

Readiness report — FUXA Web SCADA/HMI Station

Checked 2026-09-03 03:06 · 15 searches, 12 pages fetched

Readiness: FUXA Web SCADA/HMI Station

Verdict: Ready · 2026-09-03 · est. parts cost \$61-\$165 for the required host, plus \$21-\$123 if both optional peripherals are bought **Cybersecurity — software & network: Do not place on an open network**

This is the cold check for this lab — there is no previous report, so this one establishes the baseline every future check will measure drift against. On the hardware side the lab is easy: it has no custom PCB, no schematic and no discrete component list, just three commodity host-side items, two of which the lab's own materials mark optional. All three are current mass-market products available from several sellers today, and the lab grants high-to-wide substitution latitude on each — any machine that runs Node.js 18 LTS or Docker can host the station, so an instructor with a spare PC can start without buying anything. Nothing is obsolete, discontinued or out of stock, which is why the parts verdict is Ready. The station's software and network posture is a separate matter and is judged in the Cybersecurity section below; read it before this station goes anywhere near a shared network.

Action required

None — all checked parts are sourceable.

Cybersecurity — software & network

Do not place on an open network — The station ships with authentication disabled and a documented default password, listens on all interfaces over plain HTTP, runs on a Node.js release that went end of life in April 2025, and carries critical advisories in the dependency tree it installs.

Component	Version	How known	Support status
Node.js	18	read from project (README.md (fetched/05-README.md): 'Recommended: Node.js 18 LTS')	unsupported since 2025-04-30
fuxa-server (FUXA backend application server)	1.3.4-2890	read from project (version field of server/package.json (fetched/01-package.json), printed from the fetched file this run)	—
frangoteam/fuxa Docker image	not determined	unpinned (compose.yml (fetched/04-compose.yml) pins the floating tag frangoteam/fuxa:latest)	—

Component	Version	How known	Support status
Angular frontend (FUXA web client)	not determined	not determined (Version not stated in the snapshot; the client is not covered by the fetched server manifests)	—
node-snap7 (Siemens S7 native addon)	not determined	not determined (Optional addon; not declared in server/package.json (fetched/01-package.json))	—
odbc (database native addon)	not determined	not determined (Optional addon; not declared in server/package.json (fetched/01-package.json))	—
node-red	4.1.11	read from project (server/package-lock.json (fetched/02-package-lock.json); server/package.json (fetched/01-package.json) declares ^4.1.10)	—
express	4.22.2	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^4.22.2)	—
socket.io	4.8.3	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^4.8.3)	—
ws	8.21.0	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^8.21.0)	—
serialport	12.0.0	read from project (server/package.json (fetched/01-package.json) (exact pin))	—
sqlite3	5.1.7	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^5.1.7)	—
swagger-ui-express	5.0.1	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^5.0.1)	—
jsonwebtoken	9.0.3	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^9.0.3)	—
bcryptjs	2.4.3	read from project (server/package.json (fetched/01-package.json) (exact pin))	—
mqtt	4.3.7	read from project (server/package.json (fetched/01-package.json) (exact pin))	—
pg	8.22.0	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^8.18.0)	—
winston	3.7.2	read from project (server/package.json (fetched/01-package.json) (exact pin))	—
axios	1.18.1	read from project (server/package-lock.json (fetched/02-package-lock.json) top-level copy; declared ^1.16.1)	—

