

E I G E N I A B . V .

Cyber Digital Twin · Fail Fast, Fail Safe

CASE STUDY · CRA COMPLIANCE · OPEN-SOURCE RESEARCH MODEL

An open-source farming robot, modelled as a Cyber Digital Twin for the Cyber Resilience Act

From aluminium extrusion to CE mark: one model that holds the machine, its software, its supply chain and its compliance evidence.

Product

FarmBot Genesis v1.8, 1.5 m × 3 m

Design source

FarmBot public CAD (CC0) and repositories

Regulation

(EU)
2024/2847

01

Summary

A manufacturer of a connected machine has to prove, product by product, that what it places on the market 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 shows how a Cyber Digital Twin turns those obligations into something the manufacturer can query, rather than a set of spreadsheets assembled before an audit.

The model represents FarmBot Genesis, an open-source CNC farming robot, as a manufactured product with digital elements. It is a compliance and provenance model with a simulated controller. It is not connected to a live machine, and no command is ever sent to real hardware.

12 system records: 9 hardware, 3 software	1,105 named parts in the 3D model	5 bills of materials: SBOM, HBOM, CBOM, MBOM, OBOM
10 interfaces typed end to end, with 13 cables and hoses traced	12 controller I/O signals mapped to pins	24 h early-warning window the model is built to meet

APPROACH — OPEN-SOURCE RESEARCH

This model was built from open-source, publicly available information: the FarmBot Genesis v1.8 documentation and bill of materials, the published product specifications, the CC0-licensed CAD models, and the FarmBot OS, Arduino firmware and Web App repositories. It was produced independently of FarmBot Inc. and does not represent the company's configuration, test results or compliance status.

02

The product

FarmBot Genesis is a gantry robot that runs on aluminium tracks along a raised bed. It covers a 1.5 m × 3 m area, and a Universal Tool Mount lets it swap between a watering nozzle, a seeder, a weeder and a soil sensor. Four NEMA 17 stepper motors with rotary encoders drive three axes. A Farmduino microcontroller runs the motors and peripherals, and a Raspberry Pi running FarmBot OS connects the machine to the FarmBot Web App. Kits are sold to homes, schools and research labs. A connected product with software, sold commercially, falls within the Cyber Resilience Act.

SYSTEM RECORD	SUBSYSTEM	CORE COMPONENTS
FBG-SYS-001	Track assembly	Aluminium extrusion tracks, 3 m; GT2 belts fixed at each end
FBG-SYS-002	Gantry	Two columns on V-wheel plates with eccentric spacers; two X motors; 1.5 m main beam
FBG-SYS-003	Cross-slide	Y motor and V-wheels on the main beam; Z lead-nut block; vacuum pump in v1.8
FBG-SYS-004	Z axis	Z extrusion, NEMA 17 motor, 8 mm stainless lead screw
FBG-SYS-005	Universal Tool Mount	12 gold-plated pogo pins, three liquid/gas lines, magnetic coupling, USB camera
FBG-SYS-006	Interchangeable tools	Watering nozzle, seeder, weeder, soil sensor; toolbays and seed trough
FBG-SYS-007	Water circuit	24 V normally-closed solenoid valve, garden-hose inlet, tubing to the UTM
FBG-SYS-008	Farmduino	Farmduino v1.6, ATmega2560, five TMC2130 drivers, encoder co-processor, five 24 V outputs; 100 W IP67 supply
FBG-SYS-009	Raspberry Pi edge computer	Raspberry Pi 4B, 1 GB, Wi-Fi and Ethernet
FBG-SYS-010	FarmBot OS	Runs sequences on the Pi and sends G- and F-codes to the Farmduino over USB serial
FBG-SYS-011	Web App	Cloud application for sequences, farm design, tools and sensor data
FBG-SYS-012	Operator browser	The user's browser session to the Web App

Each system record is an independent node in the twin. It carries its own bill-of-materials fragments, source documentation, configuration and the buses, cables and hoses that connect it to its neighbours.

