Beyond Purdue: Levels of Authority Drawings

Drawings A, B, C, D, K and M | V1.1 | 6 November 2026 | Petr Roupec, BM Global

Evaluation

Drawing	Shows well	Watch	Best use
A. Authority against physical and virtual	Clean and direct: the vertical axis now means authority, not position. Each level has a virtual and a physical side. L5 has no physical side; L0 has no in lane.	The command from the HMI has to cross L3 (drawn as a bridge that touches nothing).	Engineering explanation of each level.
B. Diagonal: process against context	The data plane is visible as the border between the physical process and the context of humans and AI.	Authority is not on an axis; the levels are read from their positions.	Cover, website hero, LinkedIn.
C. Combined	Authority, machine / human control and the data plane in one view. Only L0 and L1 touch the process; humans and AI have no physical side. Every gate sits on the border of the data plane.	Needs to be shown large.	Main reference: founding document, website home.
D. Data plane as a name space	Every L3 node as its own small page with a name. Who writes (equipment, machines, humans, AI, documentation) and who reads, each through its own gate.	Example names only; the naming scheme is still to be decided.	Website, engineering and community explanation.
K. Four plant states	What each level is allowed to do while part of the plant is in service, released for work, under test or returning to service. The lock sits in L0 and outranks every level.	Cells are short on purpose; the detail lives in the Maintenance is Operation paper.	Maintenance and safety explanation, training.
M. The enablers	Every data diode as a named asset: who sends, who receives, and the node of the diode with its name, type, direction, what it carries and its plant state. Aliases find the same node.	Principles only; no detail of how a diode is built.	Data plane and security explanation.

Shall L2 and L3 sit next to each other?

Yes, both belong between the physical and the virtual world, together forming the data plane. L2 should surround L3 rather than sit beside it: L2 is the only level that touches both worlds, and L3 sits inside it and is reached only through L2. Drawn this way, the command lane runs in L2 between the L3 nodes and never passes through them.

How the data plane is shown and updated

Each L3 node is shown like a small web page: its name in brackets on top, as in a browser address bar, and its content below (value, time, history, alarms, meaning, aliases, links to the asset and the manual, notes). The node stands alone; there is no central database.

- **Names.** A node has one name in a hierarchy (signal, unit, plant), and plant, vendor and drawing identifiers point to it as aliases, the way DNS canonical names work (RFC 1034, https://www.rfc-editor.org/rfc/rfc1034). The drawing uses the reserved example domain (RFC 2606, https://www.rfc-editor.org/rfc/rfc2606) instead of a real plant name.
- **Writers.** Equipment registers itself once; machines (L0, L1, meters) write automatically; humans write notes on the HMI, signed with their level; AI writes advice, labelled as AI; documentation is published once and linked by name. Each writes only into its own node, through its own one-way gate.
- **Readers.** Anyone reads by any of the names through an out gate. A name finds data; it never grants authority.
- **Open points.** The naming scheme, how a node proves who wrote it (for example with signed names, DNSSEC, RFC 9364, https://www.rfc-editor.org/info/rfc9364), and how names are offered to the HMI.

