INTERFACE CONTROL DOCUMENT

BLADE-INFRA-OT

IT/OT Bridge Governance Variant of the BLADE-INFRA Reference Platform

Document number:	**ICD-INFRA-OT-001**
Revision:	**A (BOM finalized from Blueprint hardware export)**
Issue date:	**May 2026**
Author:	**Burak Oktenli, Independent Researcher**
Affiliation:	**Washington, DC, USA**
ORCID:	**0009-0001-8573-1667**
Parent platform:	**BLADE-INFRA (NERC CIP / FIPS 140-2 aligned)**
TRL - hardware:	**2–3**
TRL - simulation:	**3–4**
Distribution:	**Public release under CC BY 4.0**
Distribution:	**Open. No export-controlled content.**

Abstract. This Interface Control Document specifies the hardware, mechanical, electrical, environmental, and protocol interfaces of the BLADE-INFRA-OT appliance. BLADE-INFRA-OT is a bump-in-the-wire governance variant of the BLADE-INFRA critical-infrastructure platform, dedicated to inspection of cross-boundary traffic at the IT/OT segmentation interface. The appliance applies the AUTHREX eight-stage authority pipeline to every cross-boundary message before propagation to OT control assets. The design is structured as a reference implementation of the joint CISA / ASD ACSC / NSA principles for AI integration into operational technology (December 2025) and is informed by the documented Monterrey water-utility intrusion attempt (Dragos, May 2026).

Status. Fundamental research. No penetration testing or operational deployment. Published openly. The hardware design uses commercial off-the-shelf components only. The simulation is scripted against documented threat patterns and does not target any operational utility.

Revision History

Rev.	Date	Author	Summary of changes
-	2026-05	B. Oktenli	Initial release. Establishes baseline against BLADE-INFRA parent platform.
A	2026-05	B. Oktenli	BOM finalized (47 line items) from Blueprint hardware export. Added schema

Contents

1 Scope

This Interface Control Document (ICD) establishes the interfaces of the BLADE-INFRA-OT appliance: a 1U rack-mount (or DIN-rail) fanless, conformal-coated bump-in-the-wire governance device installed at the IT/OT segmentation boundary of critical-infrastructure environments. The appliance hosts the AUTHREX authority pipeline (SATA, ADARA, IFF, HMAA, MAIVA, FLAME, ERAM, CARA) and applies it to every cross-boundary message at protocol-aware granularity (Modbus, DNP3, IEC 61850 MMS / GOOSE / SV, OPC UA, EtherNet/IP, BACnet).

The document specifies the mechanical envelope, electrical and power interfaces, data interfaces, AUTHREX pipeline allocation between the governance plane and the network plane, audit-ledger interface, environmental envelope, bill of materials, compliance alignment, and verification procedures.

The document is informative for the simulation tier (TRL 3–4) and specification-level for the hardware tier (TRL 2–3). No operational deployment is contemplated under this revision. The BLADE-INFRA-OT appliance is a research artifact; it has not been fabricated and has not undergone first-article test under this revision.

1.1 Relation to BLADE-INFRA

BLADE-INFRA-OT inherits approximately seventy percent of the BLADE-INFRA reference platform. Inherited subsystems include the compute stack family (Xilinx Kria SOM governance plane plus x86 Atom-class network plane), the hardware security module family, the audit-ledger format and signing chain, the out-of-band management interface, and the mechanical-enclosure family. The differentiating subsystems are (a) the OT-protocol parser layer; (b) the bump-in-the-wire network architecture with read-only default posture; and (c) the IT/OT-specific HMAA authority-tier mapping.

1.2 Intended use

BLADE-INFRA-OT is intended as a reference appliance for academic research, standards-body reference implementations, and the education of utility security engineers. It is not a fielded product and is not certified to any operational security level under this revision.

