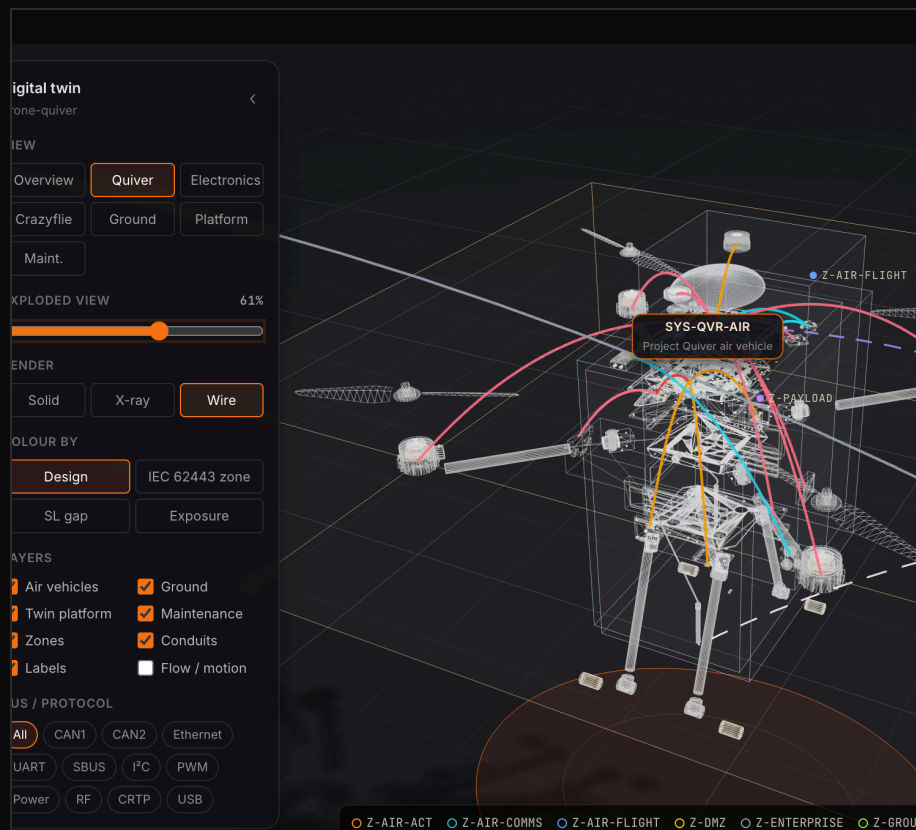
Risk portfolio

Prioritised remediation

Assumptions, provenance

Provenance for auditors and buyers

Project Quiver built as a Cyber Digital Twin from open-source information



9

system records

143

BOM items

297

PCB components

135

harness wires

34 · 58

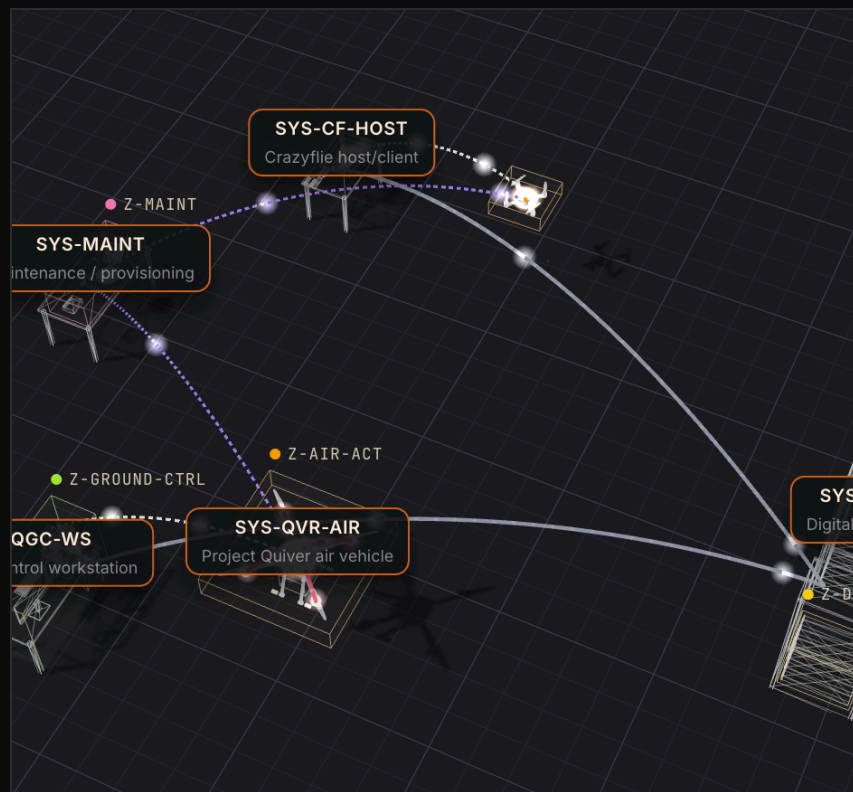
interfaces · sub-
interfaces

45

failure modes, 10
attacker-
triggerable

Representational only. Public sources and engineering judgement; firmware unpinned, geometry procedural, no hardware tested. Client engagements use controlled engineering data and stay under the client's control.

A system of systems, not a single airframe