03

Why this matters now

Connected machines that move, switch power and handle water are reaching households, classrooms and labs. They now meet several EU regimes at once. The dates that shape the work:

SIGNAL	WHAT IT MEANS FOR A CONNECTED FARMING ROBOT
CRA in force	Regulation (EU) 2024/2847 entered into force on 10 December 2024 and covers products with digital elements made available on the EU market
Reporting from 2026	Article 14 reporting of actively exploited vulnerabilities and severe incidents applies from 11 September 2026
Full application	All CRA obligations, including conformity assessment and CE marking, apply from 11 December 2027
Radio equipment	The RED delegated act (EU) 2022/30 has applied cybersecurity requirements to internet-connected radio equipment, such as a Wi-Fi-enabled controller, since 1 August 2025
Machinery	The Machinery Regulation (EU) 2023/1230 applies from 20 January 2027 and addresses corruption and safety-related control functions in machinery
Open-source design	A public, CC0 design does not remove manufacturer obligations: the party that sells the product commercially carries them

Dates are taken from the regulations as published. Confirm each against EUR-Lex and any implementing acts before relying on them.

The squeeze on an open-source hardware maker

An open-source maker carries two obligations at once. Its community expects frequent software releases and open designs. Its commercial kits, sold into the EU, bring the product under the CRA, and the radio and machinery rules apply to the same machine. Every software release changes the software bill of materials, and every hardware revision changes the parts list.

WHERE THE TWIN FITS

Fast releases and formal compliance usually pull against each other: every new release means a new SBOM, a new risk assessment and new test evidence. When those are generated from one model, a release is a change to the model rather than a new compliance project, and the evidence for CRA, RED and machinery obligations comes from the same record.

The same six-phase method

This product model was built with the same six-phase EIGENIA readiness method used for facility-scale twins such as the hyperscale AI data centre. 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 FARMBOT	FEEDS THE CRA EVIDENCE
1 • Scope and classify	Confirm CRA scope and exclusions, core functionality, class, conformity route and support period	Robot, Farmduino and Pi scoped as a product with digital elements; Web App assessed as remote data processing; class and route recorded with reasoning; twelve system records and 1,105 parts inventoried	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)	Five zones from physical process to external services, four conduits, SL-T per zone; nine threat scenarios with physical consequences (unexpected motion, overwatering, misleading state)	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	Ten interfaces and 13 cables and hoses typed with protocol, direction and rate; 12 controller I/O signals mapped; each requirement a row in the RTM	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)	Five CycloneDX BOMs; FarmBot OS, firmware and Web App releases to pin; update signing to evidence; 24 h early-warning drill	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	SL-C agreed against SL-T; unauthenticated serial control weighed against command allowlisting, E-stop and fail-closed valve; failing gaps return to phase 3	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	Twin package frozen and hashed (SHA-256 manifest); safe test plan for motion tests; open items listed, not hidden	RTM, test results, declaration readiness

Zones inside the product

Zones and conduits are not only a facility idea. Inside the machine the same partitioning applies, and it is what makes the separation between the network-facing computer and the controller that moves the motors auditable.

ZONE	CONTAINS	CONDUITS OUT	WHY IT IS SEPARATE
Z0 · Physical process and safety	Motors, belts, lead screw, tools, solenoid valve, vacuum pump, E-stop	C01 to the controller: defined signals only	Where a cyber event becomes motion, water or force; protective functions must hold if everything above fails
Z1 · Embedded control	Farmduino, TMC2130 drivers, encoder co-processor	C02 to the Pi: USB serial	Deterministic control of motors and peripherals; small attack surface but no authentication on its command input
Z2 · Edge and operator	Raspberry Pi, FarmBot OS, USB camera	C03 to the twin gateway; Wi-Fi or Ethernet to the cloud	Network-facing Linux computer with the largest software estate; must not be able to bypass limits in Z1
Z3 · Twin integration	EIGENIA gateway, broker, model and telemetry services	C04 to external services	Read-only by default; any twin-to-machine command needs allowlisting, authorisation and interlocks
Z4 · External services	Web App, release repositories, update and remote access	Internet	Outside the operator's control; treated as untrusted

ONE METHOD, TWO SCALES

A customer that has seen the method on a facility recognises it on a product, and the reverse. The same workshops, the same zone and conduit reasoning and the same evidence discipline serve a hyperscale campus, a greenhouse or a single farming robot, and a product twin can later sit inside a facility twin as one of its assets.

05

Inside the machine

FarmBot keeps a network-facing computer and a motion controller on separate boards joined by one USB serial link. That link is the most important security boundary in the design: whatever reaches it can move the machine. The twin models it, and every other connection, link by link.