2 Applicable documents

Reference	Title
CISA · ASD ACSC · NSA · Dec 2025	Principles for the Secure Integration of AI in Operational Technology
CISA · NSA · Five Eyes · 1 May 2026	Careful Adoption of Agentic AI Services - joint advisory
Dragos · May 2026	Monterrey water utility - AI-assisted IT-to-OT pivot attempt (failed at OT layer). Threat intellige
NERC CIP-005 / 007 / 008 / 010	Critical Infrastructure Protection: electronic security perimeter, system security management,
FIPS PUB 140-2	Security Requirements for Cryptographic Modules.
IEC 62443 (multi-part)	Industrial communication networks - Network and system security.
IEC 61850 (multi-part)	Communication networks and systems for power utility automation.
IEEE 1815	Distributed Network Protocol (DNP3).
Modbus V1.1b3	Modbus Application Protocol Specification.
OPC Foundation	OPC UA Specification, Parts 1–14.
ODVA	EtherNet/IP and Common Industrial Protocol (CIP).
ASHRAE 135 / ANSI	BACnet - A Data Communication Protocol for Building Automation and Control Networks.
NIST SP 800-82 Rev. 3	Guide to Operational Technology (OT) Security.

IEC 61850-3 / IEEE 1613	Substation EMC profile.
DoD Directive 3000.09	Autonomy in Weapon Systems. Cited for HMAA tier model lineage.
AUTHREX framework	Oktenli, B. (2026). AUTHREX: A Unified Authority-Lifecycle Framework. Zenodo.

3 System overview

BLADE-INFRA-OT is structured as two cryptographically separated planes hosted within a single chassis. The **network plane** carries the bump-in-the-wire packet path and the protocol parser layer. The **governance plane** hosts the AUTHREX pipeline as a partitioned set of processes and, where deterministic latency is required, as FPGA fabric. The two planes communicate through a policy-enforced inter-plane channel that is monotonic, audited, and rate-limited.

3.1 Block diagram (informative)

IT network ingress	→	Network plane (parsers, packet path, MAC/IP)	→	OT network egress
	↕	Inter-plane policy channel (rate-limited)	↕	
Operator OOB	↔	Governance plane (AUTHREX pipeline on Kria K26)	↔	HSM root-of-trust
		Audit ledger (TPM-signed, append-only)		

Figure 3.1 - Top-level block representation. Plane separation enforced by both software policy and a dedicated inter-plane bus with cryptographic envelope.

3.2 Operational modes

Two operational postures are defined. The default posture is **read-only inspection**: traffic that clears the AUTHREX pipeline is forwarded unchanged; traffic that triggers a CARA isolation is dropped, with an alarm on the out-of-band channel. An optional **policy-enforcement** posture rewrites or holds messages during a FLAME deliberation window. The conservative read-only deployment is the documented starting posture for utilities and is the assumption for the simulation tier.

3.3 Authority tiers

Tier	Posture	Operator role	Trigger to enter
T3	Supervised autonomous	Monitor	Steady-state, all stages pass
T2	Bounded deliberation	Confirm window	FLAME deliberation opened
T1	Elevated, human-on-loop	In-loop confirm	CARA isolation event
T0	Manual fallback	In-the-loop	Multiple isolation / loss-of-trust

4 Mechanical interface

4.1 Form factor and envelope

Primary form factor: 1U rack-mount, 19-inch (482.6 mm) standard rack width, 1U height (44.45 mm), depth 12 inches (305 mm). Secondary form factor: industrial DIN-rail mount kit, IP54-rated chassis variant for cabinet deployment. Chassis material: extruded aluminum with steel front bezel.

Parameter	Value
Width	482.6 mm (19 inch)
Height	44.45 mm (1U)
Depth	305 mm (12 inch)
Mass (typical)	5.2 kg
Mounting	Front and mid-rail rack mount; optional DIN-rail kit
Material	Extruded aluminum chassis, steel front bezel
Finish	Powder coat, matte black; conformal coating on PCBs
IP rating (rack variant)	IP30
IP rating (DIN-rail variant)	IP54
Vibration	IEC 60068-2-6, sinusoidal sweep, 1g, 10–500 Hz
Shock	IEC 60068-2-27, half-sine, 30 g, 11 ms

4.2 Front and rear panels

Front panel: power-on indicator (green), AUTHREX-ARMED indicator (amber), ALARM indicator (red), serial console DB-9 (OOB), USB type-A maintenance port (read-only by default; admin-toggled), system identification field-replaceable serial-number plate. Rear panel: redundant AC inlet IEC C14 with locking clip, dual 24 VDC station-service terminal block, four RJ-45 GbE ports labeled *IT-in* / *IT-mon* / *OT-out* / *OT-mon*, two SFP+ cages, IPMI RJ-45 port, system-reset recessed pushbutton, Kensington security slot.

