

Readiness report — Pioreactor Open-Source Bioreactor Cluster

Checked 2026-09-03 03:49 · 14 searches, 11 pages fetched

Readiness: Pioreactor Open-Source Bioreactor Cluster

Verdict: Ready with caveats · 2026-09-03 · est. parts cost \$384–\$514 per bioreactor unit
Cybersecurity — software & network: Review before networking

Every part this lab needs can be bought today. The two ICs the software actually drives are Active and deeply stocked, the Raspberry Pi 4 Model B is on sale at many retailers, and the proprietary 40 mL bioreactor assembly is orderable from the manufacturer at \$349.00 with a stated 4-week lead time. Three things keep it from a clean "Ready". The FT232RL-REEL USB-UART bridge is obsolete with zero stock at every authorized distributor checked, and even its manufacturer-recommended successor is backordered everywhere — but the snapshot marks this device optional, so it does not block the core build. The 40 mL assembly is sole-sourced with a 4-week lead, which is a scheduling risk for a term-dated course. And Raspberry Pi listings range from \$35 to \$165 depending on RAM and kit contents, so budget to the 4GB specification rather than the cheapest headline price. This is the cold check for this lab — there is no previous report, so it establishes the baseline every future check will measure drift against.

Action required

Part	Problem	Recommended action
FT232RL-REEL	Obsolete; 0 stock at DigiKey (50-week factory lead), RS (357-day lead) and Mouser (out of stock). ECIA lifecycle and supply-chain risk both High. The whole FT232RL family is affected — FT232RL-TUBE is likewise Obsolete with 0 stock.	Optional part — confirm whether your build uses the auxiliary FTDI serial expansion at all. If it does and you need <code>pyftdi</code> bit-bang modes, order FT232RNL-REEL far ahead (Active, but backordered everywhere). If you only need plain USB-to-serial, CY7C65213-28PVXI is in stock now (16,977 pcs). See Substitutes.

Cybersecurity — software & network

Review before networking — The pinned frontend carries several fixable high-severity advisories and one Markdown-rendering flaw with no fixed release, the documented broker allows anonymous access, and the build runtime (Node.js 25) is past end of life - all manageable, but they should be addressed before these units go on a shared network.

Component	Version	How known	Support status
Raspberry Pi OS / Debian (host operating system)	12	inferred (Not stated in any fetched source; the snapshot's check plan treats the Raspberry Pi OS base as Debian 12, and the support lookup was run on that basis.)	extended/LTS support only until 2028-06-30
CPython (Python runtime)	3.13.0	read from project (fetched/07-getting-started.md pins it exactly: 'pyenv install 3.13.0' and 'pyenv global 3.13.0'.)	supported until 2029-10-31
Node.js (frontend build and dev server runtime)	25	inferred (fetched/07-getting-started.md says 'nvm install 25' - a major-line pin only, no exact release.)	unsupported since 2026-06-01
Eclipse Mosquitto (MQTT broker)	not determined	unpinned (fetched/07-getting-started.md installs it via 'apt install mosquitto' / 'brew install mosquitto' with no version.)	—
SQLite3 (database engine)	not determined	unpinned (fetched/07-getting-started.md installs it via 'apt install sqlite3' with no version.)	—
Flask (backend REST API)	3.1.3	read from project (fetched/01-requirements.txt (requirements/requirements.txt) pins Flask==3.1.3.)	—
Werkzeug	3.1.8	read from project (fetched/01-requirements.txt pins Werkzeug==3.1.8.)	—
Jinja2	3.1.6	read from project (fetched/01-requirements.txt pins Jinja2==3.1.6.)	—
paho-mqtt (Python MQTT client)	2.1.0	read from project (fetched/01-requirements.txt pins paho-mqtt==2.1.0.)	—
huey (task consumer)	3.3.0	read from project (fetched/01-requirements.txt pins huey==3.3.0.)	—
msgspec	0.21.1	read from project (fetched/01-requirements.txt pins msgspec==0.21.1.)	—
mcp-utils-msgspec (leader node)	3.0.1	read from project (fetched/02-requirements_leader.txt pins mcp-utils-msgspec==3.0.1.)	—
Adafruit-Blinka (worker hardware layer)	9.1.0	read from project (fetched/03-requirements_worker.txt pins Adafruit-Blinka==9.1.0.)	—
adafruit-circuitpython-ads1x15 (ADC driver)	2.2.23	read from project (fetched/03-requirements_worker.txt pins adafruit-circuitpython-ads1x15==2.2.23.)	—