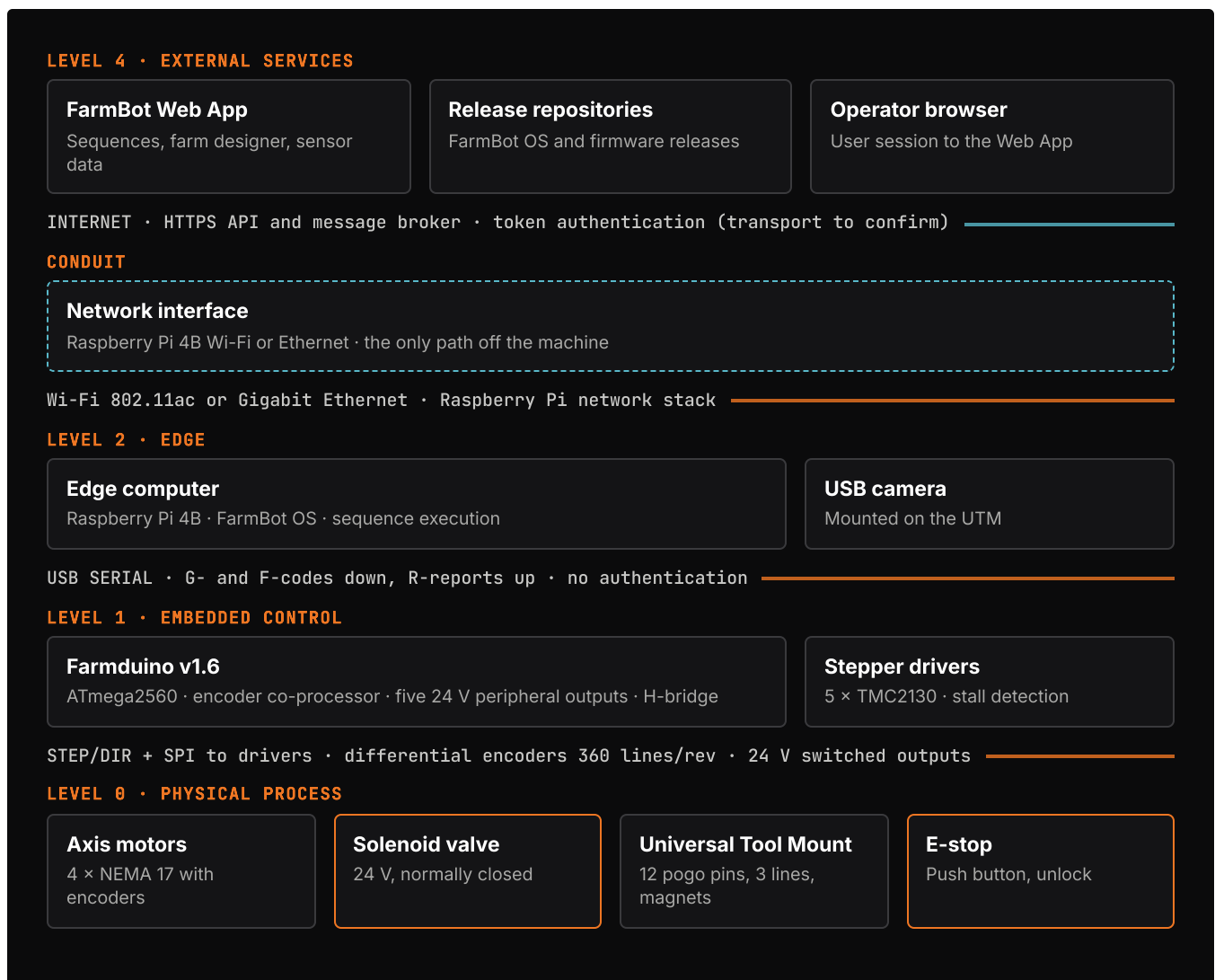


Figure 1. Control architecture by Purdue level, drawn from the model. Orange boxes are protective functions that hold when software fails; the dashed box is the network conduit leaving the machine.