Component	Version	How known	Support status
jsonata	2.0.6	read from project (server/package-lock.json (fetched/02-package-lock.json) (transitive, via node-red))	—
tar	7.5.15	read from project (server/package-lock.json (fetched/02-package-lock.json); server/package.json (fetched/01-package.json) overrides tar to ^7.5.15)	—
fast-uri	3.1.3	read from project (server/package-lock.json (fetched/02-package-lock.json) (transitive))	—
js-yaml	4.1.1	read from project (server/package-lock.json (fetched/02-package-lock.json) (transitive))	—
multer	2.1.1	read from project (server/package-lock.json (fetched/02-package-lock.json) (transitive, via node-red))	—
nodemailer	8.0.11	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^8.0.8)	—
form-data	4.0.4	read from project (server/package-lock.json (fetched/02-package-lock.json) (transitive))	—
brace-expansion	2.0.3	read from project (server/package.json (fetched/01-package.json) overrides block (exact pin))	—
ip-address	10.1.1	read from project (server/package.json (fetched/01-package.json) overrides block (exact pin))	—
qs	6.15.2	read from project (server/package.json (fetched/01-package.json) overrides block (exact pin))	—
picomatch	4.0.4	read from project (server/package.json (fetched/01-package.json) overrides block (exact pin))	—
morgan	1.10.1	read from project (server/package.json (fetched/01-package.json) (exact pin))	—
body-parser	1.20.5	read from project (server/package-lock.json (fetched/02-package-lock.json); declared ^1.20.5)	—
npm CLI (bundled under node-red-admin)	10.9.8	read from project (server/package-lock.json (fetched/02-package-lock.json) (install-time tooling))	—

Component	Finding	Severity	Fix available?
jsonata 2.0.6 (Node-RED expression engine)	The flow engine FUXA installs resolves jsonata 2.0.6, where a crafted JSONata expression runs arbitrary code on the station itself. — GHSA-2943-5xfg-gq5f , GHSA-66mm-25pp-rfff , GHSA-8gq3-vp5j-2grp , GHSA-86vw-mfpg-www9	critical	Mitigation only - pin jsonata 2.2.1 or later through the existing overrides block in server/package.json and reinstall, and keep the station off untrusted networks meanwhile.
tar 7.5.15	The archive library the project pins by override crashes, hangs or mis-reads crafted archives, which matters wherever the station unpacks an uploaded or downloaded project file. — GHSA-23hp-3jrh-7fpw , GHSA-r292-9mhp-454m , GHSA-8x88-c5mf-7j5w , GHSA-gvwx-54wh-qm9j (+2 more)	critical	Yes - update to 7.5.21 (the project's own ^7.5.15 override already permits it; reinstall to refresh the lockfile).
axios 1.16.0 (nested under node-red-admin)	FUXA's own HTTP client is axios 1.18.1 and came back clean, but a second copy at 1.16.0 is installed under node-red-admin and carries proxy-handling and prototype-pollution flaws. — GHSA-gcfj-64vw-6mp9 , GHSA-42h9-826w-cgv3 , GHSA-7q8q-rj6j-mhjq , GHSA-f4gw-2p7v-4548 (+2 more)	high	Mitigation only - reinstall to refresh the lockfile, or drop node-red-admin if the Node-RED command-line tool is not used in this lab.
brace-expansion 2.0.3	The version the project pins by override can be driven into an out-of-memory crash by crafted glob patterns. — GHSA-rgw5-rvv9-x895 , GHSA-mh99-v99m-4gvg , GHSA-3jxr-9vmj-r5cp	high	No - project pins 2.0.3 in the overrides block of server/package.json; raising that override to 2.1.4 is the fix.
fast-uri 3.1.3	The URL parser in the station's request-validation stack can be tricked into reading an attacker's host as a trusted one, which is the classic setup for server-side request forgery. — GHSA-5jgf-p345-68v8 , GHSA-f65p-4m7j-42xc , GHSA-fph4-wmhf-6fwf , GHSA-jqff-g426-hqxp (+2 more)	high	Mitigation only - reinstall to refresh server/package-lock.json onto fast-uri 3.1.6; nothing in server/package.json pins it directly.
form-data 4.0.4	Multipart request bodies the station builds do not escape field names, so header content can be injected into outgoing requests (a second copy at 4.0.5 sits under axios and node-red-admin). — GHSA-hmw2-7cc7-3qxx	high	Mitigation only - reinstall to refresh the lockfile onto form-data 4.0.6; nothing in server/package.json pins it directly.
ip-address 10.1.1	The address parser the project pins by override mis-classifies some IPv4 and IPv6 forms, so address-based allow and deny checks around the station can be bypassed. — GHSA-mwp4-54f8-5fhr , GHSA-22jq-vg5j-6vgg , GHSA-4xrf-jv44-h6hh	high	No - project pins 10.1.1 in the overrides block of server/package.json; raising that override to 10.3.1 is the fix.