Each record is a node with its zone volume; conduits run between them.

SYS-QVR-AIR	Air vehicle Pix32 v6, ArduPilot, Raspberry Pi 5
SYS-HM30-AIR	Airborne link RC, MAVLink and video on one radio
SYS-MK32-GCS	Ground controller SIYI MK32 handheld
SYS-QGC-WS	Operator workstation QGroundControl
SYS-CF21-AIR	Air vehicle Crazyflie 2.1
SYS-CRADIO	Radio gateway Crazyradio 2.0 USB
SYS-CF-HOST	Operator workstation cfclient / cflib host
SYS-DT-PLAT	Twin platform DMZ broker, asset graph, stores
SYS-MAINT	Maintenance debug probe, provisioning laptop

Every value marked reported, from a cited source, or assumed.

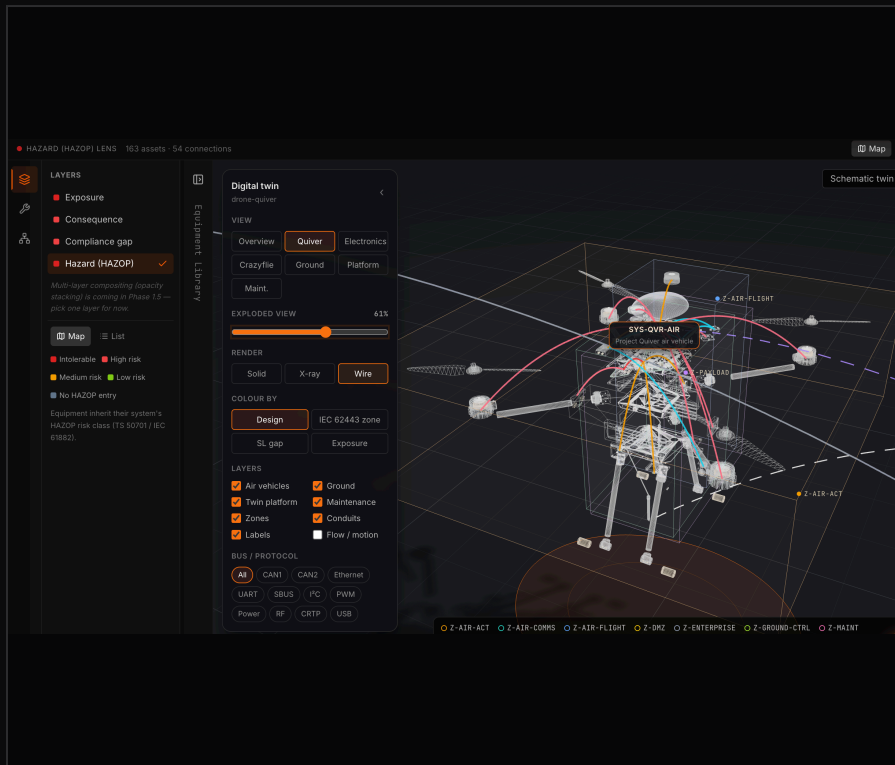
Each phase produces part of the CRA technical file