Every link, typed

The twin records each interface with its protocol, direction, rate and the control that protects it. A selection of the most security-relevant links:

LINK	PROTOCOL	DIRECTION · RATE	CONTROL
Pi ↔ Farmduino	G/F-codes over USB serial	Two-way · per command	None on the link; queue numbers only
Farmduino → stepper drivers	Step/dir, SPI configuration	One-way · per step	Driver stall detection
Encoders → Farmduino	Differential quadrature, 360 lines/rev	One-way · continuous	Closed-loop check for missed steps
Farmduino → solenoid valve	24 V switched output, pin 8	One-way · on command	Valve fails closed on power loss
Farmduino → vacuum pump	24 V switched output, pin 9	One-way · on command	Load sense on an analog input
UTM → Farmduino (tool check)	Digital input with pull-up, pin 63	One-way · on read	Reads 0 with a tool, 1 without
UTM → Farmduino (soil sensor)	Analog input, pin 59	One-way · on read	Plausibility range ~250 dry to ~850 wet
Pi ↔ Web App	HTTPS API and message broker	Two-way · event-driven	Token authentication; TLS to confirm

WHY THIS MATTERS FOR THE CRA

The serial link is where an injected command would become physical motion or an open valve. Because the twin holds the link, its protocol and its exposure, it can answer "who can reach it and what happens if they do?" for this product configuration, not for Linux or Arduino in general.

Five bills of materials, one record

The model holds CycloneDX bills of materials, extended beyond software to hardware, cryptography, a machine BOM and an operations BOM, alongside DEXPI engineering data derived from the design. Each entry links to the system record it belongs to. The three below carry most of the CRA weight.

BOM	WHAT IT RECORDS	WHY IT MATTERS FOR THE CRA
SBOM	FarmBot OS, Farmduino firmware, Web App and their dependencies with versions, package URLs and licences. Currently 12 system-level entries, pending pinned releases	The manufacturer must know every component and handle its vulnerabilities, including open-source code it did not write
HBOM	295 part types and 1,105 placed parts, from the published BOM: NEMA 17 motors, encoders, Farmduino, Raspberry Pi, valve, extrusions and fasteners	Provenance and substitution risk, and the vendor behind each part
CBOM	Keys, tokens and algorithms: Web App API tokens, TLS to the cloud, Wi-Fi credentials stored on the Pi, update verification (to evidence)	Confidentiality and integrity claims become checkable, and crypto agility can be planned

07

Supply chain, tier by tier

Compliance and resilience both depend on knowing where each part comes from. The twin maps the chain from the kit to the main component vendors and marks the choke points.

TIER	SUPPLIER AND LOCATION	ROLE	EXPOSURE
1	FarmBot Inc., California (US)	Designer and kit seller; manufacturer of record for the EU	Non-EU manufacturer: needs an EU importer or authorised representative
2	Raspberry Pi Ltd, Cambridge (UK)	Edge computer	UK origin; single-board computer supply
3	Microchip Technology, Chandler (US)	ATmega2560 microcontroller on the Farmduino	US jurisdiction
3	Trinamic (Analog Devices), Hamburg (DE)	TMC2130 stepper driver ICs	EU domestic silicon design
2	LDO Motors (CN)	NEMA 17 stepper motors	Single-source motor family
2	Honest Sensor (vendor of record)	Rotary encoders	Location to confirm
2	Extrusion, plate and ABS moulding vendors	Structure and plastic parts	To map from purchasing records

Vendors come from FarmBot's published BOM and public company information. Locations and tiers must be confirmed against the manufacturer's purchasing records before they support any claim.

08

From vulnerability to report

The model links each software component to the system that carries it and 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. For FarmBot, matching starts when versions are pinned.

COMPONENT	SOURCE	EXPOSURE	STATUS IN THE MODEL
FarmBot OS and its Linux base	farmbot_os repository	Network-facing	Version unpinned. CVE matching waits for the release hash
Erlang/OTP and Elixir dependencies	farmbot_os lock files	Network-facing	Dependency list to extract from the pinned release
Farmduino firmware	farmbot-arduino-firmware repository	Serial only	Version unpinned. Reachable only through the Pi
Web App and its dependencies	Farmbot-Web-App repository	Internet	Assessed as remote data processing; versions unpinned
TLS and crypto libraries	SBOM after pinning	Network-facing	Feeds the CBOM once versions are known

No CVEs are recorded against FarmBot in this model. The absence reflects unpinned versions, not a clean result.

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.

T + 24 H Early warning 	T + 72 H Notification 	FINAL Final report 	MODEL Pre-filled 
---	--	--	---

Because the affected component, software releases, hardware revision and mitigation status sit in the model, the early-warning payload can be assembled in minutes. The hard part of meeting 24 hours is knowing what you shipped, and that is what the twin holds.

How an adversary would attack it

A machine that moves and switches water has to be assessed for what an attacker can make it do, not only for what they can read. The twin carries two threat trees mapped to MITRE ATT&CK for ICS, each linked to the components it targets and the countermeasures that answer it.