4.3 Internal layout

Two-board design. A network-plane motherboard hosts the x86 Atom SBC, switch chip, and front/rear panel I/O. A governance-plane mezzanine hosts the Kria K26 SOM, the HSM module, and the inter-plane bus connector. Boards are mechanically separated by a steel divider. The inter-plane bus crosses the divider through a single shielded ribbon cable. Cooling is convective; no fans are present. Heat-spreading bars couple the K26 and Atom to the chassis top cover.

5 Electrical and power interface

5.1 Power inputs

Two redundant power inputs are supported. The primary input is an industrial AC/DC supply accepting 90–264 VAC, 47–63 Hz, with active power-factor correction and a holdup time of 20 ms at full load. The secondary input is a 24 VDC station-service rail (18–36 VDC tolerance). Either input is sufficient for full operation. Source selection is automatic with hot-swap; an audible alarm and an out-of-band log entry are generated on source loss.

Rail	Voltage	Load (typ.)	Tolerance
AC primary	90–264 VAC, 47–63 Hz	≤ 65 W	Active PFC
DC secondary	24 VDC	≤ 2.8 A	18–36 VDC
Internal 12 V	12.0 V	1.2 A	±5%
Internal 5 V	5.0 V	1.5 A	±5%
Internal 3.3 V	3.3 V	2.0 A	±5%
Internal 1.8 V (Kria core)	1.8 V	0.6 A	±3%
Internal 1.0 V (Kria core)	1.0 V	2.4 A	±3%

5.2 Grounding and isolation

Chassis ground is bonded to safety earth at the AC inlet. The 24 VDC input is referenced through an isolated DC/DC converter to support station-service grounding conventions in substations. Signal grounds (network plane and governance plane) are tied at a single star point at the inter-plane bus connector. All Ethernet ports are magnetically isolated to 1500 V RMS, in accordance with IEEE 802.3 isolation requirements.

5.3 Surge and transient protection

AC mains: IEC 61000-4-5 surge withstand to 2 kV line-to-line and 4 kV line-to-earth. DC input: IEEE C37.90 surge withstand capability for substation deployment. Ethernet ports: TVS-array secondary protection beyond magnetic isolation. RS-232 console: TVS-array, ±15 kV ESD.

5.4 EMI / EMC

Targeted compliance with FCC Part 15 Class A and CISPR 32 Class A for emissions; IEC 61000-4 series for immunity, with deviations noted for substation environment per IEC 61850-3. Final EMC qualification is deferred to a fabricated prototype campaign and is not in scope for this revision.

6 Network and data interface

The appliance presents four GbE ports and two SFP+ cages on the rear panel. Two of the GbE ports form the bump-in-the-wire path: *IT-in* connects to the IT-side network egress at the segmentation boundary; *OT-out* connects to the OT-side ingress. The other two GbE ports, *IT-mon* and *OT-mon*, are dedicated read-only mirror taps for span-based monitoring. SFP+ cages provide fiber alternatives for either duty; typical substation deployments use multimode fiber for galvanic isolation.

Port	Speed	Role	Posture
IT-in (RJ-45)	10/100/1000	Bump-in-wire ingress from IT	Inline
OT-out (RJ-45)	10/100/1000	Bump-in-wire egress to OT	Inline
IT-mon (RJ-45)	10/100/1000	IT-side mirror tap	Read-only
OT-mon (RJ-45)	10/100/1000	OT-side mirror tap	Read-only
SFP+ A	1G / 10G optical	Bump-in-wire alternative	Inline (configurable)
SFP+ B	1G / 10G optical	Mirror or OOB telemetry	Read-only
IPMI (RJ-45)	10/100	Out-of-band management	Air-gapped from data path
Console (DB-9)	RS-232	Serial console, OOB	Air-gapped

6.1 Inline path latency budget

The inline path is designed for an end-to-end inspection latency budget under 250 microseconds at line rate for short-header control traffic (Modbus, DNP3, IEC 61850 MMS). The latency budget is partitioned: physical layer ingress and egress at 5 µs each; protocol parsing and AST formation at 30 µs typical; AUTHREX stages SATA through ERAM at 150 µs typical; egress queuing at 20 µs. GOOSE messages are handled on an accelerated path through the Kria fabric, targeting a sub-100 µs envelope. Final measured latencies are deferred to a fabricated prototype.