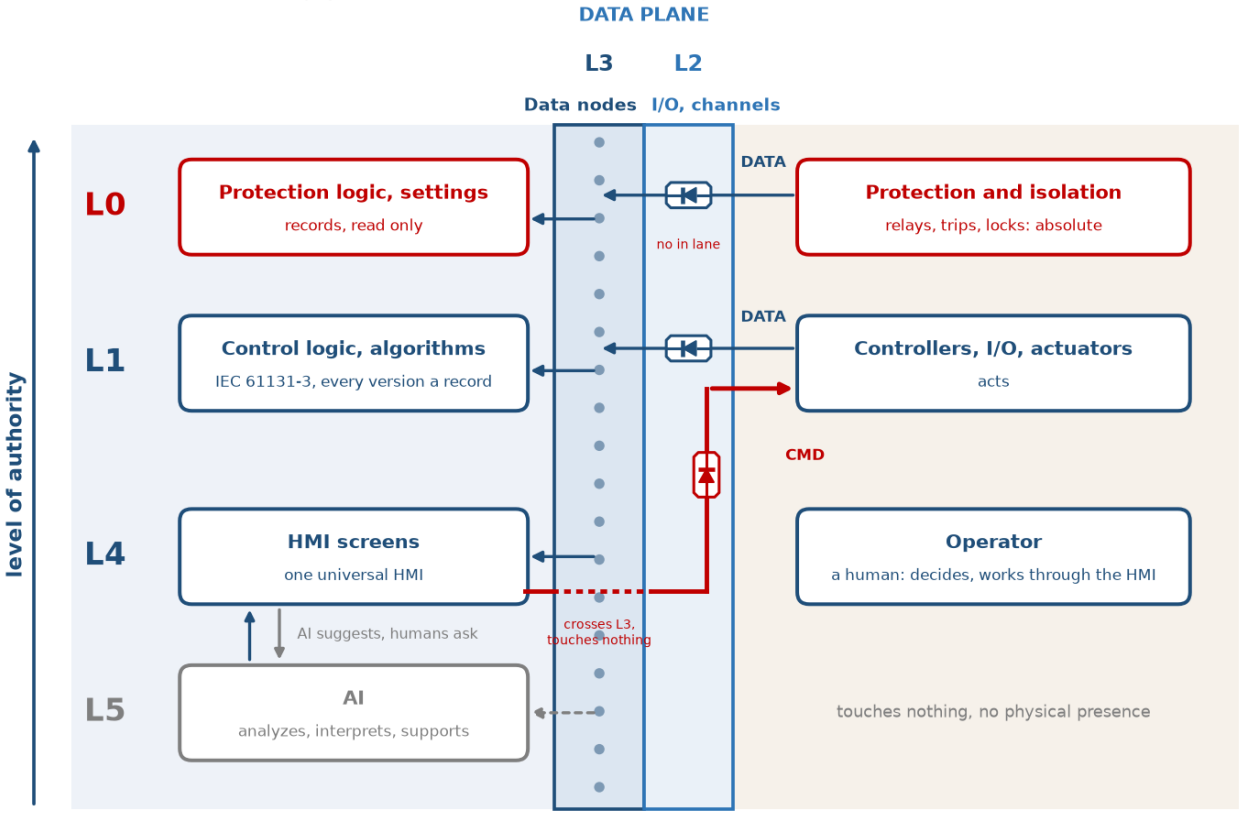
Notes

- **Naming.** "Data core" is replaced by L3 Data nodes, the original level name.
- **Original levels kept.** L0 Protection and isolation absolute, L1 Controller acts, L2 gatekeeper, L3 holds and serves, L4 Operator decides, L5 AI voice, no vote.
- **Inspiration from the passive diode work.** Only the principle is used, not the disclosure: one-way by construction, and data out and commands in as separate lanes that share nothing. The disclosure is unfiled, so nothing specific to it appears in the drawings.
- **AI dialogue.** AI and humans talk both ways: AI suggests and explains, humans ask. It is dialogue, not command; the advice is kept in the L5 nodes.
- **Diodes.** Every one-way channel uses the same inline component: the wire enters one end and leaves the other, with the diode symbol inside pointing in the direction of flow.
- **Dropped.** The circle on two axes.

- **Changes in V0.2.** L0 is renamed Protection and isolation: isolation is there because of maintenance, and the lock is the simplest protection device. The tagline now reads "allowed to do". Drawing K is new.
- **Changes in V1.0.** Drawing M is new: the data diode as the enabler and as a named asset.
- **Changes in V1.1.** Drawing M adds dd05.u1.plant.example: a second out diode from the L3 Data nodes to the readers (L4, L5, HQ), so data leaves on two paths.

Drawing A. Authority against physical and virtual

Each level has a virtual and a physical side. L2 and L3 form the spine between the two worlds

