

Readiness report — foxBMS 2 Battery Management Development Platform

Checked 2026-09-03 03:54 · 16 searches, 5 pages fetched

Readiness: foxBMS 2 Battery Management Development Platform

Verdict: Ready with caveats · 2026-09-03 · est. parts cost \$288–\$352 (active silicon + one debug probe for one bench; discretes and PCB fabrication not priced) **Cybersecurity — software & network: Review before networking**

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. foxBMS 2 is modular: a bench needs the BMS Master, **one** interface card and **one** slave family, not all three variants the bill of materials lists. One complete path is fully in stock today — TMS570LC4357 master, LTC6820 interface and LTC6811-1 12-cell slave are all Active with healthy stock. The caveats are real, though: the JTAG debug probe every bench needs shows zero stock at all three authorized distributors on a 12-week factory lead, the MAXIM interface line's part number does not resolve to any catalog product and the closest real part is a different package, the 18-cell LTC slave is discontinued at DigiKey in both temperature grades, and the NXP 14-cell slave is on Last Time Buy. Take the LTC 12-cell path, order probes a term ahead, and the lab runs.

Action required

Part	Problem	Recommended action
MAX17841BAGU/V+ (MAXIM interface U1)	Part number returns no match at DigiKey and no ECIA-authorized distributor lists it. The only orderable MAX17841B variants are 16-TSSOP, while the snapshot requires a 28-pin TQFN-EP.	Open the <code>interface-maxim-max17841b-v1.0.0</code> board file and read U1's actual footprint before ordering anything. Simplest fix: build the LTC or NXP interface instead.
TMDSEMU110-U (XDS110 JTAG probe)	Active but zero stock at DigiKey, Arrow and Mouser, all quoting a 12-week factory lead. Required for every bench — without it nothing can be flashed.	Order roughly 3 months ahead of the term. The XDS200 is compatible but costs 2–3x and is equally out of stock; a TI LaunchPad with an onboard XDS110 is a plausible cheaper route (not checked this run).

Part	Problem	Recommended action
LTC6813HLWE-1#3ZZPBF (18-cell LTC slave U1)	"Discontinued at DigiKey"; only Rochester Electronics holds stock (3 units). DigiKey quotes a 13-week factory lead. The industrial-grade sibling is discontinued at DigiKey too.	Prefer the 12-cell LTC6811-1 path. If 18-cell modules are required, buy the Rochester stock early or accept a 10-13 week lead.
MC33775ATA1AE (14-cell NXP slave U1)	Status "Last Time Buy"; ECIA rates lifecycle risk High. The snapshot's own part number, MC33775ATE, is not orderable at all.	Obtainable in volume today — Arrow holds 11,878 at \$5.18. If this path is wanted, buy the lab's whole expected lifetime now, and plan a redesign.
MC33664ATL (NXP interface U1)	Snapshot part number is not orderable as written; no ECIA-authorized distributor lists it. DigiKey's supply-voltage parameter (4.5-5.5 V) also disagrees with the snapshot's stated 3.15-5.5 V range.	Order the full orderable part number (MC33664ATL1EG / MC33664ATL1EGR2) after confirming it against the board BOM and the MC33664 datasheet.

Cybersecurity — software & network

Review before networking — Fourteen pinned Python build dependencies carry known advisories (six rated high, including remote-code-execution class flaws in GitPython and click) and the documented toolchain install performs unverified binary downloads, though the target board itself exposes no network services.

Component	Version	How known	Support status
Host operating system (Windows or Linux)	not determined	not determined (INSTALL.md gives only install prefixes (C:\foxbms, /opt/devel/foxbms-2); no OS version is stated anywhere in the file)	—
PowerShell	not determined	unpinned (INSTALL.md requires 'PowerShell 7 or later' - a minimum, not a pin)	—
Git	not determined	unpinned (INSTALL.md links git-scm.com with no version)	—
TI Code Composer Studio (CCS)	12.8.1	read from project (INSTALL.md (fetched/03-INSTALL.md) lines 117/126 pin CCS 12.8.1)	—
TI HALCoGen	04.07.01	read from project (INSTALL.md (fetched/03-INSTALL.md) line 133 pins HALCoGen 04.07.01)	—
Python	3.12.8	inferred (INSTALL.md requires 'exactly 3.12.x' (a range); 3.12.8 appears only as example <code>python --version</code> output, so the exact patch level is not pinned)	supported until 2028-10-31