Unauthorised actuation through the edge computer

T0855 • T0831

1. An attacker gains code execution on the Raspberry Pi, through the network or a stolen account token.
2. They open the serial port and send G00 moves and F41 pin writes directly to the Farmduino.
3. The gantry drives outside its sequence and the water valve is held open.

COUNTERMEASURES

- Command allowlisting and rate limits in FarmBot OS before the serial port
- Encoder stall detection and the hardware E-stop
- Normally-closed valve; twin flags motion outside any scheduled sequence

Firmware substitution and false reporting

T0839 • T0843 • T0856

1. A tampered update or a local flash replaces the Farmduino firmware.
2. The new firmware ignores axis limits or peripheral timeouts.
3. Spoofed position reports (R82) tell the operator and the twin all is normal.

COUNTERMEASURES

- Signed updates with verification before flashing (to evidence)
- Firmware hash recorded in the SBOM and checked at boot
- Camera position and encoder counts cross-checked against reports

Both trees end in a physical control rather than a software one. That is deliberate: once an attacker holds the edge computer, only the E-stop, the normally-closed valve and independent position checks remain, and the twin records exactly where each one sits.

Annex I requirements, mapped to evidence

The CRA sets essential cybersecurity requirements in Annex I. The twin maps each one to the design choice that meets it, or the gap where none is evidenced, and the evidence that would prove it.

REQUIREMENT	IMPLEMENTATION ON THE PLATFORM	EVIDENCE
No known exploitable vulnerabilities	SBOM tracking across FarmBot OS, firmware and Web App once releases are pinned	VEX record per release
Secure by default	Setup and Wi-Fi onboarding defaults reviewed; unused services disabled on the Pi image	Build configuration and scan of a factory image
Protection against unauthorised access	Token authentication to the Web App; serial link to the Farmduino unauthenticated (gap)	Authentication tests per interface
Confidentiality	Camera images, garden data and credentials identified per link; TLS to the cloud to confirm	CBOM and traffic capture
Integrity	Encoder feedback for position; firmware and update integrity to evidence	Firmware hash checks, injection tests
Minimal attack surface	Ten interfaces enumerated: USB, Wi-Fi, Ethernet, the tool mount and the cloud API	Port and service scan results
Resilience to denial of service	Valve fails closed; behaviour on loss of cloud or serial link simulated	Link-loss tests on the bench
Secure updates	FarmBot OS and Farmduino firmware update paths modelled; signing not evidenced (gap)	Signed and unsigned bundle tests

11

The CRA evidence pack

Conformity is shown with evidence, not assertions. The twin produces three things a manufacturer needs before a conformity assessment: the digital files that describe the product, a test bench that can reproduce the claims, and a Requirements Traceability Matrix that ties every requirement to the evidence for it.

Digital files

Every file is machine-readable and generated from the same model, so they agree with each other by construction.

FILE	FORMAT	WHAT IT IS FOR
<code>sbom.cdx.json</code>	CycloneDX	Software inventory with versions, package URLs and licences
<code>hbom.cdx.json</code>	CycloneDX	Hardware inventory with part types, quantities and vendors
<code>cbom.cdx.json</code>	CycloneDX	Keys, tokens, algorithms and storage locations
<code>mbom.cdx.json</code> · <code>obom.cdx.json</code>	CycloneDX	Machine and operations BOMs linked to the same IDs
<code>farmbot-genesis-derived.xml</code>	DEXPI	Equipment, nozzles and connections derived from reviewed design data
<code>farmbot-genesis-full.glb</code>	glTF 2.0	Physical placement of all 1,105 parts, each with its twin ID
<code>kinematics.json</code> · <code>sequence.json</code>	JSON	Axes, limits, tool changes and the simulated controller sequence
<code>interface-register.csv</code> · <code>connections.csv</code>	CSV	Ten interfaces and 13 traced cables and hoses with their endpoints
<code>telemetry-sample.ndjson</code>	NDJSON	Simulated telemetry in the twin's schema, marked as simulated

Test bench readiness

A test bench reproduces the product's security claims on real hardware, so an assessor can watch them hold rather than read that they do. The twin defines what the bench must test and tracks whether each test is ready.