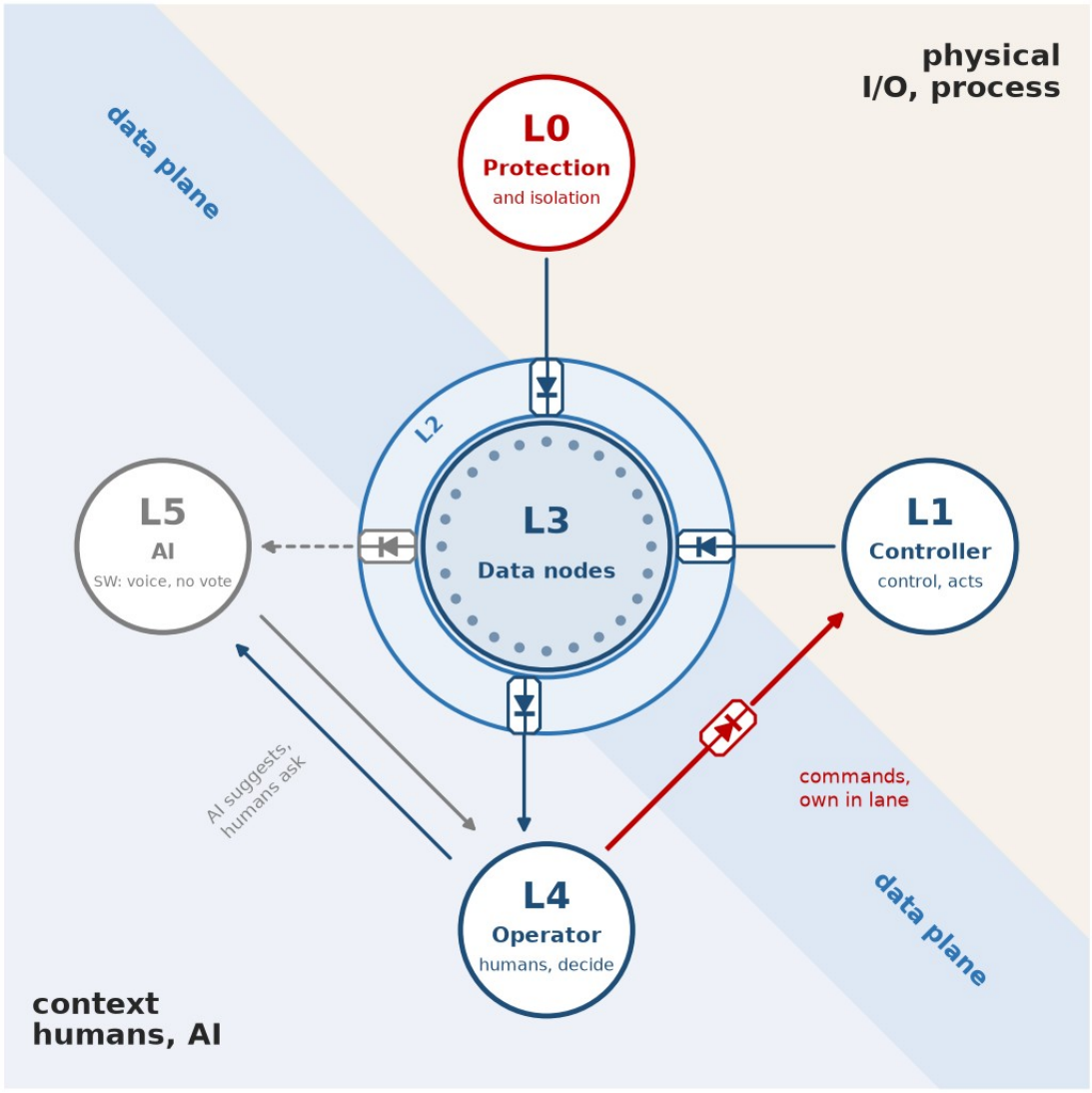


Purdue sorts devices by where they sit. Beyond Purdue sorts them by what they are allowed to do.

Level of authority on the vertical, the L3 and L2 spine (the data plane) between the two worlds, each level split into its virtual and physical side. AI and humans talk both ways: AI suggests, humans ask.

