Beyond Purdue: The Data Plane

Implementation and Deployment Plan V1.1 | 6 November 2026 | Petr Roupec, BM Global | INTERNAL

1. Purpose and scope

This plan describes how the data plane of the concept document (Beyond Purdue - Data Plane Concept V1.0) is built, tested and deployed: from a written specification, through a bench, a read-only shadow pilot at one plant and headquarters, to a full unit and then the fleet. Plant, unit and host names are examples (plant.example, RFC 2606). Durations are planning estimates, to be confirmed after the bench. Prices, offers and commercial choices are not part of this plan.

2. Rules that hold in every phase

- **The laws first.** Every phase obeys the laws of authority. The data plane holds and serves; it never commands.
- **Data in independent nodes, named first.** A node is built only once it has a name and its aliases. Naming and asset management is planned before any software is installed (section 6).
- **At least two copies.** Every node, the registrar and the names run in at least two copies, on different hardware, power and rooms, from the first day of the bench.
- **Read only first.** Until phase 5 the data plane only listens. It never writes into L0 or L1 and changes nothing in the controllers.
- **Protection stays hardwired.** Nothing in this plan touches protection or isolation. Locks stay with the people at work; the data plane only reads them.
- **One way, by construction.** Every path into or out of the plant is a data diode, passive by preference. The diode is the enabler. Nothing is installed that needs a reply across a diode.
- **Nothing is switched off.** The existing historian and HMI keep running. The data plane runs beside them until it is accepted, and longer if the plant wants.
- **A gate after every phase.** A phase ends only when its tests pass. The next phase starts on your decision.
- **Human-free after installation.** People rack, cable and load the tag list. After that, nodes are born, copied, moved and retired by shouts.

3. Software components

Program	Runs on	Built with	Does
Edge adapter	behind each L1 gate	Rust. Pilot: Node-RED flows already in use (for example the ION reader)	Reads the controller or meter, applies the delta, shouts CHANGE, REPEAT, HEARTBEAT; later EXECUTED
Node host	every L3 host	Rust	Runs many nodes in one process. Each node: own IPv6 address, on-change history file, alarms, meaning text, answers to ASK
R worker	every L3 host	R, DEWA layer scripts unchanged	Runs the node analysis in turn for all nodes on the host; results go back into each node
Keeper	every L3 host	Rust	Listens to heartbeats; starts a copy when fewer than two remain; the hash of the name decides which host
Registrar	two L3 hosts	standard authoritative DNS server plus Rust	Holds and signs the zone; turns NEWTAG into names and addresses; shouts NAMES in a carousel
Forwarder	each diode	Rust	Hears a group on one side and shouts it again on the other side
HQ listener	HQ hosts	open62541 (OPC UA, C)	Builds its address space from NAMES and serves values read only to office clients
Permit adapter	beside the permit system	Rust	Reads permits from the permit or maintenance system through its own one-way gate and shouts them into permit nodes (concept section 17)
Maintenance out channel	one L3 host	Rust	Serves plant states, permits and lock records one way out to the maintenance system (CMMS) and the permit system
GIVEN shouter	each HMI console (phase 5)	Rust library	Shouts GIVEN for every command through the console's own diode

One code base for all Rust programs, one signed host image for all hosts. A host becomes a node host, registrar or forwarder by its name in the zone, not by different software.

4. The shout format (fixed in phase 0)

Field	Content
kind	CHANGE, REPEAT, HEARTBEAT, ASK, ANSWER, NEWTAG, NAMES, BORN, MOVED, RETIRED, GIVEN, EXECUTED
name id	short id of the canonical name; the full name is in the zone
state number	goes up on every change (as stNum in GOOSE)
sequence number	goes up on every repeat (as sqNum in GOOSE); every gap is visible to the receiver
source time	time at the source, with time quality
value, unit, quality	the value as measured, never resampled
writer key id, signature	Ed25519 (RFC 8032), checked by every receiver
ask fields	request number, answer group, answer window (ASK and ANSWER only)

Encoding CBOR (RFC 8949). One shout is one UDP datagram on an IPv6 multicast group, under 200 bytes for a value. Large objects (zone, history segments, host images) are shouted with forward error correction (FLUTE, RFC 6726, with RaptorQ, RFC 6330) in a carousel.