PHASE	IN THE DRONE EXAMPLE	CRA EVIDENCE
1 Scope and classify	Nine system records inventoried	Classification record; product description
2 Risk assessment	Eight zones, SL-T per requirement; 45 failure modes, five fault trees	The cybersecurity risk assessment
3 Requirements, design	34 interfaces and 58 sub-interfaces typed to security level	Annex I mapped to 62443; traceability rows
4 Secure development	CycloneDX 1.6 SBOM, 19 components; HBOM from 143 items	Vulnerability handling; update plan
5 ALARP review	SL-C against SL-T per sub-interface; cascades per failure mode	Residual risk argument
6 Test-bench handover	Frozen dossier, test scope, API access	Test results; declaration readiness

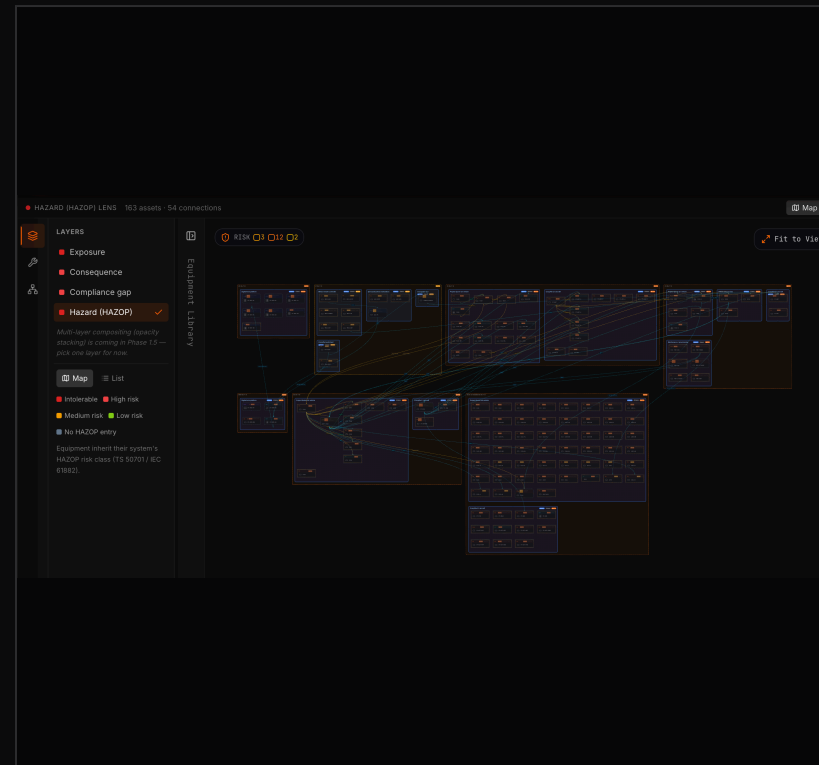
Phases 1–4 follow IEC 62443 (3-2, 3-3, 4-1, 4-2). Phases 5 and 6 are Eigenia additions.

Every asset, zone and conduit, with its hazard class

PLATFORM VIEW



3D twin. Exploded wire view, coloured by design, IEC 62443 zone, SL gap or exposure; filtered by bus and protocol.



HAZOP lens. 163 assets and 54 connections, each carrying its system's HAZOP risk class (TS 50701 / IEC 61882).