BENCH TEST	EXERCISES	STATUS
Port and service scan of the Pi on Wi-Fi and Ethernet	Minimal attack surface	Ready
Injected G/F-codes on the serial link, controller on the bench with motors disconnected	Protection against unauthorised access	Ready
Factory image review: setup and onboarding defaults	Secure by default	Ready
Tool-verification and soil-sensor signals spoofed at the UTM	Integrity of sensor data	Ready
Loss of cloud and loss of serial link during a sequence	Denial-of-service resilience	Partial
E-stop and valve behaviour under injected motion, with a safe test plan	Protective functions	Partial
Signed and unsigned FarmBot OS and firmware updates	Secure updates	Blocked
Early-warning drill: disclosure to draft report inside 24 hours	Vulnerability reporting	Partial

Statuses describe readiness of the test definition in this research model. On a real engagement each one links to the test procedure, the bench configuration that ran it and the dated result. No motion test runs on a powered machine without an approved safe test plan.

Requirements Traceability Matrix

The Requirements Traceability Matrix (RTM) is the backbone of the pack. Each row starts from a requirement and traces it through the design element that meets it, the components involved, the test that proves it and the evidence file it produces. Read top to bottom it shows coverage; read along a row it shows the pathway from obligation to proof.

REQ.	REQUIREMENT	DESIGN ELEMENT	COMPONENTS	TEST	EVIDENCE
R-01	No known exploitable vulnerabilities	SBOM and VEX per release	FarmBot OS, firmware, Web App	CVE scan after pinning	SBOM + VEX record
R-02	Secure by default	Hardened factory image	Raspberry Pi, FarmBot OS	Image review, service scan	Scan report
R-03	Unauthorised access	Command allowlist before serial	FarmBot OS, Farmduino	Injected G/F-codes	Bench log
R-04	Confidentiality	TLS to cloud, protected credentials	Pi, Web App	Traffic capture	CBOM + capture
R-05	Integrity	Encoder feedback, firmware hashes	Farmduino, encoders	Spoofed reports, hash check	Bench log
R-06	Minimal attack surface	Ten enumerated interfaces	Pi, UTM, USB	Port and service scan	Scan report
R-07	Denial-of-service resilience	Fail-closed valve, safe stop on link loss	Valve, Farmduino, OS	Link-loss test	Test report
R-08	Secure updates	Signed OS and firmware updates	FarmBot OS, Farmduino	Signed and unsigned bundles	Update test report
R-09	Vulnerability reporting	Pre-filled early-warning payload	Whole product	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. It is also the pathway assessment for a new revision: copy the matrix, change the components, and the rows that no longer trace are the work to do.

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 DEXPI data derived from the CAD and reviewed engineering evidence, 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, plus machine and operations BOMs, 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, kinematics, 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 and operations BOMs	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	FarmBot OS, 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.

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, the 3D model and CycloneDX SBOM, HBOM, CBOM, MBOM and OBOM, 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, expected result and safe test plan 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, every link with protocol, direction, rate and control, and the controller I/O map	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 revision, FarmBot OS release, 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.

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 and the 3D model, the risk assessment from the zones, threat trees and simulated consequences, the test results from the bench and the RTM, the BOMs from the CycloneDX layer, and the update plan from the FarmBot OS and firmware release 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, and the Machinery Regulation from 20 January 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, each software release and each hardware revision.

15

What this gives the manufacturer

TEAM	WHAT THEY GET
Executives and compliance	A defensible position on CRA, RED and machinery obligations, with evidence for each requirement and a clear view of where the gaps are
Engineering	Their own mechanics, controller, I/O and software, 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	Vendors and single-source parts by tier, and the EU importer position for a non-EU manufacturer
Open-source community	A public design whose security properties are documented with the same IDs as the CAD and code
Notified bodies and auditors	A technical file that is current, machine-readable and traceable to the product

Beyond farming robots

The same structure applies to any product with digital elements: drones, industrial controllers, CNC machines, 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. For FarmBot, the public CAD, BOM and repositories were enough to build this model; pinned releases, purchasing records and bench results are what turn it into evidence.

NO WARRANTY

This case study and the model it describes are provided for illustration and education only, without warranty, and make no declaration that any figure, component, configuration or finding is correct for any real product. FarmBot and FarmBot Genesis are products of FarmBot Inc.; this work was produced independently, from public information, and implies no endorsement or assessment by FarmBot Inc. Gaps described here are open questions in the model, not test results. Regulatory summaries are not legal advice; product classification under the CRA must be confirmed for each product.