5. Network and address plan

- **Prefix.** One unique local IPv6 prefix per plant (RFC 4193), split by unit and system, so the address says where a node belongs. Example:

```
plant.example       fd12:3456:789a::/48
u1                  fd12:3456:789a:1000::/52
boiler.u1           fd12:3456:789a:1114::/64   hp-steam ::114:1 and ::114:2
groups              boiler.u1 data, ans.u1, names, cmd.u1 (RFC 3306 based)
```

- **Groups.** One data group per system, one answer group per unit, one names group per plant, one command record group per unit.
- **Switches.** MLDv2 (RFC 3810) with MLD snooping (RFC 4541) and a querier on every L3 segment. Each group stays inside one switched segment; forwarders join segments. No multicast routing in the plant.
- **Separate from today.** The L3 network is its own segment set. It touches the control network only through the L1 gates (diodes).

6. Names plan

- **Zone.** plant.example, signed with DNSSEC (RFC 9364). Every host keeps a full local copy and resolves locally.
- **Records.** AAAA for each copy of a node; TXT for class (event or normal), meaning text reference and writer key id; aliases for every other name (KKS, vendor tag, HMI name, meter number).
- **Three ways to update.** A name is updated automatically when a node is born, by a person at the HMI or engineering station, or by a shout from equipment. Each ends as one signed change from the registrar.
- **Diode inventory.** Every diode is named before it is installed, like any other asset: dd01.u1.plant.example, with aliases by level, asset number and cabinet. Its node records type (passive or active), direction and channel, what it carries, its plant state and the result of its one-way test. Only the sending side writes the record; out and in diodes are never linked in one record.

Diode	Sends	Receives	Direction	Carries
dd01	L0 Protection and isolation	L3 Data nodes	out	Protection records
dd02	L1 Controller	L3 Data nodes	out	Process data, executed
dd03	L4 Operator	L3 Data nodes	out	Commands given
dd04	L3 Data nodes	L4, L5, HQ readers	out	Data to readers, first path
dd05	L3 Data nodes	L4, L5, HQ readers	out	Data to readers, second path. Same data as dd04, from a different host, so a failed diode or host loses nothing.
dd11	L4 Operator	L1 Controller	in	Commands, on their own lane

Every name is in u1.plant.example (for example dd05.u1.plant.example). All are passive by preference and in service in the example. The inventory matches Drawing M.

- **Changes.** Only the registrar edits the zone (RFC 2136). Every change is signed and shouted on the names group; the full zone is shouted in a carousel, so a host that missed a change catches up. No zone transfer and no NOTIFY across a diode, because both expect a reply (RFC 1996).

- **First load.** The tag list from the plant (KKS, description, unit, range, delta) is turned into NEWTAG shouts. An electrician or technician checks the mapping; nobody writes code.

7. Time plan

- **Each side its own clock.** One GPS grandmaster per side of every diode (two where the budget allows), PTP to the hosts and adapters with linuxptp (ptp4l).
- **Quality.** Every shout carries time quality. When a host loses its clock it keeps running and marks its shouts.
- **Checks.** Two copies on different hosts compare their arrival times; a drifting host clock is visible in the heartbeat and raises an alarm.

8. Keys

- **Writer keys.** One key per adapter, per registrar, per forwarder and (phase 5) per HMI console. The public keys are in the zone; nodes accept only the key named for them.
- **Root key.** Kept offline. It signs the registrar keys and the host image.
- **Rotation.** A new key is shouted signed by the old one and the registrar; both are valid for an overlap period.
- **Command authorization.** Who is allowed to command, refused commands, authentication nodes: kept for later (concept section 16).