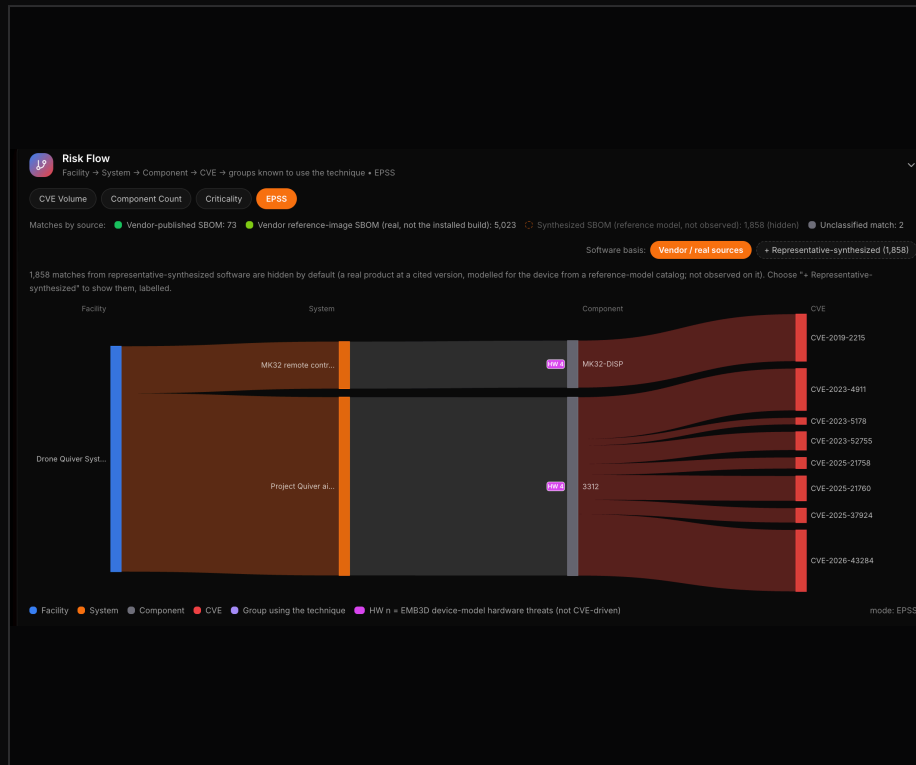
Eight zones, from flight control to maintenance

ZONE	CONTAINS	WHY IT IS SEPARATE
Z-AIR-FLIGHT	Pix32 v6, FC PCB, GNSS, LiDAR, radars	Flight control integrity and availability
Z-AIR-ACT	Battery, BC PCB, X6 Plus motors and ESCs	Prevent unsafe actuation; keep a safe state
Z-AIR-COMMS	HM30 air unit, CubeNode ETH, switches, Remote ID	Terminates every externally exposed conduit
Z-PAYLOAD	Raspberry Pi 5, A8 mini camera	Potentially lower-trust applications
Z-GROUND-CTRL	MK32, QGroundControl, cfclient, Crazyradio	Holds operator authority and credentials
Z-DMZ · Z-ENTERPRISE	Twin integration DMZ; twin services	Separates operational from enterprise data
Z-MAINT	Debug probe, provisioning laptop	Privileged cross-zone capability