Component	Version	How known	Support status
DAC43608 (DAC driver)	0.2.7	read from project (fetched/03-requirements_worker.txt pins DAC43608==0.2.7.)	—
pyftdi (FTDI serial driver)	0.57.2	read from project (fetched/03-requirements_worker.txt pins pyftdi==0.57.2.)	—
numpy	2.3.2	read from project (fetched/03-requirements_worker.txt pins numpy==2.3.2.)	—
PyYAML (base-image preinstalled)	6.0.2	inferred (Listed in fetched/01-requirements.txt only as a commented 'preinstalled on base image' line, so the manifest parser does not install it; checked against OSV directly this run.)	—
rpi-lgpio (base-image preinstalled)	0.6	inferred (Commented 'preinstalled on base image' line in fetched/01-requirements.txt; checked against OSV directly this run.)	—
lgpio (base-image preinstalled)	0.2.2.0	inferred (Commented 'preinstalled on base image' line in fetched/01-requirements.txt; checked against OSV directly this run.)	—
React (web user interface)	19.2.7	read from project (fetched/06-package-lock.json resolves react@19.2.7 (frontend/package.json declares the range ^19.2.7).)	—
Vite (frontend dev server)	7.3.6	read from project (fetched/06-package-lock.json resolves vite@7.3.6.)	—
mqtt (browser/JS MQTT client)	5.15.1	read from project (fetched/06-package-lock.json resolves mqtt@5.15.1.)	—
react-router	7.17.0	read from project (fetched/06-package-lock.json resolves react-router@7.17.0.)	—
ws (WebSocket library, transitive under mqtt)	8.18.3	read from project (fetched/06-package-lock.json resolves ws@8.18.3.)	—
ip-address (transitive dependency)	10.1.0	read from project (fetched/06-package-lock.json resolves ip-address@10.1.0.)	—
showdown (Markdown renderer, transitive under react-showdown)	1.9.1	read from project (fetched/06-package-lock.json resolves showdown@1.9.1.)	—

Component	Finding	Severity	Fix available?
ip-address (transitive dependency)	An address-parsing helper bundled into the web interface misreads addresses written with leading zeros, which can be used to slip past checks meant to stop the software contacting internal network addresses. — GHSA-mwp4-54f8-5fhr , GHSA-v2v4-37r5-5v8g	high	Yes — update to 10.3.1
react-router	The routing library behind the Pioreactor web interface has five known flaws at the pinned version 7.17.0, including one that lets an unauthenticated visitor stall the interface by requesting awkward URLs, plus cross-site scripting and open-redirect issues. — GHSA-chx6-hx7r-mcp5 , GHSA-qwww-vcr4-c8h2 , GHSA-h8fp-f39c-q6mh , GHSA-337j-9hxr-rhxg (+1 more)	high	Yes — update to 7.18.2
ws (WebSocket library, transitive under mqtt)	The WebSocket library that carries live bioreactor data to the browser can be driven to exhaust memory by a flood of tiny message fragments, and can leak uninitialised memory contents. — GHSA-96hv-2xvq-fx4p , GHSA-58qx-3vcg-4xpx	high	Yes — update to 8.21.0
showdown (Markdown renderer, transitive under react-showdown)	The Markdown renderer used for text shown in the interface can be tricked into running injected scripts or into a slow parsing loop, and no fixed release of this library exists. — GHSA-22g5-r2x5-97cx , GHSA-cr32-g25g-vxjj , GHSA-rmmh-p597-ppv	moderate	Mitigation only — no fixed version is published; only render Markdown the class authors, not text supplied by outsiders
Eclipse Mosquitto (MQTT broker)	The documented broker configuration sets 'allow_anonymous true', so anything that can reach the message broker can read every measurement and send commands without a password; the same file binds the listeners to 127.0.0.1, which is what currently keeps that off the network.	posture	Mitigation only — keep the broker bound to localhost, and require a username and password before exposing it to a shared or multi-unit network
Node.js (frontend build and dev server runtime)	The setup guide installs Node.js 25, a release line that stopped receiving security updates on 2026-06-01, so the machine building and serving the interface runs an unmaintained runtime.	posture	Mitigation only — install a Node.js release line that is still supported instead of 'nvm install 25'
React frontend dependencies (frontend/package.json)	dependencies unpinned: 32 of 34 in frontend/package.json - the manifest declares version ranges, so a fresh install can pull newer, unreviewed versions than the ones checked here.	posture	Mitigation only — install from the committed package-lock.json (npm ci) rather than npm install

What this means for your lab

The Pioreactor's web interface, its message broker and its data are all reachable over the network by design, and as set up in the project's own guide none of them ask for a password - the guide turns anonymous access on for the message broker and relies on keeping everything bound to the machine itself. That is fine on a single unit on a bench. If you put these units on a shared campus or lab network, or run a multi-unit cluster, assume anyone else on that network could read your experiment data and send commands to the hardware - starting or stopping stirring, heating and pumps - unless you add authentication first. The web interface also carries several known flaws at the versions currently pinned, the most serious of which lets an unauthenticated visitor tie the interface up, and it is built and served on a Node.js version that stopped getting security updates in June 2026. Practical steps: keep the units on an isolated network segment or their own VLAN rather than the general campus network, set a username and password on the message broker before any multi-unit or networked use, update the frontend packages that have fixes available, and move the build machine to a supported Node.js version. Talk to campus IT before connecting these to a shared network. Some things could not be checked at all - the broker and database versions are never pinned, and the cluster's remote-login credentials are not documented in the material supplied - so treat those as unknown rather than safe.

