DRAFT, NOT POSTED.

The Laws of Authority

A Beyond Purdue statement on machines, people and AI | Draft V0.4 | 3 November 2026 | Petr Roupec, BM Global

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

Asimov gave his robots three laws in 1942. Our plants need the same for machines, people and AI. The simpler and more predictable a level, the more authority it holds: authority is earned by predictability, not by intelligence. People work inside the plant. Their safety is designed in from the start, not added later.

Level	Authority	Allowed to vote on	Never allowed to	Standards
L0 Protection and isolation	**Absolute**	Trip. Veto over every level. Hold the lock.	Be overridden, or depend on any other level.	IEC 61508, IEC 61511, IEC 62061 / ISO 13849, IEC 60255, API 670, ISO 14118
L1 Controller	**Acts**	Actuators, within its logic and protection limits. Shouts every command it executes.	Act outside protection limits.	IEC 61131-3
L2 Channels	**Gatekeeper**	What crosses, and in which direction. Every level speaks only through L2. Out channels carry data and records out; in channels carry commands in.	Originate a command. Mix data and commands.	One-way transfer by construction
L3 Data nodes	**Holds and serves**	Nothing. It processes, stores and presents data on demand. Holds the asset records and every command given and executed.	Grant access. Act on the plant. Pass a command.	DNS / DNSSEC (RFC 4033), OPC UA, MQTT or other open standards
L4 Operator	**Decides**	Commands to controllers, each one shouted to L3 as given. Override and stop of any advice.	Disable protection.	EU AI Act Article 14
L5 AI	**Voice, no vote**	Nothing. It analyzes, interprets and supports the operator.	Touch an actuator.	System One models (e.g. Jev)

Isolation keeps people safe at work: the lock holds a machine still while someone is inside it. The emergency stop stops a machine; only the lock keeps it stopped. [17][18]

AI has a voice, not a vote.

LinkedIn article V1.0 | 3 November 2026 | Petr Roupec, BM Global | Heading: the one pager, V1.0

In 1942 Isaac Asimov gave his robots three laws [1]. Our plants have been full of robots for decades: turbines, pumps, breakers, valves. They do not walk, but they can kill. Now AI is arriving in the control room, and the real question is not whether machines can think. It is who is allowed to act.

I have put my answer on one page. This article walks through it.

Authority, not location

The Purdue model, published in 1992, gave plants their levels [19]. Over thirty years those levels became places on a network drawing [20]. Beyond Purdue keeps the numbers and changes the question. A level is a grant of authority, and every level states what it is allowed to vote on and what it is never allowed to do.

The ordering rule is inverse authority: the simpler and more predictable a level, the more authority it holds. A relay and a copper wire hold absolute authority. A model with billions of parameters holds the least. Authority is earned by predictability, not by intelligence.

Why does this matter now? Because AI is the most capable participant ever to enter a control room, and capability is exactly the wrong reason to hand out authority. A model can be brilliant and still be wrong in a

way nobody can predict. A relay is dull and always right about one thing. The plant should trust the relay with the trip and the model with the explanation.

The six levels

- L0 Protection and isolation: absolute. Trips and vetoes every level, holds the lock while people work, never overridden. IEC 61508, IEC 61511, API 670, ISO 14118 and related standards [3][4][9][17].
- L1 Controller: acts, within protection limits. Shouts every command it executes.
- L2 Channels: gatekeeper. Data and records out, commands in, never mixed, one-way by construction.
- L3 Data nodes: hold and serve. Present data on demand and record every command given and executed. Never command.
- L4 Operator: decides. Every command is shouted to L3 as it is given. Human oversight as in EU AI Act Article 14 [13].
- L5 AI: analyzes, interprets, supports. A voice, not a vote [14].

The laws in one line each

- Meta-law: no level acts outside these laws [2].
- Law Zero, Protection: no harm to people or the environment; nothing is allowed to weaken protection; a lock outranks every level.
- First, Independence: if every other level fails, protection still acts [5].
- Second, Obedience: the controller obeys the operator, unless that breaks Law Zero or the First Law.
- Third, Self-preservation: the machine protects itself, but people come first.
- Fourth, The gate: data out, commands in, never mixed; channels never originate an action.
- Fifth, The record: data nodes present data and record every command, permit, lock and bypass; they grant no access and take no action.
- Sixth, The human decides: the operator can always ignore, override or stop any advice.
- Seventh, See everything, touch nothing: AI reaches an actuator only through a human decision.
- Eighth, Authority flows down only: failure never grants authority.

As in Asimov, a lower-numbered law always overrides a higher one.

Data in independent nodes

The second idea follows from the laws. Data does not live in one big database. It lives in many small, independent nodes, one for each signal, asset or record, each with its own name, its own data and its own meaning. Everything that follows is a result of this. The technology is technology people already know: DNS, IPv6, multicast and OPC UA [11][23].

Names and aliases

Naming and asset management is always a big issue in a plant. So every node has a DNS-style name, such as hp-steam.u1.plant.example, because people already read names like these. DNS also has aliases: the KKS code, the vendor tag, the HMI name and the asset number all find the same node [23]. A name is updated automatically when a node is born, by a person, or by a shout.

Every node lives in at least two copies, on different hardware, power and rooms, to be really redundant. Both copies hear the same messages, so they hold the same data without ever syncing. Losing one copy loses nothing.