9. Hardware

Item	Bench	Pilot (one plant)	Note
L3 hosts	3	3 to 6	Low-cost industrial mini PCs, at least two makes, so one fault cannot take all copies. Number set from the bench load test
Switch with MLD snooping	1	1 per L3 segment	Group limit to be checked for the real switch model
Diode, L1 gate	1	1 per data source	Cheap fibre transmit-only link with forwarder
Diode, plant to HQ	1	1	Can be an existing diode if it passes UDP multicast or a forwarder pair
Diode, L4 record gate	0	0 until phase 5	One per HMI console group
GPS grandmaster	1	1 per side	Holdover rated
HQ hosts	1	2	Run HQ copies and the OPC UA listener
Rack, power, UPS	bench	per site	From plant standard

10. Phases

Phase	Goal	Main work	Gate	Estimate
0 Spec	Freeze what everybody builds to	Shout format and kinds, address plan, names rules, key handling, test list with pass limits	Spec approved by you	2 to 3 weeks
1 Bench	Prove the shouts work	Write the programs; three hosts, one switch, one diode, GPS; DEWA data replayed as a fake plant	All bench tests pass (section 12)	6 to 8 weeks
2 Shadow pilot	Prove it on a real plant, read only	Site survey, permits, install, 100 to 500 tags from one existing read-only data source, parallel run beside the existing historian	Values match, no unexplained gaps, survival tests on site	8 to 12 weeks, of which 4 parallel run
3 HQ and AI	Office and AI read without touching the plant	Plant to HQ forwarder, HQ copies, OPC UA listener, historian and dashboard listeners, AI 24 h question	HQ clients served only by HQ copies; nothing crosses back	4 to 6 weeks
4 Full unit	All signals of one unit	Waves by system (boiler, turbine, electrical, BOP); more hosts as sized; tag list per wave	Each wave passes the pilot tests	per unit, from pilot result
5 Command record	L3 knows every command	GIVEN shouter in the universal HMI, EXECUTED in the adapter, L4 record diode, cmd nodes	Every test command paired; missing EXECUTED raises an alarm	with the universal HMI

Phase	Goal	Main work	Gate	Estimate
6 Fleet	Next units and plants	Same image and template; new prefix and zone per plant	As phase 4	per site

Phases 0 to 3 are about 5 to 7 months if run one after another. Phase 3 can start during the phase 2 parallel run.

11. Deploying one plant, step by step

1. Survey. Data sources available read only (OPC, archive interface, meter ports), rack space, power, fibre routes, time source, switch models.

2. Agree the source and the permit. Which interface is read, by which adapter, with the plant's written permit. No change to controller configuration.

3. Rack, power, cable. Hosts, switch, GPS, diodes.

4. Prove one way. For every diode: send from the receiving side and confirm nothing arrives on the sending side. Record the result on the node of the diode.

5. Time. Grandmaster locked, all hosts and adapters within the agreed limit.

6. Image the hosts. One signed image; each host gets its name; registrar starts on two hosts.

7. Load the tag list. Tag list turned into NEWTAG shouts; the technician checks the mapping table.

8. Start the adapters. Nodes are born by themselves, two copies each, on different hosts. Check: every name has two copies.

9. Parallel run. Values, events and gaps compared every day against the existing historian. Breaker positions, lock contacts and permit records are read too, so L3 shows each plant state beside the permit register.

10. Acceptance and handover. Section 12 tests on site; report; the plant decides.

12. Acceptance tests

Test	How	Pass (proposed, fixed in phase 0)
One way	Send from the far side of each diode	Nothing arrives
Change delivery	Step a replayed or real value	Both copies hold it within the agreed time
Lost shouts heal	Drop packets on purpose (network emulator, for example 5 % loss)	No value lost; gaps visible and closed by the repeat
Copy survives	Pull the power of a host	Second copy keeps serving; a new copy is born on another host within the agreed time
Ask	Ask the same question many times	One answer per request; copies do not both answer
New tag	Shout NEWTAG for an unknown signal	Name, two addresses and two copies appear without a person
Names cross	Change a name on the plant side	HQ zone and OPC UA tree follow
Time	Unplug the GPS antenna	Shouts marked with lower time quality; alarm raised
Match	Parallel run against the existing historian	Same values and events within the agreed tolerance
Permit match	Release one item for work with its permit and lock, then return it	State shown as released for work and back; permit and sensed lock paired; a lock without a permit raises an alarm
Command record (phase 5)	Give test commands, and one that is not executed	All paired; the missing one raises an alarm