6.2 Failure modes

Three failure modes are defined. **Fail-closed** (default): on any internal fault, the inline path is broken; traffic ceases. **Fail-bypass** (configurable): on fault, an internal relay bypasses the inspection path, restoring connectivity at the cost of governance. Fail-bypass is deliberately not the default and must be explicitly enabled per CIP-007 configuration management. **Fail-alarm-only**: governance plane fault while network plane remains healthy - traffic continues, audit ledger logs degradation, OOB alarm raised.

7 OT protocol parsers

Six protocol parser processes execute on the network plane. Each parser produces a uniform abstract syntax tree (AST) representation of the message, on which the AUTHREX pipeline operates without knowledge of protocol-specific encoding. A common-AST design is used to keep AUTHREX stages free of protocol-coupled logic.

Protocol	Standard	Typical domain	Throughput target
Modbus TCP / RTU	Modbus V1.1b3	Water, gas, general SCADA	10 kpps
DNP3	IEEE 1815-2012	Electric, gas	5 kpps
IEC 61850 MMS	IEC 61850-8-1	Substation, station bus	5 kpps
IEC 61850 GOOSE	IEC 61850-8-1	Substation, process bus	10 kpps (acc.)
IEC 61850 SV	IEC 61850-9-2	Sampled values	4 kpps (acc.)
OPC UA	OPC UA 1.05	Industrial IoT, vendor remote	2 kpps
EtherNet/IP CIP	ODVA CIP	Discrete manufacturing PLC	5 kpps
BACnet/IP	ASHRAE 135	Building management	2 kpps

7.1 Modbus

The Modbus parser produces an AST with fields: transaction-id, function-code, target-register or coil, value-or-range, and originating-host identity (derived from the L2/L3 envelope). Function codes 5, 6, 15, 16 (writes) are flagged for elevated scrutiny by HMAA. Function-code patterns associated with exploratory scanning are recognized by ADARA.

7.2 DNP3

DNP3 parsing covers application-layer object groups 10 (binary outputs), 12 (CROB), 41 (analog outputs), and 70 (file transfer). Class 0 polls, integrity polls, and unsolicited messages are modeled. Authentication mechanisms per IEC 62351-5 are recognized and contribute to SATA scoring when present.

7.3 IEC 61850 MMS / GOOSE / SV

MMS write services to non-status data attributes are flagged for HMAA. GOOSE and SV are time-critical multicast streams; they are processed on the Kria-accelerated path. GOOSE state-number and sequence-number consistency checks form part of the SATA score for streams. R-GOOSE and R-SV (routed variants) are supported through the same AST.

7.4 OPC UA

OPC UA secure-channel and session establishment are parsed; the AST exposes the client application URI, the requested service set (Browse, Read, Write, CallMethod), and the security mode (None, Sign, SignAndEncrypt). CallMethod invocations are flagged for HMAA. Anonymous user tokens are recognized and contribute a negative SATA bias.

7.5 EtherNet/IP and BACnet

EtherNet/IP CIP messaging is parsed to expose service-code, class-id, instance-id, and attribute-id; CIP Safety messages carry an additional safety-envelope token. BACnet/IP WriteProperty and WritePropertyMultiple operations against schedule and override objects are flagged for HMAA.

8 AUTHREX pipeline allocation

The eight-stage AUTHREX authority pipeline is allocated between the network plane and the governance plane, and between software and FPGA fabric within the governance plane, according to the latency and determinism requirements of each stage.

Stage	Function	Allocation	Latency target
SATA	Provenance score of originating IT system	Kria - software	20 µs
ADARA	Anomalous / AI-pattern detection	Kria - sw + LUT	40 µs
IFF	OT-side target authentication	Kria - software	15 µs
HMAA	Authority-tier check vs operator roster	Kria - fabric	10 µs
MAIVA	Consensus across redundant inspection nodes	Kria - sw (inter-node)	60 µs
FLAME	Bounded deliberation window for high-stakes	Kria - fabric + sw	5 µs (open/close)
ERAM	Risk-based gating against current posture	Kria - software	10 µs
CARA	Automatic isolation on detected compromise	Kria - fabric (cut-through)	5 µs (trigger)

Table 8.1 - Pipeline stage allocation. Latency targets are typical design-intent values; final measured values are deferred to a fabricated prototype.