Component	Version	How known	Support status
Ruby (RubyInstaller x64)	3.4.2	read from project (INSTALL.md (fetched/03-INSTALL.md) line 204 pins RubyInstaller-3.4.2-1 (x64))	supported until 2028-03-31
Ceedling (Ruby gem)	1.0.1	read from project (INSTALL.md (fetched/03-INSTALL.md) line 214 installs ceedling into C:\foxbms\Ceedling\1.0.1)	—
MinGW-w64 toolchain (GCC)	8.1.0	read from project (INSTALL.md (fetched/03-INSTALL.md) lines 227-232 pin x86_64-8.1.0-release-posix-seh-rt_v6-rev0)	—
7-Zip	not determined	unpinned (INSTALL.md links 7-zip.org with no version)	—
Doxygen	1.14.0	read from project (INSTALL.md (fetched/03-INSTALL.md) lines 236/241 pin Doxygen 1.14.0)	—
Graphviz	14.0.0	read from project (INSTALL.md (fetched/03-INSTALL.md) lines 247/252 pin Graphviz 14.0.0)	—
draw.io Desktop	28.1.2	read from project (INSTALL.md (fetched/03-INSTALL.md) lines 258/263 pin drawio-desktop 28.1.2)	—
Visual Studio Code	not determined	unpinned (INSTALL.md links code.visualstudio.com with no version)	—
click	8.3.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
GitPython	3.1.45	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
lxml	6.0.2	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
pillow	11.3.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
pyarrow	21.0.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
urllib3	2.5.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
diskcache	5.6.3	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
filelock	3.19.1	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
fonttools	4.60.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—

Component	Version	How known	Support status
idna	3.10	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
requests	2.32.5	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
setuptools	80.9.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
virtualenv	20.34.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
Pygments	2.19.2	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
python-can	4.6.1	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
cantools	40.6.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
pymodbus	3.4.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
PyVISA	1.15.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
RsInstrument	1.102.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—
paho-mqtt	2.1.0	read from project (requirements.txt (fetched/01-requirements.txt), pinned with ==)	—

Component	Finding	Severity	Fix available?
click 8.3.0	The pinned click has a command-injection flaw in its click.edit() helper, so a foxBMS command-line tool that opens an editor could be made to run arbitrary operating-system commands. — PYSEC-2026-2132	high	Yes — update to 8.3.3
GitPython 3.1.45	The pinned GitPython can be tricked into running arbitrary shell commands through crafted git options, so any foxBMS build or CI script that passes untrusted input to a git call could execute attacker-chosen commands on the build machine. — GHSA-x2qx-6953-8485 , GHSA-jm78-9fvv-mhgr , GHSA-wvpp-8hx9-p66j , GHSA-r9mr-m37c-5fr3 (+2 more)	high	Yes — update to 3.1.58
lxml 6.0.2	The pinned lxml parses XML with external-entity resolution enabled by default, so parsing an untrusted XML or SVG file could read local files off the build machine. — GHSA-vfmq-68hx-4jfw	high	Yes — update to 6.1.0