Drawing B. The diagonal: process against context

The data plane is the border; physical I/O and process on one side, humans and AI on the other

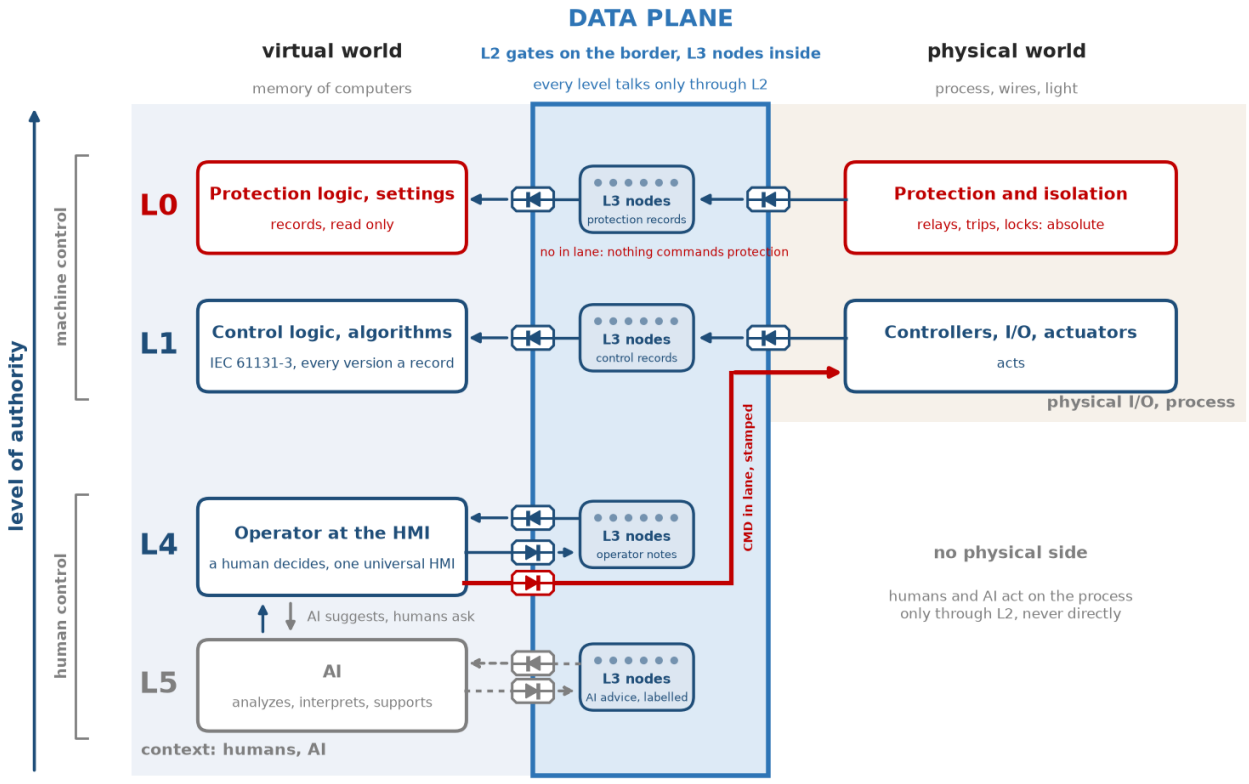


Purdue sorts devices by where they sit. Beyond Purdue sorts them by what they are allowed to do.

Physical I/O and process top right, context, humans and AI bottom left, the data plane as the diagonal border. AI talks with the operator both ways; only the operator commands.

Drawing C. The Levels of Authority and the data plane

Only L0 and L1 touch the process. Humans and AI act only through L2. Every gate sits on the border of the data plane