8.1 Inter-stage data envelope

Stages communicate through a fixed-format envelope containing the AST handle, current verdict, current authority tier, FLAME-window state, MAIVA consensus vote, and a TPM-signed transcript chain. The envelope is monotonic - later stages may degrade the verdict but never elevate it.

8.2 Decision outcomes

Three terminal outcomes are defined per message: **PROPAGATE** (message forwarded unchanged); **DELIBERATE** (message held; FLAME window opened; operator confirmation required); **ISOLATE** (message dropped; CARA action executed; tier degraded; OOB alarm). Every outcome is committed to the audit ledger before the message is forwarded or dropped.

9 Audit ledger interface

The audit ledger is an append-only, TPM-signed log of every cross-boundary message processed by the appliance. Each entry is a fixed-schema record with the fields below. The ledger is designed for forensic chain-of-custody and is structured to be compatible with NERC CIP-008 incident-response evidentiary requirements.

Field	Type	Description
ts_utc	uint64	Microsecond timestamp, UTC
msg_id	uint128	Per-appliance monotonic identifier
src_endpoint	string	Originating IT host identity
dst_endpoint	string	Target OT asset identity
protocol	enum	Modbus / DNP3 / IEC61850-MMS / GOOSE / SV / OPC-UA / EIP / BACnet
operation	string	Protocol operation summary
sata_score	float32	Provenance score $\tau \in [0, 1]$
adara_verdict	enum	baseline / scan / AI-pattern / AI-burst / corr
iff_status	enum	valid / unknown / invalid
hmaa_tier_granted	enum	T3 / T2 / T1 / T0 / DENY
maiva_consensus	string	n/m local nodes agreeing
flame_state	enum	open / window / closed / trip / n/a
eram_risk	enum	low / med / high / crit
cara_action	enum	no-op / watch / isolate / drop / region-iso
outcome	enum	PROPAGATE / DELIBERATE / ISOLATE
tpm_signature	bytes[64]	Ed25519 over (msg_id ■ prev_hash ■ entry)
prev_hash	bytes[32]	BLAKE3 of previous entry

9.1 Ledger root rotation

The ledger root is rotated every 24 hours of operation, every 10 million entries, or on operator command, whichever is first. A rotated root is sealed with the TPM and is exportable through the OOB channel for off-appliance custody. The previous root's hash becomes the prev_hash of the first entry under the new root.

9.2 Export formats

The ledger is exportable in three formats: a compact binary format for archive (12-byte header + variable-length records); a newline-delimited JSON format for forensic analysis; and a CIP-008-aligned XML format for utility incident-response submission. Exports are themselves TPM-signed.

10 Out-of-band management interface

The out-of-band (OOB) management interface is air-gapped from both the inline data path and the mirror taps. It is the only interface through which an operator can interrogate appliance state, retrieve ledger exports, or update policy. The OOB interface is bound to a dedicated IPMI/serial port; it does not share NIC, switch fabric, or memory pages with the data plane.

Function	Channel
Operator console (text)	DB-9 RS-232, 115200 8N1
Out-of-band IP management	IPMI 2.0 over dedicated RJ-45
Ledger export	IPMI-mounted virtual storage; SCP over OOB
Policy update	Signed bundle; TPM-attested; OOB only
Firmware update	Signed image; dual-slot rollback; OOB only
Alarm output	Dry contact relay (Form C); SNMP trap via OOB

11 Environmental and reliability

Parameter	Value	Reference
Operating temperature	–40°C to +70°C	Industrial
Storage temperature	–55°C to +85°C	Industrial
Operating humidity	5–95% non-condensing	-
Cooling	Fanless, passive convection	-
Altitude	Up to 3000 m operating	-
Vibration	1 g, 10–500 Hz	IEC 60068-2-6
Shock	30 g, 11 ms	IEC 60068-2-27
Salt fog	Coastal substation envelope	IEC 60068-2-52
Substation EMC	Substation profile	IEC 61850-3 / IEEE 1613
MTBF target	≥ 200,000 h (Telcordia SR-332)	-
MTTR	≤ 30 min (FRU-replaceable)	-

11.1 Reliability allocation

The MTBF target of 200,000 hours is a calculated allocation against the Telcordia SR-332 parts-count method. Allocations are: power supply 30%, governance plane (Kria + supporting circuitry) 25%, network plane (Atom + switch chip + magnetics) 30%, balance (HSM, OOB module, mechanical) 15%. The fanless design eliminates the dominant failure mode of comparable appliances.