Component	Finding	Severity	Fix available?
pillow 11.3.0	The pinned Pillow has several out-of-bounds write and decompression-bomb flaws, which matter when the documentation build processes image files that did not come from the project itself. — GHSA-xj96-63gp-2gmr , GHSA-pwv6-vv43-88gr , GHSA-jjj6-mw9f-p565 , GHSA-6r8x-57c9-28j4 (+2 more)	high	Yes — update to 12.3.0
pyarrow 21.0.0	The pinned pyarrow can hit a use-after-free when reading an Arrow IPC file, which matters only if measurement data from an untrusted source is loaded in that format. — GHSA-rgxp-2hwp-jwgg	high	Yes — update to 23.0.1
urllib3 2.5.0	The pinned HTTP library mishandles compressed responses and leaks sensitive headers across origins on proxied redirects, which affects the toolchain and package downloads the install performs over HTTP(S). — GHSA-38jv-5279-wg99 , GHSA-qccp-gfcp-xxvc , GHSA-2xpw-w6gg-jr37 , GHSA-gm62-xv2j-4w53	high	Yes — update to 2.7.0
diskcache 5.6.3	The pinned diskcache unpickles cached data unsafely, so anything able to write into the cache directory could run code as the user; no fixed release exists. — GHSA-w8v5-vhqr-4h9v	moderate	Mitigation only — no fixed version is published; keep the cache directory private to the user and never share or reuse one from another machine
filelock 3.19.1	The pinned filelock has symlink race conditions when creating lock files, which a local user on a shared lab machine could abuse to overwrite files. — GHSA-w853-jp5j-5j7f , GHSA-qmgc-5h2g-mvrw	moderate	Yes — update to 3.20.3
fonttools 4.60.0	The pinned fontTools can write arbitrary files when processing a crafted font, relevant only when building documentation with fonts from outside the project. — GHSA-768j-98cg-p3fv	moderate	Yes — update to 4.60.2
idna 3.10	The pinned idna can be fooled by crafted domain names into producing a different host than intended, which weakens the URL checks around the project's own downloads. — GHSA-65pc-fj4g-8rjx	moderate	Yes — update to 3.15
requests 2.32.5	The pinned requests reuses temporary files insecurely in one helper, which a local user on a shared machine could exploit. — GHSA-gc5v-m9x4-r6x2	moderate	Yes — update to 2.33.0
setuptools 80.9.0	The pinned setuptools can include files that the packaging rules meant to exclude when building a source distribution on macOS. — GHSA-h35f-9h28-mq5c	moderate	Yes — update to 83.0.0

Component	Finding	Severity	Fix available?
virtualenv 20.34.0	The pinned virtualenv has a race condition when creating directories, which a local user could abuse while the foxBMS environment is being built. — GHSA-597g-3phw-6986	moderate	Yes — update to 20.36.1
Pygments 2.19.2	The pinned Pygments can be made very slow by a crafted input during documentation builds; the impact is a stalled build, not a compromise. — GHSA-5239-wwwm-4pmq	low	Yes — update to 2.20.0
Binary toolchain downloads (Ruby, MinGW-w64, Doxygen, Graphviz, draw.io)	INSTALL.md tells the student to download binary toolchain archives from sourceforge.net, github.com and gitlab.com and extract them into C:\foxbms with no checksum or signature check anywhere in the file - its 'verify' steps only confirm the .exe file is present at the expected path.	posture	Mitigation only — download over HTTPS only, and compare each archive against the publisher's own published checksum before extracting

What this means for your lab

Everything checked this run runs on the instructor's or student's build PC, not on the battery-management board itself. The target board is flashed over JTAG and, per the snapshot, exposes no Ethernet, web interface or SSH login, so there is nothing on it for someone on the network to log into. The real exposure is the build machine: the project pins 114 Python packages, and fourteen of them have known security bugs, including a GitPython flaw that can turn a crafted git option into arbitrary commands and a click flaw that can do the same through an editor helper. These bite when the machine processes something from outside the project - an untrusted repository, image, font or XML file - so the practical risk is a compromised lab PC rather than a hijacked battery pack. The install instructions also download toolchains as binary archives without any checksum or signature check, which means a bad download or a tampered mirror would not be noticed. What to do: bump the flagged pins in requirements.txt (most have fixed versions available), check each downloaded archive against the publisher's checksum before extracting, and keep the CAN, Modbus and instrument links on an isolated bench network. One thing this check could not establish is the operating system: the documentation never states a Windows or Linux version, so whether the host OS is still receiving security updates is unknown and worth confirming with campus IT.

Not checked

- Host operating system (Windows / Linux): no OS version is stated in INSTALL.md, so no end-of-life or support lookup is possible; the snapshot's suggested 'Windows 11 / Ubuntu 22.04' is not supported by the sources and was not assumed

- PowerShell: unpinned - INSTALL.md requires only '7 or later', so there is no specific version to check
- Git: unpinned - no version stated in INSTALL.md
- 7-Zip: unpinned - no version stated in INSTALL.md
- Visual Studio Code: unpinned - no version stated in INSTALL.md
- TI Code Composer Studio 12.8.1: vendor IDE with no public advisory database indexed by OSV; version is pinned but not checkable
- TI HALCoGen 04.07.01: vendor code generator with no public advisory database indexed by OSV; version is pinned but not checkable
- MinGW-w64 8.1.0 (GCC 8.1.0): SourceForge toolchain builds are not an OSV ecosystem, and an endoflife.date lookup for product 'gcc' returned product_not_found, so its support state is unknown
- Doxygen 1.14.0: upstream Doxygen releases are not covered by an OSV ecosystem
- Graphviz 14.0.0: upstream Graphviz releases are not covered by an OSV ecosystem
- draw.io Desktop 28.1.2: upstream drawio-desktop releases are not covered by an OSV ecosystem
- pre-commit hook tools (.pre-commit-config.yaml): the hook config was not fetched this run; its tool versions are pinned separately from requirements.txt and were not checked
- foxBMS 2 embedded firmware (target C source, FreeRTOS): source-only embedded code with no package registry or advisory database to check against
- gcc 8.1.0: support status: endoflife.date has no such product