A ring, not a stack

The levels are not stacked. They stand around the data plane, the L3 Data nodes that hold the record of the plant, and L2 is the ring. Every level speaks to every other only through an L2 channel. Protection sends its records out through a one-way diode. The operator sends commands in through a separate one-way channel. The record plane is wide and flows out; the command plane is narrow and flows in. The data diode is the enabler: light travels one way, so data and commands cannot mix, and the levels hold because the diode holds. A passive diode has no power and nothing to configure, so it is as predictable as a relay, and it is named like any other asset [24].

Every command leaves two marks. L4 shouts GIVEN, L1 shouts EXECUTED, and the data node pairs them. A command given and never executed raises an alarm. The record becomes an account of authority: who asked for what, and what the plant actually did.

Authority also follows people and devices. Every user, device and application carries its level, and a credential grants only what that level is allowed to do. The controller checks the stamp on every command, not only the login screen. Names identify; they never authorize. Nobody receives protection authority through the system; protection settings are changed only at the protection equipment, under its own procedure.

Maintenance is operation

People work inside the plant, and maintenance is part of operation. Between 10 and 15 percent of fatal accidents at work in Europe are linked to maintenance [21]. Isolation is there for them: the lock holds a machine still while someone is inside it, and the data plane hears 11MBN12AP001 released for work. The emergency stop stops a machine; only the lock keeps it stopped [18].

Enforced by construction

Asimov wrote his laws to show how they fail. So these laws are not left to software: copper for protection, light and direction for channels, signatures for names. A law that lives only in software is a wish.

The First Law can be proven before commissioning: disconnect every level other than L0 at once and watch protection still trip. If it does not, the plant is not ready.

What this is not

It is not a certified safety architecture and not a product. The standards in the table are the basis for each level; how they apply to a given plant is a matter for that plant's own safety and security studies. Some questions are open on purpose, such as how a controller confirms a command's authorization before it obeys.

This is V1.0, a statement and not a standard. The full article and the one pager are on the Beyond Purdue site [15]. Which law would you challenge first?

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

#BeyondPurdue #OTSecurity #IndustrialAutomation #FunctionalSafety #AI

References

1. Asimov, Three Laws of Robotics and the Zeroth Law: https://en.wikipedia.org/wiki/Zeroth_Law_of_Robotics
2. Clarke, Asimov's laws of robotics: implications for information technology (meta-law): https://cse.buffalo.edu/~rapaport/Papers/Papers.by.Others/clarke-asimov-2.pdf
3. IEC 61508, Functional safety of E/E/PE safety-related systems: https://webstore.iec.ch/en/publication/5515
4. IEC 61511-1, Safety instrumented systems for the process industry sector: https://webstore.iec.ch/en/publication/24241
5. IS/IEC 61511-1, clause 11.2.4, separation and independence of BPCS and SIS: https://law.resource.org/pub/in/bis/S05/is.iec.61511.1.2003.pdf
6. IEC 62061, Safety of machinery, functional safety of safety-related control systems: https://webstore.iec.ch/en/iec_catalog/product/preview/?id=L3B1Yi9wZGYvcHJldmlldy9pbmZvX2llYzYyMDYxe2VkMj4yfWVuLnBkZg==
7. ISO 13849-1, Safety-related parts of control systems: https://www.iso.org/standard/69883.html
8. IEC 60255-1, Measuring relays and protection equipment: https://cdn.standards.iteh.ai/samples/100210/08c2059a2d7f406f8290ee090e93b0ee/IEC-60255-1-2022.pdf
9. API 670, Machinery Protection Systems: https://www.intertekinform.com/en-us/standards/api-std-670-2025-97086_saig_api_api_3641258/
10. Munich Re, Steam turbine overspeed protection (separation of overspeed detection from speed control): https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/Overspeed_Protection_White_Paper_BRO-FINAL.pdf/_jcr_content/renditions/original./Overspeed_Protection_White_Paper_BRO-FINAL.pdf
11. OPC Foundation, OPC UA specifications: https://reference.opcfoundation.org/
12. RFC 4033, DNS Security Introduction and Requirements: https://www.rfc-editor.org/rfc/inline-errata/rfc4033.html
13. EU AI Act, Article 14, Human oversight: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-14
14. TypeSafe AI, Introducing System One Models and Jev: https://typesafe.ai/blog/introducing-system-one-models-and-jev
15. Beyond Purdue newsletter: https://www.beyondpurdue.com/
16. OASIS, MQTT Version 5.0: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html
17. ISO 14118:2017, Safety of machinery, prevention of unexpected start-up: https://www.iso.org/standard/66460.html
18. ISO 13850:2015, Safety of machinery, emergency stop function: https://www.iso.org/standard/59970.html
19. ISA Global Cybersecurity Alliance, Why the Purdue hierarchy is still relevant: https://gca.isa.org/blog/excerpt-2-industrial-cybersecurity-case-studies-and-best-practices
20. SANS Institute, The Purdue Model, Introduction to ICS Security Part 2: https://www.sans.org/blog/introduction-to-ics-security-part-2
21. EU-OSHA, Maintenance and occupational safety and health: a statistical picture: https://osha.europa.eu/en/publications/maintenance-and-occupational-safety-and-health-statistical-picture
22. IEC 61511 ed.2, clause 16.2, bypass authorization and bypass log (ABB summary): https://library.e.abb.com/public/52dc61cd2284462c8f66bdcafb1fefcb/11%20C%20Bratt%20ABB%20changes%20in%20IEC61511.pdf
23. RFC 1034, Domain names, concepts and facilities (CNAME aliases): https://www.rfc-editor.org/rfc/rfc1034
24. NIST glossary, data diode: https://csrc.nist.gov/glossary/term/data_diode