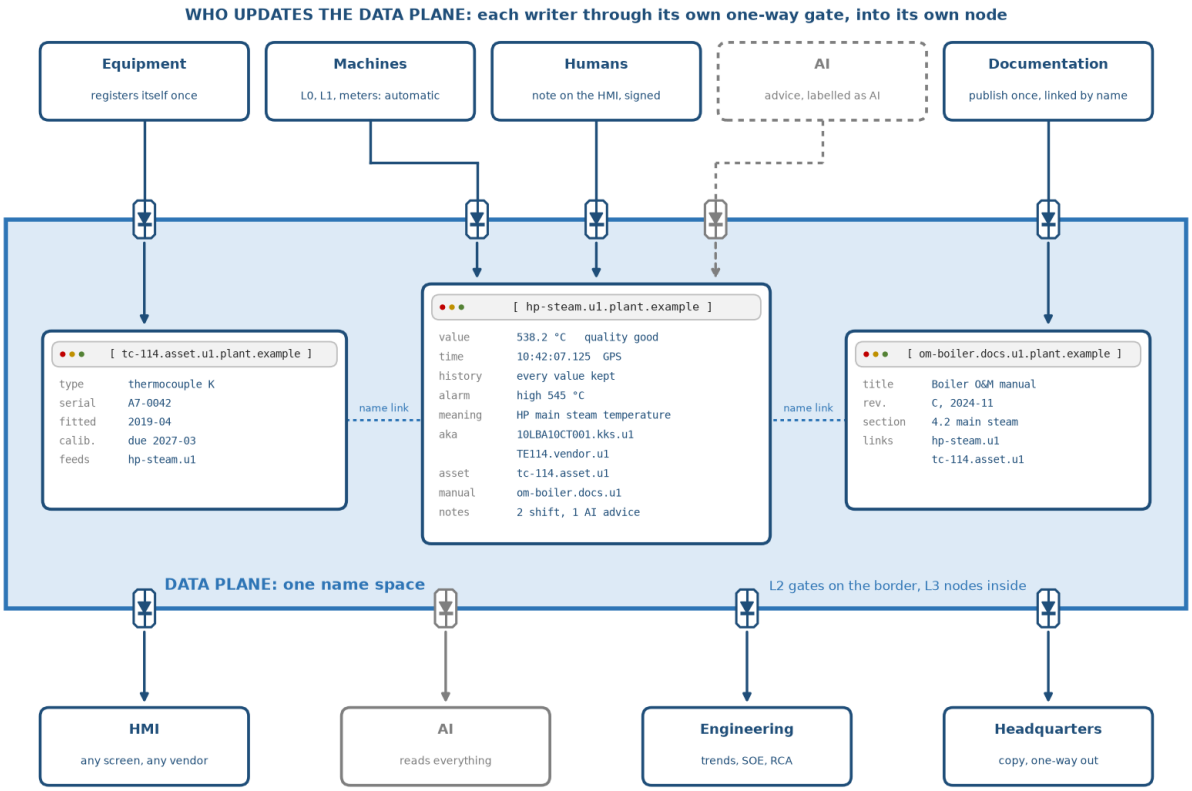
Purdue sorts devices by where they sit. Beyond Purdue sorts them by what they are allowed to do.

Commands flow only on their own in lane, never through L3, never from AI. Every L3 node has its own name: see Drawing D.

Read it row by row: each level of authority has its own L3 nodes inside the data plane, and every gate sits on its border. Only L0 and L1 touch the process; humans and AI act only through L2. AI suggests, humans ask; commands come only from the operator on their own lane.

Drawing D. The data plane as a name space

Every L3 node is its own small page with its own name. Writers fill their own node; readers ask by name. No central database.



Names: hp-steam.u1.plant.example and its aliases (KKS, vendor tag) resolve to the same node. Commands never pass through the data plane.

Each L3 node is its own small page with its own name in brackets. Equipment, machines, humans, AI and documentation each update their own node through their own one-way gate; HMI, AI, engineering and headquarters read by name through out gates. Names are examples.

Drawing K. Four plant states across the six levels

People work inside the plant. Their safety is designed in, not added.

	In service	Released for work	Under test	Returning to service
L0 Protection and isolation	Trips. Veto over every level.	**Holds the lock. Trips stay live.**	Bypass only by key at the panel, timed.	Every bypass cleared.
L1 Controller	Acts within protection limits.	Shouts "released for work". Never starts.	Runs the test scope only.	Starts on the L4 decision.
L2 Channels	Data out, commands in.	In lane closed by the key.	In lane open for the test only.	In lane reopened when the key returns.
L3 Data nodes	Records every command.	Records permit, lock, bypass. Alarms on mismatch.	Records the test and the bypass timer.	Shows "ready" or what is missing.
L4 Operator	Decides.	Never commands a locked machine.	Commands within the test permit.	Decides the return.
L5 AI	Voice, no vote.	Checks. Never signs.	Watches limits and time.	Summarises the evidence.

A lock outranks every level.