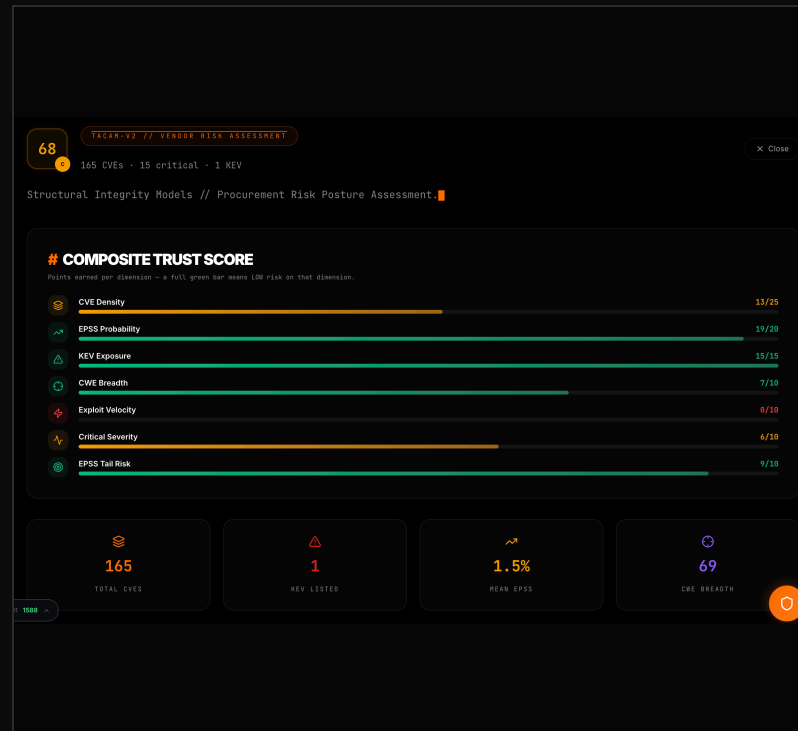
The same workshops, zone and conduit method apply to a single product, a facility or a whole organisation.

From product to component to CVE to the threat actors that exploit it

PLATFORM VIEW



Risk flow. Facility → system → component → CVE, weighted by EPSS. Matches are split by source: vendor SBOM, reference image or synthesised, and labelled.



TACAM vendor assessment. Composite trust score from CVE density, EPSS, KEV exposure, CWE breadth, exploit velocity and tail risk.

Where the facility's partners sit, and which rules apply to them

PLATFORM VIEW



FLEET FACILITIES (1) SUPPLY CHAIN FLOW-DOWN (36) STRATEGIC CORRIDORS (3) GLOBAL ATLAS (250)									
STATUTORY ROADMAP & TIMELINES									
Compare Tour									
Search OEM, partner, category.. All Downstream / value chain Upstream - tier 1 Upstream - tier 2									
PARTNER / DEN	CATEGORY	TIER	FLOW DIRECTION	HOST NATION	COUNTRY STATUTE	COUNTRY PATCH SLA	ACTIONS		
Survey, construction and asset inspection operators (commercial specific-category) country-level (no researched site)	Downstream / value chain	Tier 1	Downstream	GBR United Kingdom	PRA PS7/26 and FCA PS26/2 (operational incident and third-party reporting)	14d	Inspect Host		
Public-safety agencies and delivery/logistics trials (heavy-lift) country-level (no researched site)	Downstream / value chain	Tier 1	Downstream	USA United States	NRC 10 CFR 73.54	unknown	Inspect Host		
University and research labs (Bitcraze Crazyflie nano-drones, indoor swarm and autonomy research) country-level (no researched site)	Downstream / value chain	Tier 1	Downstream	USA United States	NRC 10 CFR 73.54	unknown	Inspect Host		
Public-safety and emergency-services operators (search and rescue, fire, incident overwatch) using a heavy-lift multirotor country-level (no researched site)	Downstream / value chain	Tier 1	Downstream	NLD Netherlands	Cyberbeveiligingswet	unknown	Inspect Host		
Infrastructure inspection and research users in an Asian market country-level (no researched site)	Downstream / value chain	Tier 1	Downstream	JPN Japan	unknown	unknown	Inspect Host		
Infrastructure inspection: energy and utilities (power-line and pipeline linear inspection) country-level (no researched site)	Downstream / value chain	Tier 1	Downstream	DEU Germany	unknown	unknown	Inspect Host		

Global atlas. Facilities, partners and strategic corridors, with countries shaded by exposure.

Supply chain flow-down. Partners by tier and direction, host nation, country statute and patch SLA. Unknowns are shown as unknown.