Component	Finding	Severity	Fix available?
js-yaml 4.1.1	A crafted YAML file - a project or flow import - can pin the station's CPU and stall the HMI for everyone watching it. — GHSA-5p4m-2wfm-xmqj , GHSA-52cp-r559-cp3m , GHSA-h67p-54hq-rp68	high	Mitigation only - reinstall to refresh the lockfile onto js-yaml 4.3.1; nothing in server/package.json pins it directly.
multer 2.1.1	The upload handler behind the editor can be exhausted by deeply nested field names or repeatedly aborted uploads, taking the station offline. — GHSA-72gw-mp4g-v24j , GHSA-3p4h-7m6x-2hcm	high	Mitigation only - reinstall to refresh the lockfile onto multer 2.2.0; it arrives through node-red rather than a direct pin.
nodemailer 8.0.11	If alarm e-mail is configured, a message-level raw option bypasses the file and URL access guards, letting a crafted message read files off the station. — GHSA-p6gq-j5cr-w38f	high	No - project pins ^8.0.8, and the fix is in 9.0.1, a major version the range excludes.
npm CLI bundled under node-red-admin	The vendored npm command-line tree (pacote 20.0.1 and 19.0.2, @sigstore/core 2.0.0, @tootallnate/once 1.1.2) carries advisories, but it is install-time tooling rather than part of the network-facing station. — GHSA-w4pp-8pjf-rmxw , GHSA-jfc7-64v2-mr8c , GHSA-vpq2-c234-7xj6	high	Mitigation only - reinstall to refresh the lockfile, or drop node-red-admin if the Node-RED command-line tool is not used.
morgan 1.10.1	The HTTP request logger writes unescaped control characters from the remote-user field, so an attacker can forge entries in the station's own logs. — GHSA-4vj7-5mj6-jm8m	moderate	No - project pins morgan 1.10.1 exactly in server/package.json; the fix is in 1.11.0.
qs 6.15.2	The query-string parser the project pins by override can be pushed into a denial of service through crafted URLs on the station's HTTP API. — GHSA-4mjr-xmp4-gh2g , GHSA-x5fp-wj9c-mxmx	moderate	No - project pins 6.15.2 in the overrides block of server/package.json; raising that override to 6.16.0 is the fix.
body-parser 1.20.5	An invalid body-size limit silently disables size enforcement on the station's HTTP API, removing a guard against oversized requests. — GHSA-v422-hmwv-36x6	low	Yes - update to 1.20.6 (the declared ^1.20.5 range already permits it; reinstall to refresh the lockfile).
frangoteam/fuxa Docker image	The compose file pulls the floating tag frangoteam/fuxa:latest, so two installs made weeks apart can run different code and neither matches what was checked here.	posture	Mitigation only - pin a released image tag or its digest in compose.yml so the deployment is reproducible.

Component	Finding	Severity	Fix available?
FUXA web server (authentication)	Authentication is off until an administrator turns it on: the shipped default settings leave <code>secureEnabled</code> commented out, and the project's own security policy treats <code>secureEnabled=false</code> as an intended configuration that is out of scope for vulnerability reports.	posture	Mitigation only - set <code>secureEnabled: true</code> with a strong <code>secretCode</code> in <code>server/_appdata/settings.js</code> before the station is connected to any shared network.
FUXA web server (default credentials)	The project documents the starting account as user 'admin' with password '123456'.	posture	Mitigation only - change the admin password in the same sitting as enabling security.
FUXA web server (network binding)	The station serves its editor, dashboards, REST API and Swagger documentation over plain HTTP on port 1881 and by default accepts connections on every IPv4 interface, because <code>uiHost</code> is left commented out.	posture	Mitigation only - set <code>uiHost</code> to 127.0.0.1 or a single management interface, place the station on an isolated segment, and terminate TLS in front of it.
fxa-server dependencies	Dependencies unpinned: 19 of 39 in <code>server/package.json</code> use caret ranges, so an npm install resolves whatever is current that day - though the repository does ship <code>server/package-lock.json</code> , which pins all 762 resolved packages.	posture	Mitigation only - install with <code>npm ci</code> against the repository's <code>server/package-lock.json</code> rather than <code>npm install</code> , and pin the Docker tag.
Node.js 18	The runtime the project recommends reached end of life on 2025-04-30 and no longer receives security updates, so flaws in the runtime under the station will not be fixed.	posture	No - requires platform migration (to a Node.js release still in support).