12 Bill of materials

Finalized BOM (Rev. A), 47 line items, generated from the Blueprint hardware export (3E8 Robotics) and reconciled against this ICD. Commercial off-the-shelf components only except the two custom PCBs; no export-controlled parts. Vendor part numbers are indicative and may be second-sourced.

Item	Component / Part number	Qty	Ext. (USD)
1	Governance Plane Compute - Xilinx Kria K26 Industrial SOM	1	3,000.00
2	Network Plane Compute - AAEON GENE-EHL5-A10-01 (Intel Atom x…	1	1,800.00
3	Managed Ethernet Switch - Marvell LinkStreet 88E6390X	1	240.00
4	TPM 2.0 Security Module - Infineon SLB 9670 VQ2.0	1	30.00
5	Root of Trust Element - Microchip ATECC608B-TFLXTLS	1	30.00
6	IPMI BMC Controller - ASPEED AST2500	1	200.00
7	Primary AC/DC Unit - TDK-Lambda CUS100ME-12/U	1	180.00
8	Secondary 24V DC Input - Vicor DCM3623T36G13C2T00	1	65.00
9	Form-C Fault Relay - TE Connectivity IM03TS	1	15.00
10	10G SFP+ Port A - Molex 74754-0220	1	37.50
11	10G SFP+ Port B - Molex 74754-0220	1	37.50
12	Power Indicator LED - Dialight 550-2406F	1	2.50
13	AUTHREX Armed LED - Dialight 550-2206F	1	2.50
14	System Alarm LED - Dialight 550-2306F	1	2.50
15	RJ-45 GbE IT-IN - Amphenol RJE721881411	1	4.50
16	RJ-45 GbE OT-OUT - Amphenol RJE721881411	1	4.50
17	RJ-45 GbE IT-MON - Amphenol RJE721881411	1	4.50
18	RJ-45 GbE OT-MON - Amphenol RJE721881411	1	4.50
19	Quad GbE Magnetics - Bourns PT61018AAPEL	1	8.00
20	12V POL Regulator - Texas Instruments LM25085	1	4.00
21	5V POL Regulator - Texas Instruments TPS5450	1	5.00
22	3.3V POL Regulator - Texas Instruments TPS5430	1	3.00
23	1.8V Kria Core Supply - Analog Devices LTC3633	1	12.00
24	1.0V Kria Core Supply - Analog Devices LTC7130	1	15.00
25	Inter-Plane 40-pin Ribbon - Custom Shielded 40-way Ribbon Ca…	1	12.00
	Sub-total - electrical		5,719.50
26	1U Rack Chassis - Penn Elcom R1288/1UK 1U Rack Enclosure	1	125.00
27	EMI Isolation Divider	1	45.00
28	Industrial Front Bezel	1	65.00
29	DIN Rail Adapter - 1U Rack to DIN Rail Brackets	2	30.00
30	Governance Plane Heatsink	1	12.00
31	Network Plane Heatsink	1	14.00
32	PSU Retainer	1	5.00
33	PCB Standoffs - M3 Hex Brass Standoff Assortment	24	3.60
34	EMI Fingerstock - Laird Technologies EMI Gasketing	2	16.00
35	IEC C14 Locking Clip - Schurter 4700.0001 Cord Retainer	1	4.50
36	Front Panel Light Pipes	1	3.00
37	Managed Ethernet Switch Mount	1	2.00
38	TPM 2.0 Security Module Mount	1	2.00
39	Root of Trust Element Mount	1	2.00
40	IPMI BMC Controller Mount	1	2.00