The CRA turns product security into evidence, product by product

11 SEP 2026 · NOW IN FORCE

Article 14 reporting: actively exploited vulnerabilities and severe incidents, early warning within 24 hours

A MANUFACTURER HAS TO SHOW

The product is secure by design

It knows every component inside it

It can report an exploited vulnerability within 24 hours

11 DEC 2027 · FULL APPLICATION

CE marking requires demonstrated conformity for products with digital elements

FOR EVERY PRODUCT, AND EVERY NEW VERSION

Risk assessment	SBOM
Technical file	Conformity route
Eigenia builds the product as a twin first, so these become questions the model answers, not spreadsheets assembled before an audit.	

What the CRA asks of a manufacturer, in detail

CLASS SETS THE ROUTE

- Default** · self-assessment (module A)
- Important class I** · self-assessment if harmonised standards applied; otherwise third party
- Important class II** · third-party assessment (modules B+C or H)
- Critical** · European certification where required

ESSENTIAL REQUIREMENTS · ANNEX I

- Part I** · secure by default, no known exploitable vulnerabilities, access control, confidentiality and integrity, data minimisation, attack-surface limits, logging, security updates
- Part II** · SBOM, vulnerability handling and testing, coordinated disclosure policy, free security updates

REPORTING · ARTICLE 14

- 24 h** Early warning
 - 72 h** Notification with details
 - 14 days** Final report, after a fix is available
 - 1 month** Final report on a severe incident
- Via the ENISA single reporting platform

Support period At least five years, unless expected use is shorter	Technical file Kept ten years after market placement	Importers, distributors Must verify CE marking and documentation	Penalties Up to €15m or 2.5% of worldwide turnover
--	--	--	--

In the drone example: classification is left open for a representational product; the twin holds the reasoning, the SBOM and the Article 14 contact path for when it is decided.

Cybersecurity for radio equipment, applicable since 1 August 2025

Article 3(3)(d) · Network

Equipment must not harm the network or its operation, or misuse network resources

Article 3(3)(e) · Privacy

Safeguards to protect personal data and privacy of users

Article 3(3)(f) · Fraud

Features that protect against fraud, for equipment that transfers money or value

SCOPE

Radio equipment that can communicate over the internet, directly or through other equipment

Also childcare, toys and wearables that process personal data

Applies alongside, and ahead of, the CRA

HOW CONFORMITY IS SHOWN

EN 18031-1, -2, -3 · harmonised standards for (d), (e) and (f)

Self-assessment · when the standards are applied in full

Notified body · where a standard is not applied or a restriction applies

In the drone example: the HM30 air link, the Crazyradio dongle, Remote ID and the Raspberry Pi network interfaces are the radio and network paths the twin maps against (d) and (e).

Three baseline requirements for consumer connectable products, in force since 29 April 2024

No universal default passwords Each device has a unique password, or the user sets one	Vulnerability disclosure A published point of contact and how reports are handled	Security update period The minimum period of security updates, stated at sale
--	---	---

WHO CARRIES DUTIES

- Manufacturers** · meet the requirements; issue a statement of compliance
- Importers** · check compliance and the statement before sale
- Distributors** · do not supply products they know do not comply

ENFORCEMENT

- Regulator** · Office for Product Safety and Standards
- Penalties** · up to £10m or 4% of worldwide revenue
- Scope** · consumer products; exemptions include products covered by other regimes

In the drone example: credentials on the MK32 controller and QGroundControl workstation, the disclosure contact and the stated support period are records in the twin.

Four parts carry the product work

3-2 · Risk assessment Zones and conduits; target security level (SL-T) per zone	3-3 · System requirements Requirements and security levels for the system	4-1 · Secure lifecycle Eight practices, from requirements to update management	4-2 · Component requirements Embedded, host, network and software application devices
---	---	--	---

SEVEN FOUNDATIONAL REQUIREMENTS · SECURITY LEVELS 1 TO 4

FR1 Identification, authentication	FR2 Use control	FR3 System integrity	FR4 Data confidentiality	FR5 Restricted data flow	FR6 Timely response	FR7 Resource availability
--	---------------------------	--------------------------------	------------------------------------	------------------------------------	-------------------------------	-------------------------------------