Not checked

- Eclipse Mosquitto (MQTT broker): Installed unpinned via apt/brew; no version is stated in any source, so there is no version to check against the advisory databases.
- SQLite3: Installed unpinned via apt; no version is stated in any source.
- Raspberry Pi OS exact release: Not stated in the sources; the support status shown is for Debian 12, the base the snapshot's check plan assumes, not a release read from the project.
- 434 further transitive npm packages in frontend/package-lock.json: Beyond the 500-row automatic advisory check cap; 500 of the 938 locked packages were checked this run.
- Frontend dependencies as actually installed: Versions were checked from the committed package-lock.json; an 'npm install' against the unpinned ranges in package.json may resolve to different versions than those checked.
- Cluster inter-node SSH and remote access credentials: The snapshot records that default SSH credentials, keys and remote port definitions are not stated in the uploaded sources, so nothing could be checked.
- Unpinned build tools (build-essential, curl, git, make, direnv): Installed unpinned via apt/brew; versions come from the operating system and are not stated.
- Python packages installed from the base image (PyYAML, rpi-igpio, igpio): Checked against OSV this run and clean at the versions the manifest names in comments, but whether the image actually carries those versions was not verified.

- 434 further dependencies in package-lock.json: beyond the 500-dependency automatic check cap (e.g. @rollup/rollup-linux-ppc64-gnu, @rollup/rollup-linux-ppc64-musl, @rollup/rollup-linux-riscv64-gnu, @rollup/rollup-linux-riscv64-musl, @rollup/rollup-linux-s390x-gnu)

Parts

Host Platform and Processing Hardware

Part	Spec/Package	Status	Stock	Price	Source
Raspberry Pi 4 Model B	85 mm × 56 mm SBC, 40-pin GPIO header (2.54 mm pitch), 5.0 V DC ≥ 3.0 A, 3.3 V GPIO logic	Readily available	Multiple retailers	~~\$35.00~~ - ~~\$165.00~~	Seed Studio (\$35.00, RAM size not stated in listing); Vilros 4GB bulk \$100.00; PiShop USA desktop kit (\$165.00)

The vendor's own product page notes one Raspberry Pi is needed per Pioreactor, and that the microSD card and power supply are not included in the kit.

Integrated Circuits and Sensor Interfaces

Part	Spec/Package	Status	Stock	Price	Source
ADS1115IDGSR	VSSOP-10 (DGS), 16-bit 4-ch I2C ADC, supply 2.0–5.5 V	Readily available	42,250	~~\$5.28~~	DigiKey (Texas Instruments, Active)
DAC43608RTER	16-WQFN exposed pad, 16-WQFN (3×3), supply 1.8–5.5 V	Readily available	3,547	~~\$5.61~~	DigiKey (Active); also Spirit Electronics 3,000 @ \$4.69, Mouser 1,652 @ \$5.39
FT232RL-REEL	28-SSOP (0.209", 5.30 mm width), supply 3.3–5.25 V	Obsolete — unobtainable	0 (DigiKey, RS, Mouser)	~~\$4.80 last catalog price~~	DigiKey (Obsolete); ECIA lifecycle risk High. Optional part per the snapshot

System Electromechanical & Assemblies

Part	Spec/Package	Status	Stock	Price	Source
Pioreactor 40 mL Bioreactor Assembly (model pioreactor_40ml v1.5, HW rev 1.2, FW rev 1.1)	Custom vial holder, Eye-Spy optics, magnetic stirring base, heating jacket, 40 ml borosilicate vial, Vial Cap S	Available — sole-source, 4-week lead time	Made to order	~~from \$349.00~~	Pioreactor (SKU 1041), kit or pre-assembled

Spare and repair parts priced on the vendor's catalog page this run: Pioreactor HAT PCB (SKU 2032) \$99.68 · Eye-Spy PCB (SKU 2070) \$19.60 · Heating PCB and accessories (SKU 2014) \$44.74 · 40 ml glass vial (SKU 2056) \$5.04 · 15×6 mm PTFE stir bar (SKU 2046) \$2.24 · Vial Cap S (SKU 2059) \$14.00 · Raspberry Pi 27 W PSU (SKU 2073) \$16.74.