Parts

Hardware bill of materials and silicon elements

Part	Spec/Package	Status	Stock	Price	Source
TMS5704357BZWTQQ1 — BMS Master U1 (Hercules safety MCU)	337-NFBGA (16x16), supply 3 V ~ 3.6 V	Active — readily available	944	\$95.09	DigiKey
LTC6820HMS#PBF — LTC interface U1 (isoSPI transceiver)	16-MSOP / 16-TFSOP (3.00 mm), supply 2.7 V ~ 5.5 V	Active — readily available	45 DigiKey; Mouser 351, Newark 283	\$9.23 (Mouser \$8.48)	DigiKey + ECIA
MC33664ATL — NXP interface U1 (isolated transceiver)	Snapshot: 16-pin SOIC, 150 mil. Catalog orderables are 16-SOIC (0.154")	Not orderable as written — buy MC33664ATL1EGR2 / MC33664ATL1EG	1020 (MC33664ATL1EGR2)	\$8.35 · \$4.88	DigiKey

Part	Spec/Package	Status	Stock	Price	Source
MAX17841BAGU/V+ — MAXIM interface U1 (SPI to isolated UART)	Snapshot: 28-TQFN-EP (4 mm x 4 mm)	Not obtainable as specified — no catalog match anywhere checked	—	—	—
LTC6811HG-1#PBF — LTC 12-cell slave U1 (stack monitor)	48-SSOP / 48-FSOP (5.30 mm)	Active — readily available	750	\$29.06	DigiKey
LTC6813HLWE-1#3ZZPBF — LTC 18-cell slave U1 (stack monitor)	64-LQFP-EP (10x10), -40 °C ~ 125 °C (TJ)	Discontinued at DigiKey — hard to obtain	0 DigiKey (13-week lead); Rochester 3	Rochester \$18.74 (qty break 25)	ECIA (DigiKey link for reference)
MC33775ATE — NXP 14-cell slave U1 (cell controller)	Snapshot: LQFP-64-EP (10x10). Orderable MC33775ATA1AE is 64-LQFP-EP (10x10)	Not orderable as written; MC33775ATA1AE is Last Time Buy	53 DigiKey; Arrow 11,878, Mouser 191	\$11.23 (Arrow \$5.18)	DigiKey + ECIA
TMDSEMU110-U — XDS110 JTAG debug probe (1 per bench)	TI 14/20-pin JTAG, 3.3 V target I/O	Active but no stock — 12-week lead everywhere	0 at DigiKey, Arrow, Mouser	\$218.30 (Arrow \$155.35)	DigiKey + ECIA

Substitutes

For part	Substitute	Differences	Verified	Judgment
MAX17841BAGU/V+	MAX17841BGUE/V+ — \$11.88, 1439 in stock	Same device family and the only MAX17841B orderable in stock. Package differs from the snapshot's requirement: 16-TSSOP (0.173", 4.40 mm) vs the stated 28-pin TQFN-EP (4 mm x 4 mm) — different pin count and different package family. Operating temp -40 °C ~ 105 °C (TA).	verified: package/case and supplier device package (DigiKey parametrics); lifecycle and stock (DigiKey exact match). not verified: footprint compatibility with the foxBMS board — the catalog package contradicts the snapshot, and the ADI product page (fetch blocked) and datasheet PDF could not be read this run. Supply-voltage range not verified — no supply parameter returned.	Not verified — plausible identity match, but not a drop-in claim. Check the board file and datasheet before ordering.