What this means for your lab

Out of the box this station is wide open. FUXA ships with authentication switched off - the setting that turns it on is commented out in the default settings file - and it listens for web connections on every network interface of the host, over ordinary unencrypted HTTP on port 1881. Anyone who can reach that address can open the editor, read every value the station is collecting, redraw the screens, and write values back to whatever PLCs and instruments are wired to it; on a bench connected to real equipment that means starting and stopping the process. When security is switched on, the documented starting account is 'admin' with the password '123456', so that has to be changed in the same sitting. Separately, the runtime the project recommends - Node.js 18 - stopped receiving security updates in April 2025, and several packages the server installs have known flaws; the most serious lets a crafted expression in the built-in flow editor run code on the station itself. What to do: keep this station on its own isolated network segment or a lab-only VLAN and never on the campus network or the open internet, turn security on and change the admin password before the

first class, install with 'npm ci' so you get the versions the project actually tested, and raise it with campus IT before connecting it to anything shared. One thing remains unknown: because the compose file pulls the 'latest' Docker tag, we cannot say whether the prebuilt image contains the same package versions checked here.

Not checked

- Transitive dependencies in server/package-lock.json (261 of 762 rows): Beyond the 500-row automatic OSV check cap. The lab's own named production dependencies that fell past the cap were then checked individually this run: serialport, socket.io, sqlite3, swagger-ui-express, winston, ws, yamlls, qs, tar and picomatch.
- fuxa-server 1.3.4-2890: The application's own release string is not published to the npm registry (the registry check returned 'version not found'), so no advisory database covers the FUXA server package itself.
- frangoteam/fuxa Docker image: Pinned to the floating tag latest, so there is no version to look up; whether the published image contains the package versions checked here is unknown.
- Angular frontend (FUXA web client): Version not stated in the snapshot and not covered by the fetched server manifests, so nothing could be checked.
- node-snap7 (Siemens S7 native addon): Optional addon with no version stated; it is not declared in server/package.json, so there is nothing to check.
- odbc (database native addon): Optional addon with no version stated; it is not declared in server/package.json, so there is nothing to check.
- Industrial protocol endpoints (Modbus TCP 502, S7 102, OPC-UA 4840, BACnet IP 47808, MQTT 1883, EtherNet/IP 44818, Redis 6379): The snapshot records the ports these use, but the protocol endpoints themselves carry no version and no advisory database applies to them.
- npm registry pages for @frangoteam/fuxa and @frangoteam/fuxa-min: npmjs.com refused the automated fetch this run, so the published npm packages could not be inspected.
- fuxa-server 1.3.4-2890: this version does not exist in the package registry (a kit or hardware release number is not a software version)
- 250 further dependencies in package-lock.json: beyond the 500-dependency automatic check cap (e.g. @mapbox/node-pre-gyp, @sinonjs/commons, @sinonjs/fake-timers, @sinonjs/samsam, @sinonjs/text-encoding)