Substitutes

For part	Substitute	Differences	Verified	Judgment
FT232RL-REEL	FT232RNL-REEL — FTDI, \$4.80, Active	Same package/case (28-SSOP, 0.209" / 5.30 mm width), same supply range 3.3–5.25 V, same 15 mA supply current, same –40 °C to 85 °C range. Genuine FTDI silicon, so <code>pyftdi</code> bit-bang modes still work. DigiKey lists it as the manufacturer-recommended replacement. But: 0 stock everywhere checked — DigiKey 50-week factory lead, Mouser 384,761 on order, RS 84-day lead.	verified: package/case + body width (DigiKey parametrics on both parts), supply range (DigiKey parametrics on both), FTDI silicon (manufacturer field). not verified: pin-for-pin pinout equivalence — <code>ftdichip.com</code> could not be fetched this run; lead pitch not given in DigiKey parametrics for either part	Correct long-term replacement, but not a near-term fix — order well ahead or design around it
FT232RL-REEL	CY7C65213-28PVXI — Infineon, \$4.54, Active, 16,977 in stock	Same package/case (28-SSOP, 0.209" / 5.30 mm width). Supply range 1.71–5.5 V is wider than the original's 3.3–5.25 V and covers the lab's 3.3 V and 5.0 V rails — exceeds the requirement, acceptable. Supply current 20 mA vs 15 mA, negligible on a USB rail. Not FTDI silicon: the snapshot requires genuine FTDI parts for <code>pyftdi</code> bit-bang modes, though it allows generic bridges (CH340, CP2102) for ordinary serial.	verified: package/case + body width (DigiKey parametrics on both parts), supply range (DigiKey parametrics on both — superset covering the lab's rails), stock and price (DigiKey + ECIA this run). not verified: pinout equivalence. Known mismatch, not an unknown: not FTDI silicon	Acceptable for plain USB-to-serial only; not acceptable anywhere <code>pyftdi</code> bit-bang is used

FT231XS-U, which DigiKey suggests against FT232RL-TUBE, was rejected: it is a 20-SSOP part against the required 28-SSOP — a different package and pin count, which is a hard stop.

Verify any substitute against its datasheet before ordering — particularly the pinout claims marked unverified above.

Other dependencies

- **PCB fabrication specifications — not checked.** No Gerbers, schematics, KiCad/Eagle board files or mechanical CAD were included in the upload, so layer count, board dimensions, copper weight, surface finish, trace/space clearances and drill sizes are stated nowhere in the sources. In practice this blocks nothing: the HAT is bought assembled inside the kit, or separately as SKU 2032 (\$99.68).
- **Vendor storefront (pioreactor.com) — live.** The product page and full catalog page were both fetched successfully this run.
- **Documentation hub (docs.pioreactor.com) — not checked.** Not fetched this run.
- **Vendor shipping terms and current lead time — not checked.** The fetched pages gave price and a 4-week estimated lead time but carried no retrievable statement about shipping destinations or order restrictions. Confirm both with the vendor before committing to a course schedule.
- **Missing internal repository assets** listed in the snapshot (`config.dev.ini` , `packaging/shared-assets/**` , `create_tables.sql` , `create_triggers.sql`) were absent from the uploaded bundle, not from the project — `config.dev.ini` is present in the upstream repository root as listed this run. This is an upload-completeness gap, not a dependency failure. The individual `packaging/shared-assets` paths were not checked.

Watch list

- **FT232RL-REEL and its successor FT232RNL-REEL** — the original is obsolete and gone; the successor is Active but backordered at every authorized distributor (50-week DigiKey lead, 384,761 on order at Mouser). If FTDI supply has not recovered by the next check, anyone who genuinely needs FTDI silicon will be waiting quarters, not weeks.
- **Pioreactor 40 mL assembly** — sole-sourced from one manufacturer with a 4-week lead time and no substitute of any kind. Any vendor disruption, price change or model revision (v1.5 today, with an XR upgrade path already on sale) directly threatens the lab. Re-check price and lead time before each term.
- **Raspberry Pi 4 Model B pricing** — a 3x spread across listings today, and the Pi 4 is an older generation still widely stocked. Watch for the bare-board price drifting up or listings thinning as the Pi 5 line matures; the codebase pins Blinka to `RASPBERRY_PI_4B` , so moving generations is not free.
- **DAC43608RTER** — healthy today, but it is a single-manufacturer part with one driver package pinned against it (`DAC43608==0.2.7`). Worth watching for lifecycle changes, since substitution latitude is essentially nil.