For part	Substitute	Differences	Verified	Judgment
LTC6813HLWE-1#3ZZPBF	LTC6813ILWE-1#3ZZPBF — industrial temperature grade	Same device, same package: 64-LQFP-EP (10x10) on both. Temperature grade is narrower, -40 °C ~ 85 °C (TJ) vs -40 °C ~ 125 °C (TJ) — it falls short of the H grade rather than exceeding it, so it suits benchtop use well inside 85 °C only.	verified: package/case and supplier device package match on both parts (DigiKey parametrics); operating temperature range for both (DigiKey parametrics). not verified: supply-voltage range — no supply parameter was returned for either grade, so the 11 V-82.8 V stack rail is unconfirmed.	Not acceptable as an availability fix — it is also "Discontinued at DigiKey" with 0 stock at DigiKey (10-week lead), Richardson and Mouser. Recorded for baseline only.
TMDSEMU110-U	TMDSEMU200-U — TI XDS200, \$477.02	Named by the lab snapshot itself as an acceptable probe. Materially more expensive: \$477.02 DigiKey (price break qty 6), \$407.92 Mouser, \$343.98 Arrow, against \$155.35-\$218.30 for the XDS110. Active.	verified: CCS 12.8.1 compatibility (stated by the lab snapshot); lifecycle, price and stock (DigiKey exact match + ECIA distributor data).	Acceptable on compatibility, but useless as an availability fix — DigiKey, Mouser and Arrow all report 0 stock on the same 12-week lead, at 2-3x the price.

For part	Substitute	Differences	Verified	Judgment
TMDSEMU110-U	MCU-LINK — NXP, \$16.65, 753 in stock (DigiKey's own suggestion)	DigiKey describes it as an "ARM Cortex-M debug probe". The lab's target is a TMS570LC4357, an ARM Cortex-R5F Hercules device, and the snapshot requires a probe supported by TI Code Composer Studio 12.8.1.	verified: price and stock (DigiKey); its stated target architecture, Cortex-M, from the DigiKey description. not verified: any support for Cortex-R5F / Hercules or for TI CCS — no evidence gathered this run supports it.	Rejected. Different debug architecture from the lab's MCU; DigiKey's "Similar" tag is a catalog category, not a compatibility claim.

Verify any substitute against its datasheet and against the board's own footprint before ordering.

Other dependencies

- **Source repository** <https://github.com/foxBMS/foxbms-2> — live and reachable this run; requirements.txt, pyproject.toml and INSTALL.md were all fetched successfully from the master branch.
- **Hardware release archives** <https://iisb-foxbms.iisb.fraunhofer.de/foxbms/gen2/hardware/release/> (master-v1.2.3, interface-*, slave-* zips) — **not checked**. These archives are the only source of the Altium schematics, layouts and the full discrete-component BOMs, so the entire fabrication path depends on that Fraunhofer server staying available. Worth confirming manually.
- **Project documentation site** <https://iisb-foxbms.iisb.fraunhofer.de/foxbms/gen2/docs/html/latest/> — **not checked** this run.
- **TI tool download pages** (Code Composer Studio 12.8.1, HALCoGen) — **not checked** this run; both require a TI account, which the lab setup assumes.
- **Fabrication** — designed in Altium Designer, OSHWA certified under UID DE000128. Board dimensions, layer stackup, copper weights and surface finish are not stated in the uploaded materials; they live in the Gerber, ODB++ and .PcbDoc files inside the remote release archives, so fabrication cannot be quoted from what is here. **Not checked**.
- **Discrete components, connectors and isolation transformers** — not priced; their line-by-line BOMs are inside those same remote archives.

Watch list

- **MC33775ATA1AE (NXP 14-cell slave)** — Last Time Buy with ECIA lifecycle risk High. Channel stock is deep today (Arrow ~11.9k) but this line will disappear; expect it to be unobtainable at a future check.
- **LTC6813HLWE-1#3ZZPBF (18-cell LTC slave)** — discontinued at DigiKey in both temperature grades, with a single distributor holding 3 units. The most likely part to become genuinely unobtainable next.
- **TMDSEMU110-U (XDS110 probe)** — zero stock across all three authorized distributors on a 12-week lead. Watch whether stock returns or lead times stretch further.
- **MAX17841BAGU/V+ (MAXIM interface)** — unresolved identity and footprint question. Until the board file is read, treat this whole interface variant as unbuildable.
- **LTC6820HMS#PBF** — healthy overall, but DigiKey stock is thin at 45 units; Mouser and Newark carry the depth. Worth re-checking that the other two hold.