Item	Component / Part number	Qty	Ext. (USD)
41	Form-C Fault Relay Mount	1	2.00
42	10G SFP+ Port A Mount	1	2.00
43	10G SFP+ Port B Mount	1	2.00
44	Power Indicator LED Mount	1	2.00
45	AUTHREX Armed LED Mount	1	2.00
46	System Alarm LED Mount	1	2.00
47	Network Plane Motherboard - Custom 4-Layer ENIG PCB (Network)	1	150.00
48	Governance Plane Mezzanine - Custom 4-Layer ENIG PCB (Govern…	1	75.00
	Sub-total - mechanical		568.10
	BARE-PARTS TOTAL		6,287.60
-	Documentation, ICD & assembly guide	1	1,500.00
-	Integration & first-article test	1	3,500.00
-	Engineering margin (~25%)	1	2,600.00
	TOTAL TYPICAL CONFIGURATION		13,887.60

47 BOM line items as finalized in Rev. A. Counting fasteners, ancillary passives, and per-position hardware, the assembled unit comprises approximately 92 components. Approximate reuse from the BLADE-INFRA parent design: 70%. Wiring is specified in the companion schematic (blade-infra-ot_bridge_SCHEMATIC.svg, 35 electrical edges); assembly is specified in the companion ICD-INFRA-OT Assembly Guide (Rev. A).

13 Compliance and alignment

Standard	Alignment claim
NERC CIP-005	Electronic security perimeter - bridge enforces and logs.
NERC CIP-007	System security management - config management for fail-bypass enable.
NERC CIP-008	Incident response - audit ledger export schema aligned.
NERC CIP-010	Configuration change management - signed policy bundles, dual-slot firmware.
FIPS 140-2	Cryptographic module boundary inherited from BLADE-INFRA HSM family.
IEC 62443	Conduit gateway between SL-1 IT zones and SL-3+ OT zones.
CISA Five Eyes OT (Dec 2025)	Reference implementation of joint principles.
CISA Five Eyes agentic AI (May 2026)	Bounded deliberation (FLAME) addresses agent-issued commands.
NIST SP 800-82 r3	Cross-walk for OT-security recommendations.
DoDD 3000.09	HMAA tier model lineage; human-on-the-loop posture maintained.
IEC 61850-3 / IEEE 1613	Substation EMC profile addressed in EMC test plan.
DoE C2M2	Audit and recovery domains aligned with maturity model.

14 Test and verification

This section defines the verification matrix that the BLADE-INFRA-OT appliance would be subjected to at fabricated-prototype maturity. The matrix is documentary for this revision; no items have been executed under this revision.

#	Verification item	Method	Acceptance
V-01	Mechanical fit (1U envelope)	Inspection	Within IEC 60297
V-02	Front-panel indicator function	Demonstration	All states reproducible
V-03	AC mains hold-up	Test	≥ 20 ms at full load
V-04	DC source hand-off	Test	≤ 5 ms gap, no traffic loss
V-05	Surge withstand, AC mains	Test (IEC 61000-4-5)	2 kV LL, 4 kV LE
V-06	ESD immunity, all ports	Test (IEC 61000-4-2)	±8 kV contact, ±15 kV air
V-07	Operating temperature, full envelope	Chamber test	–40°C to +70°C
V-08	Throughput, Modbus	Loadgen	10 kpps sustained
V-09	Latency, Modbus inline path	Capture analysis	≤ 250 µs typical
V-10	Latency, GOOSE accelerated path	Capture analysis	≤ 100 µs typical
V-11	Fail-closed on plane fault	Fault injection	Inline path opens within 50 ms
V-12	Fail-bypass when enabled	Fault injection	Relay closes within 10 ms
V-13	AUTHREX scenario 01 (nominal)	Sim playback	All msgs PROPAGATE, T3 sustained
V-14	AUTHREX scenario 02 (Monterrey)	Sim playback	ISOLATE on burst, T0 within 3 msgs
V-15	AUTHREX scenario 03 (maintenance)	Sim playback	FLAME window honored; T2 bounded
V-16	AUTHREX scenario 04 (coordinated)	Sim playback	MAIVA detects cross-sector
V-17	Audit ledger TPM signature chain	Cryptographic verification	BLAKE3 chain unbroken
V-18	Ledger export - JSON, XML, binary	Tool verification	Schema-conformant
V-19	Firmware rollback (dual slot)	Operational test	Rollback within 60 s
V-20	OOB air-gap (no data path leakage)	Network analysis	Zero packets cross boundary

