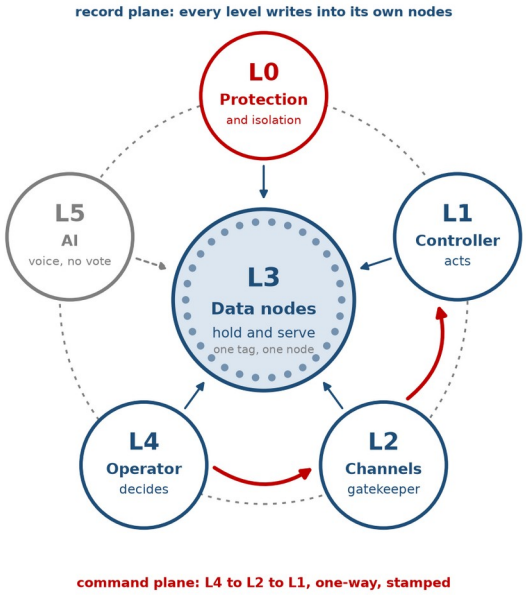
Beyond Purdue: Eight Questions by Level of Authority

Answers for Mr. Sunil (ENGIE) | V1.0 | 3 November 2026 | Petr Roupec, BM Global



1. The levels of authority

L0 Protection and isolation: absolute. Trips and overrides everything. Holds the lock.
L1 Controller: acts, within its logic and protection limits.
L2 Channels: gatekeeper. Data out, commands in, never mixed.
L3 Data nodes: hold and serve. No authority at all.
L4 Operator: decides.
L5 AI: analyzes, interprets, supports. Voice, no vote.

2. Not a hierarchy

- **Data nodes in the centre.** Every level writes its own records into its own nodes, protection included, directly.
- **One tag, one node.** Own IPv6 address, history, description and meaning. DNS gives one node all its names: field, KKS, OPC UA, authority.
- **Two planes.** The record plane is wide and flows out only. The command plane is narrow, one-way in, every command stamped with who issued it and from which level.
- **Authority decides who is allowed to act, not who is allowed to see.** Everyone is allowed to read; very few are allowed to command.
- **Everything stays on site.** An external database is just one more reader on the out channel.

3. The eight questions, each assigned to its level

#	Question	Level	Answer
1	**Can the listening point be a vulnerability?**	L2	It has no way back into the plant: passive and one-way by construction (data diode or passive tap). The data diode is the enabler, named and tagged like any other asset. At worst it can be fooled or go blind; it can never command. Protection never depends on it.
2	**Is it possible to develop logics?**	L1	Yes, in the standard IEC 61131-3 languages; existing vendor logic can be converted (our SIMADYN study is the first case). The logic belongs to the plant. Each version is kept as a record in L3.
3	**How do we issue commands?**	L4, L2, L1, L0	Only the operator commands. The command travels on a separate in channel, one-way, stamped with identity and level; the controller checks the stamp before acting. Anything stamped L5 is rejected. No command reaches equipment that carries a lock. L0 overrides all.
4	**How do we store data?**	L3	Each tag stores its own history in its own node, in at least two copies, spread across units, station and headquarters. No central historian: losing one node loses one tag, not the plant's memory.
5	**How is data retrieved for trends?**	L3, L4, L5	The HMI asks each node by any of its names through DNS; the node returns its history. 10 tags = 10 parallel queries to 10 independent nodes, from the HMI, a laptop or the AI.
6	**Where do we run the logics?**	L1	On controllers only: existing proven controllers where they still work, or a standard IEC 61131-3 runtime (CODESYS first) on PLCs or industrial PCs. Never in data nodes or AI. Protection keeps its own hardware.
7	**How do we get the sequence of events?**	L0, L1, L3	Each event is timestamped where it happens: protection relay, controller I/O. Event nodes keep their records; the sequence is built by querying and sorting by source time. Accuracy comes from time sync at the source and cannot be added later.
8	**Third-party I/O and logic on industrial PCs?**	L1	Yes. An L1 choice that changes nothing at other levels. Logic in a standard language runs on any compliant runtime with third-party I/O over open fieldbuses. Safety functions stay on certified hardware.

Why it fits obsolescence: each level stands on its own, so an obsolete part is replaced without touching the rest. Proven equipment that still works stays in place.

NB: We Have to cleverly integrate the Authorisation of the users (it has to address the level of of authority), Asset management (might be part of L3 as everything is having name and network address)