13. After handover

- **No daily care.** The keeper restarts and moves copies. A dead host is replaced by plugging in a new imaged host; it is given work by shouts.
- **Monitoring is listening.** Heartbeats show every host and node; HQ sees the same through the diode.
- **No backups to run.** Every node has two copies on site and one at HQ.
- **Software updates.** A new signed image is shouted in a carousel; hosts change one copy at a time, never both copies of a node together.
- **Retiring a tag.** RETIRED shout from the registrar; history stays at HQ.

14. Who does what

Party	Part
BM Global	Specification, software, bench, commissioning, tests, documentation
Plant	Permits, access, tag list, choice of the read-only data source, witnessing the tests, acceptance
Site technician or electrician	Racking, cabling, checking the tag mapping
HQ IT	HQ hosts, office clients on the OPC UA listener

15. Risks

Risk	What we do
Switches cannot hold enough multicast groups	Check in the survey; fewer, larger groups per system
No clean read-only data source	Use what the plant already exports through its existing diode; never connect to controllers without a permit
Controller cannot report a command as executed	Read the feedback signal instead (valve open, breaker closed); decided per controller type in phase 5
A cheap host carries fewer nodes than expected	Bench load test sets the number; add hosts, the software does not change
R worker too heavy for small hosts	Run analysis on fewer, stronger hosts; nodes keep the results only
Clock problems at a site	Time quality on every shout; two grandmasters where possible

16. Open points

- **Pass limits** for every acceptance test (phase 0).
- **Read interface** per controller and meter type at the pilot plant.
- **Switch models** and their MLD group limits.
- **Pilot plant and tag set** (your choice).
- **Command authorization** for phase 5 and later.

17. References

Beyond Purdue - Data Plane Concept V1.0 (internal). Drive folder 2026-10-29 - Data Plane Concept
RFC 2606, reserved example names. https://www.rfc-editor.org/rfc/rfc2606
RFC 4193, unique local IPv6 addresses. https://www.rfc-editor.org/rfc/rfc4193
RFC 3306, unicast-prefix-based IPv6 multicast addresses. https://www.rfc-editor.org/rfc/rfc3306
RFC 3810, MLDv2. https://www.rfc-editor.org/rfc/rfc3810
RFC 4541, IGMP and MLD snooping. https://www.rfc-editor.org/rfc/rfc4541
RFC 8949, CBOR. https://www.rfc-editor.org/rfc/rfc8949.html
RFC 8032, Ed25519. https://www.rfc-editor.org/rfc/rfc8032
RFC 6726, FLUTE. https://www.rfc-editor.org/rfc/rfc6726
RFC 6330, RaptorQ. https://www.rfc-editor.org/rfc/rfc6330
RFC 2136, DNS UPDATE. https://www.rfc-editor.org/rfc/rfc2136
RFC 1996, DNS NOTIFY. https://www.rfc-editor.org/rfc/rfc1996
RFC 9364, DNSSEC. https://www.rfc-editor.org/rfc/rfc9364
RFC 6762, multicast DNS (random answer delay). https://www.rfc-editor.org/rfc/rfc6762
GOOSE state and sequence numbers. https://www.learn61850.com/pages/goose-structure.html
GOOSE retransmission (ABB AC500). https://help.plc.abb.com/AB270_en/3d245e8f427944dfc33528ee7a40e297_2_en_us.html
linuxptp ptp4l. https://linuxptp.nwtime.org/documentation/ptp4l/
open62541 OPC UA. https://open62541.org/doc/v1.5.6/