15 Acronyms

AUTHREX	Authority Recovery & Execution framework
BACnet	Building Automation and Control Networks
BLADE	Boundary Layer Authority Domain Element (platform family)
BMS	Building Management System
CARA	Causal Authority Recovery Architecture
CIP	Critical Infrastructure Protection (NERC) / Common Industrial Protocol (CIP-EtherNet/IP)
CISA	Cybersecurity and Infrastructure Security Agency (US)
CIP-008	NERC CIP standard - Incident Reporting and Response Planning
DNP3	Distributed Network Protocol (IEEE 1815)
FLAME	Failure Latency Authority Management Envelope
FRU	Field-Replaceable Unit
GOOSE	Generic Object-Oriented Substation Event (IEC 61850)
HMAA	Human-Machine Authority Architecture
HSM	Hardware Security Module
ICD	Interface Control Document
IDS / IPS	Intrusion Detection / Prevention System
IFF	Identification, Friend or Foe
IPMI	Intelligent Platform Management Interface
MAIVA	Multi-Agent Independent Verification Authority
MMS	Manufacturing Message Specification (IEC 61850)
NERC	North American Electric Reliability Corporation
NSA	National Security Agency (US)
OOB	Out-of-Band (management channel)
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SATA	Sensor Authority Trust Allocation
SCADA	Supervisory Control and Data Acquisition
SOM	System-on-Module
SV	Sampled Values (IEC 61850-9-2)
TPM	Trusted Platform Module
TRL	Technology Readiness Level

16 References

[R1] Cybersecurity and Infrastructure Security Agency, Australian Signals Directorate Australian Cyber Security Centre, and National Security Agency. *Principles for the Secure Integration of AI in Operational Technology.* Joint publication, December 2025.

[R2] Cybersecurity and Infrastructure Security Agency and National Security Agency, with Five Eyes partners. *Careful Adoption of Agentic AI Services.* Joint advisory, 1 May 2026.

[R3] Dragos, Inc. *Monterrey water utility - AI-assisted IT-to-OT pivot attempt: threat intelligence report.* May 2026.

[R4] North American Electric Reliability Corporation. *CIP-005, CIP-007, CIP-008, CIP-010.* Critical Infrastructure Protection standards.

[R5] National Institute of Standards and Technology. *Guide to Operational Technology (OT) Security.* NIST SP 800-82 Rev. 3.

[R6] International Electrotechnical Commission. *IEC 62443 - Industrial communication networks - Network and system security.* Multi-part standard.

[R7] International Electrotechnical Commission. *IEC 61850 - Communication networks and systems for power utility automation.* Multi-part standard.

[R8] Institute of Electrical and Electronics Engineers. *IEEE 1815-2012 - Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3).*

[R9] Modbus Organization. *Modbus Application Protocol Specification V1.1b3.*

[R10] OPC Foundation. *OPC Unified Architecture Specification, Parts 1–14, Release 1.05.*

[R11] ODVA. *Common Industrial Protocol (CIP) and EtherNet/IP Specification.*

[R12] ASHRAE. *Standard 135 - BACnet, A Data Communication Protocol for Building Automation and Control Networks.*

[R13] U.S. Department of Defense. *Directive 3000.09 - Autonomy in Weapon Systems.*

[R14] Federal Information Processing Standards. *FIPS PUB 140-2 - Security Requirements for Cryptographic Modules.*

[R15] Telcordia. *SR-332 - Reliability Prediction Procedure for Electronic Equipment.*

[R16] U.S. Department of Energy. *Cybersecurity Capability Maturity Model (C2M2) v2.1.*

[R17] Oktenli, B. *AUTHREX: A Unified Authority-Lifecycle Framework for Autonomous and Semi-Autonomous Systems.* Zenodo, 2026.

[R18] Stouffer, K., Pillitteri, V. et al. *NIST Cybersecurity Framework 2.0.* National Institute of Standards and Technology, 2024.

[R19] Mitre. *ATT&CK for Industrial Control Systems.* Knowledge base of adversary tactics and techniques targeting ICS.

[R20] Stuxnet retrospective: Falliere, N., Murchu, L. and Chien, E. *W32.Stuxnet Dossier.* Symantec, 2011.