SL 1 · casual or accidental **SL 2** · simple means, low skill **SL 3** · sophisticated, IACS skills **SL 4** · extended resources

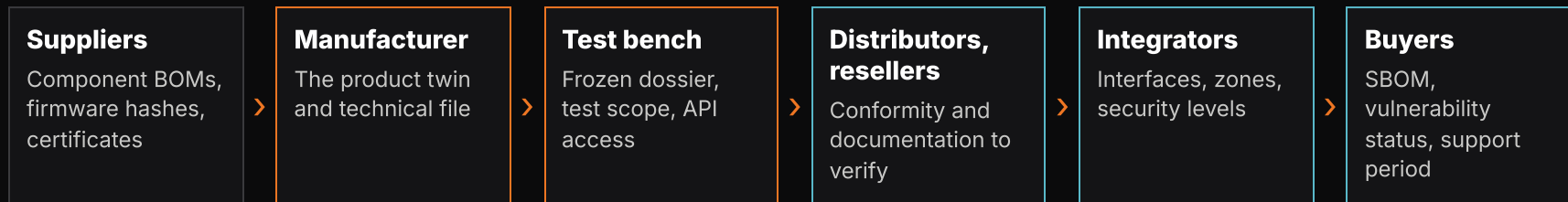
In the drone example: SL-T is set per zone and foundational requirement; SL-C is estimated per sub-interface; every gap between them is listed for the ALARP review and the test bench.

One product model, evidence for each market it is sold into

REGIME OR STANDARD	SCOPE	WHAT THE MODEL SUPPLIES
EU · Cyber Resilience Act	Products with digital elements, CE marking	Risk assessment, SBOM, technical file, Article 14 readiness
EU · Radio Equipment Directive	Delegated act on cybersecurity for radio equipment	Radio interfaces, network protection, data and fraud safeguards
EU · UAS regulations	Drone product requirements, including Remote ID	Remote ID module, its interfaces and failure modes
UK · PSTI Act	Security of connectable consumer products	Credentials, vulnerability disclosure, support period
US · FCC Cyber Trust Mark	Voluntary labelling for connected devices	Component inventory, update mechanism, support period
IEC 62443-4-1 · 4-2	Secure lifecycle and component requirements	Zones, SL-T and SL-C per sub-interface, lifecycle evidence

Obligations differ by market and product class; each engagement confirms which apply.

Everyone who handles the product can check the same evidence



Upstream

Supplier data enters with source and date, and is checked against the BOM.

At the bench

Testing starts from a known scope, not from a document hunt.

Downstream

Each party sees the view it needs, traced to the same records.

One product model, and the CRA evidence drawn from it

Risk assessment

Zones, conduits and target security levels, in the intended use

SBOM · HBOM · CBOM

CycloneDX 1.6, to five or more dependency levels

Traceability matrix

CRA Annex I mapped to IEC 62443-4-2 requirements

Vulnerability handling

CVE, KEV and EPSS on every component;
Article 14 readiness

Residual risk argument

ALARP review recorded in the technical file

Test-bench handover

Frozen dossier, test scope and API access

Shared with test benches, distributors, integrators and buyers, each with the view they need.
Next step: a 30-minute scoping call on one product.

Jim McKenney, Founder
EIGENIA B.V. · jim@eigenia.nl

SOURCES

Sources for the product example

Arrow-air Project Quiver

Open-source repository: bill of materials, PCB production files, harness guide

Bitcraze Crazyflie 2.1

Datasheets and documentation for the nano-drone stack

ArduPilot, QGroundControl, vendor manuals

Flight stack, ground control and component documentation

Regulation (EU) 2024/2847

Cyber Resilience Act, including Article 14 reporting obligations

IEC 62443-3-2, 3-3, 4-1, 4-2

Zones and conduits, system and component requirements, secure lifecycle

Eigenia Drone CRA Case Study v2

The representational model this section is drawn from

Representational example built from public sources and engineering judgement. It makes no claim about the security or compliance of Project Quiver or any product built from it.