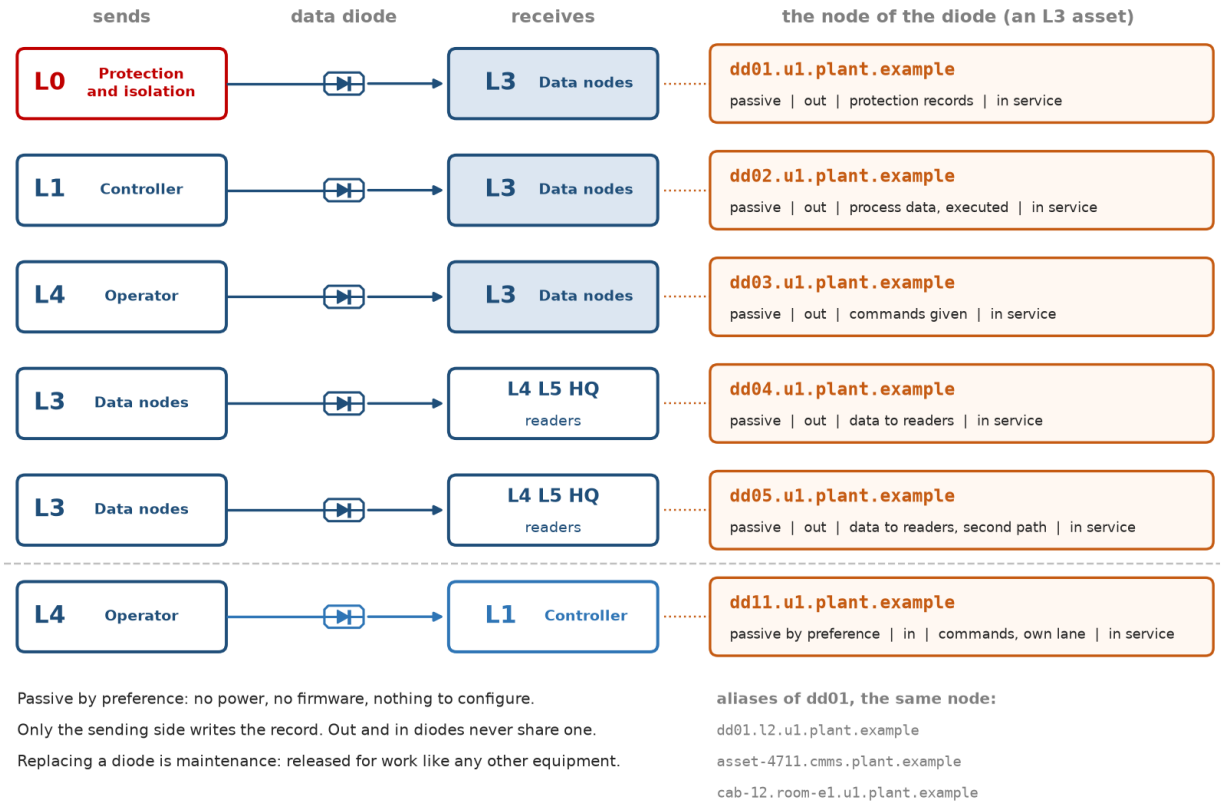
The emergency stop stops a machine; only the lock keeps it stopped.

Purdue sorts devices by where they sit. Beyond Purdue sorts them by what they are allowed to do.

People work inside the plant, so maintenance is part of operation. Each row is a level, each column a plant state. L0 holds the lock while someone works; no level commands a locked machine. The emergency stop stops a machine; only the lock keeps it stopped (ISO 13850, https://www.iso.org/standard/59970.html).

Drawing M. The enablers: every data diode is a named asset

Light travels one way, so data and commands cannot mix. The levels hold because the diode holds.



Passive by preference: no power, no firmware, nothing to configure.

Only the sending side writes the record. Out and in diodes never share one.

Replacing a diode is maintenance: released for work like any other equipment.

aliases of dd01, the same node:

`dd01.l2.u1.plant.example`

`asset-4711.cmms.plant.example`

`cab-12.room-e1.u1.plant.example`

Purdue sorts devices by where they sit. Beyond Purdue sorts them by what they are allowed to do.

The data diode is the enabler. Light travels one way, so data and commands cannot mix, and the levels hold because the diode holds. Each diode is an L3 node with a DNS-style name and aliases (RFC 1034, https://www.rfc-editor.org/rfc/rfc1034). Out diodes carry data and records; dd04 and dd05 carry data to the readers on two separate paths, so a failed diode loses nothing. The in diode carries commands on its own lane. Passive by preference (NIST glossary, data diode, https://csrc.nist.gov/glossary/term/data_diode).