T2

Tier 2 · Unified Connectivity Hub

Technical Specification

Protocol Bridges, UNS Architecture, and Closed-Loop Control Design

Version	1.0
Status	PRODUCTION
Zone	OT / IT Bridge
Standards	MQTT SparkplugB / OPC-UA IEC-62541 / Modbus TCP / ISA-88
Block Count	7 blocks
Document Date	May 2026

1. Technical Overview

Tier 2 bridges the OT and IT zones. It consumes the T1 enriched message contract and either publishes upward to enterprise systems or sends commands downward to field devices. Seven blocks implement three functional groups: UNS namespace construction, protocol translation, and enterprise/control integration.

1.1 Message Flow

```
// Upward (OT → IT)
T1 enriched msg
  → UNS Builder (constructs topic)
  → MQTT Bridge SparkplugB (encodes & publishes)
  → Enterprise Gateway SAP/MES (confirms to ERP/MES)

// Downward (IT → OT) — Closed Loop
T3 Anomaly Detection event
  → Action Logic Engine (reads Impact Array)
  → MQTT cmd topic / Modbus write (commands machine)
  ← ACK received (Port 2) or timeout (Port 3)
```

1.2 Command Message Schema

```
// Command issued by Action Logic Engine
{
  targetAssetId:  "uuid-of-control-module",
  type:           "interlock" | "setpoint" | "mode-change",
  command:        "STOP" | "START" | "SET_SP" | "RESET",
  value:          number | string | null,
  issuedAt:       "ISO 8601",
  correlationId:  "msg._msgid"
}

// Published to MQTT topic:
// {Enterprise}/{Site}/{Area}/{Line}/{Cell}/cmd
```

2. Block Specifications

2.1 UNS Builder

ID	uns-builder
Type	function + mqtt-out
Standard	ISA-95 Part 2 / MQTT 5
Topic pattern	{Enterprise}/{Site}/{Area}/{Line}/{Cell}/{tagId}
Validation	Each component must match /^[a-zA-Z0-9_-]+$/ — rejects on Port 2 otherwise
QoS	0 (fire-and-forget), 1 (at-least-once, default), 2 (exactly-once)
Retain	retainBirth=true sends BIRTH packets with retain flag set

2.2 MQTT Bridge (Sparkplug B)

ID	mqtt-sparkplugb
Type	function + mqtt-out
Standard	Sparkplug B v1.0 / MQTT 5
Encoding	Protobuf encoding per Sparkplug B specification (google-protobuf library)
Alias compression	Numeric alias map reduces topic metric name payload size after NBIRTH
Sequence numbers	uint64 seqCounter auto-incremented per NDATA publish; resets on NBIRTH
TLS	Client certificate and CA bundle configurable for mTLS (mutual authentication)
Output 1	Decoded JSON from incoming Sparkplug B messages
Output 2	Encoded Protobuf buffer for outgoing MQTT publish
Output 3	NDEATH payload { twinId, timestamp } on connection loss

2.3 OPC-UA Bridge

ID	opcua-bridge
Type	opcua-client + mqtt-out
Standard	OPC-UA / IEC 62541 (node-opcua library)
Subscription	Creates OPC-UA Subscription with configured publishingInterval; adds MonitoredItems per nodeId

Reconnect	Exponential backoff: 1s → 2s → 4s → max 30s; session recovery preserves monitored items
Deadband	Absolute deadband applied in Node-RED before MQTT publish (not OPC-UA server-side)
nodeUoMMap	Internal Map<nodeId, euString> populated from T1 tag model on startup

2.4 Modbus TCP Bridge

ID	modbus-bridge
Type	modbus-read + function
Standard	Modbus TCP (node-red-contrib-modbus)
Register types	Holding registers (default), Input registers, Coils, Discrete Inputs
Scaling formula	scaledValue = rawValue * gain + offset (per register map entry)
Error handling	Port 3 fires on Modbus exception codes 01–11 and TCP timeout

2.5 Enterprise Gateway (SAP)

ID	enterprise-gateway-sap
Type	function + RFC/OData + http
Standard	SAP PP_PROD_CONF_SRV OData v2; BAPI_PRODORD_CONFIRM via RFC
Auth methods	Basic Auth, OAuth2 (client credentials), SAP-specific CSRF token
Retry	No automatic retry — wire Port 2 to a retry subflow for idempotent operations
Idempotency	SAP confirmation BAPIs are idempotent when OrderID + PostingDate match

2.6 Enterprise Gateway (MES)

ID	enterprise-gateway-mes
Type	function + OPC-UA + REST + MQTT
Standard	ISA-95 Part 2 / Multi-MES
Direction control	msg.payload.direction = "inbound" | "outbound"
Retry	retryOnFail attempts (default 3) with 1s delay between retries
Timeout	timeoutMs (default 5000ms) — Port 2 fires on timeout

2.7 Action Logic Engine

ID	action-logic-engine
Type	function + mqtt-out + modbus-write
Standard	ISA-88 Phase / IEC 61131-3 Command Model
Input	msg.payload = { impactArray: string[], triggerType: string, triggerValue: any }
Action map	JSON file at actionMapPath keyed by assetId → triggerType → rule
Dry-run	dryRun=true logs commands to node.warn without publishing — always test first
ACK mechanism	Devices must publish to {unsTopic}/ack with { correlationId } to confirm execution
Timeout	ackTimeoutMs (default 3000ms); maxRetries (default 2) before Port 3 fires
Output 1	Command issued successfully
Output 2	ACK received from target device
Output 3	Command failed — ACK timeout exhausted or dry-run result

3. Security Considerations

3.1 MQTT TLS

All MQTT connections should use TLS (port 8883). For mTLS, provide client certificate and private key in the MQTT broker config node. Never disable TLS in production.

3.2 OPC-UA Security

Set OPC-UA security mode to SignAndEncrypt with SecurityPolicy Basic256Sha256 in production. Anonymous mode is acceptable for development only.

3.3 Action Logic Engine Safety

- Always run with dryRun=true and review the warn log before enabling live commands.
- Implement a hardware safety relay or PLC interlock as a last-resort backstop independent of the ALE.
- Log all issued commands via T3 Audit Logger by wiring ALE Port 1 to the Audit Logger input.
- Set maxRetries conservatively (default 2). Repeated commands can cause mechanical damage.