Parts

Hardware and Platform Components

Part	Spec/Package	Status	Stock	Price	Source
Host Single-Board Computer / Industrial PC — Raspberry Pi 4 Model B 4GB	SBC chassis or DIN-rail enclosure; 5 V DC via USB-C, 3.3 V LVTTL GPIO; qty 1, required	Readily available — multiple retail sellers	—	\$61.05 (Vilros basic starter kit, 4GB) · \$100.00 (bulk board) · \$165.00 (desktop kit)	Vilros, eBay, PiShop USA
Industrial Serial Bus Converter (USB-to-RS485 / RS-232)	External USB dongle or DIN-rail module; USB bus powered; FTDI / CP2102 / CH340 accepted; qty 1, optional	Readily available — cheap and plentiful	—	\$10.99 (Waveshare industrial bidirectional) · \$17.99 (isolated, FT232RL + SP485EEN) · \$75.78 (FTDI, DB-9/RJ45/terminal)	Waveshare, DigiKey
Video Capture Peripheral (USB webcam, UVC)	External USB peripheral or CSI module; 5 V DC USB bus power; any UVC-compliant camera; qty 1, optional	Readily available	—	\$16.00 (C270, 720p) · \$23.99 (C270, 720p) · \$112.00 (4K IMX317, UVC)	eBay, Walmart, econ Systems

Two notes on the pricing above, so the baseline is not read for more than it says:

- The cheapest Raspberry Pi hit this run was [\\$35.00 at Seeed Studio](#), but that listing is titled simply "Raspberry Pi 4 Model B" and does not state its memory size, so it is not evidence of a 4 GB board at that price. The lowest evidenced 4 GB price is \$61.05. A separate \$144.00 listing for a "Raspberry Pi CM4 4GB" was excluded: the Compute Module 4 is a different product with a different form factor, not the Model B this lab specifies.
- The lab's actual camera requirement is only UVC compliance, not a particular resolution. The sub-\$25 webcams found are 720p Logitech C270 models, which satisfy that requirement; listings that explicitly claim 1080p or better start at \$112.00. Budget the higher figure only if 1080p is wanted for its own sake.

Substitutes

None needed. No part is obsolete, out of stock, single-sourced or unreasonably priced, so no substitute was proposed and none required spec-by-spec verification this run.

Other dependencies

- **Upstream Git repository** — <https://github.com/frangoteam/FUXA> — live. Its `server` directory was listed and seven files were downloaded from it during this check.

- **Documentation and demo portal** — <https://frangoteam.github.io/FUXA/> — live; the FUXA wiki home page returned its expected content.
- **Docker Hub image repository** — <https://hub.docker.com/r/frangoteam/fuxa> — live and actively maintained; the page reports 100K+ pulls, a 200 MB image and "Last updated 22 days ago".
- **Community SVG graphic widgets** — <https://github.com/frangoteam/FUXA-SVG-Widgets> — live; the widget collection and its authoring guide loaded normally.
- **npm registry pages** — <https://www.npmjs.com/package/@frangoteam/fuxa> and <https://www.npmjs.com/package/@frangoteam/fuxa-min> — **not checked**: npmjs.com refused the automated fetch. That is npm blocking a script, not evidence the packages are gone; check by hand if this lab installs from npm rather than from Docker or a git clone.
- **Prebuilt Electron artifacts and headless portable binaries** (the `electron_latest.yml` and `headless_packaging.yml` GitHub Actions workflows) — **not checked**; build-artifact pages behind Actions were not retrieved this run.
- **Fabrication** — not applicable. The lab records no custom PCB, no layer count and no board dimensions, so there is nothing to send to a board house.

Watch list

- **Raspberry Pi 4 Model B 4GB** — the only required purchase, and the one with real price exposure: evidenced 4 GB prices ran \$61.05 to \$165.00 across sellers this run, with no authorized-distributor baseline behind them. Retail Pi pricing has a history of moving with supply, so this is the line to re-price next check.
- **The \$35.00 Seeed Studio listing** — worth resolving specifically: if a genuine 4 GB board is available near that price, the lab's entry cost roughly halves. This check could not confirm the memory size from the listing title.
- **Pi 4 Model B end-of-sale** — the Pi 4 generation is several years old and will eventually give way to newer models. Nothing in this run's evidence says it is discontinued, but if it goes, the lab's high substitution latitude means a newer Pi or any Node.js-capable PC absorbs the change; only labs that address GPIO pins directly would need a Pi-compatible header.
- **Optional peripherals (RS-485 adapter, UVC webcam)** — low risk. Both are commodity categories with many interchangeable sellers, and the lab accepts any FTDI/CP2102/CH340 converter and any UVC camera.