DRAFT FOR REVIEW. NOT PUBLISHED.

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.

Beyond Purdue | 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, burned into their positronic brains [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 question is no longer whether machines can think. The question is who is allowed to act.

This article explains one page. The page is above. Everything else here is commentary on it.

From Purdue levels to levels of authority

The Purdue model was published in 1992 by a team led by Theodore Williams, and it has organised plant networks for thirty years [19]. Its levels run from the physical process at Level 0 up through control, supervision, site operations and the enterprise, and security practice has grown around the boundaries between them [20]. Williams himself listed one of the reasons for levels as limiting the scope of responsibility and authority [19]. Over time that idea faded and the levels became places on a network drawing.

Beyond Purdue takes the idea back. A level is not a network segment. A level is a grant of authority, and every level must state what it is allowed to vote on and what it is never allowed to do.

The rule that orders the levels 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.

Six levels, read row by row

L0 Protection and isolation holds absolute authority. It trips and vetoes every other level, it holds the lock while people work, and it is never allowed to be overridden or to depend on anything else. This is hardwired machinery protection, protection relays, safety instrumented functions and the isolation of equipment for maintenance, built to IEC 61508, IEC 61511, IEC 62061 or ISO 13849, IEC 60255, API 670 and ISO 14118 [3][4][6][7][8][9][17].

L1 Controller acts. It moves actuators within its logic and inside protection limits, and it shouts every command it executes so the record knows what really happened. It is never allowed to act outside protection limits.

L2 Channels are the gatekeeper. They decide what crosses and in which direction. Out channels carry data and records out; in channels carry commands in. A channel is never allowed to originate a command or to mix data with commands. The direction is set by construction, not by configuration.

L3 Data nodes hold and serve. Each tag is its own node, with its own address, history, description and meaning. Nodes process, store and present data on demand, they hold the asset records, and they hold the record of every command given and executed. They are never allowed to grant access, act on the plant or pass a command. Open standards carry the names and the data: DNS with DNSSEC, OPC UA, MQTT [11][12][16].

L4 Operator decides. The operator commands the controllers, and every command is shouted to L3 as it is given, through the operator's own one-way channel. The operator can override or stop any advice and is never allowed to disable protection. This is human oversight in the sense of Article 14 of the EU AI Act [13].

L5 AI has a voice and no vote. It analyzes, interprets and supports the operator, using models built for industrial reasoning such as TypeSafe's System One models [14]. It is never allowed to touch an actuator.

AI has a voice, not a vote.

The laws

The table says who holds which authority. The laws say how those authorities meet. As in Asimov, a lower-numbered law always overrides a higher one [1]. The meta-law comes from Roger Clarke's extension of Asimov [2].

> **Meta-law. The Law of Laws.** No level is allowed to act unless its action is subject to these laws. [2]
>
> **Law Zero. Protection.** The plant is not allowed to harm people or the environment, nor, through inaction, allow harm to come to them. Protection holds this law, and no level is allowed to weaken it. A lock outranks every level. [1][3][4][17]
>
> **First Law. Independence.** Protection stands alone. If every other level fails at the same moment, protection still acts. [5][9][10]

Second Law. Obedience. The controller obeys the operator, except where the command would break Law Zero or the First Law. [1][6][7]

Third Law. Self-preservation. The machine protects its own existence, as long as this does not break the laws above. People first, machines second. [1][8][9]

Fourth Law. The gate. Channels decide what is allowed to pass, and every level speaks to every other level only through a channel. Out channels carry data out, in channels carry commands in, and the two never mix. Channels never originate an action. [15]

Fifth Law. The record. Data nodes hold the truth of the plant. They process, store and present it on demand, under any of their names, and they record every command, permit, lock and bypass. They grant no access and take no action. [11][12][16][22]

Sixth Law. The human decides. The operator can always ignore, override, reverse or stop any advice, and must never be made dependent on it. [13]

Seventh Law. See everything, touch nothing. AI is allowed to observe every tag, analyze and interpret the plant, and support the operator. It has no path to an actuator except through a human decision. [14][15]

Eighth Law. Authority never flows upward. Information rises on the out channels. Authority descends on the in channels. No level gains authority through failure, through the data path, or by asking. [15]

Data lives 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.

The ring and the data diode

The table reads top to bottom, but the plant is not built that way. The levels are not stacked like Purdue. Each level stands on its own, arranged around the data plane, the L3 Data nodes that hold the record of the plant. L2 is the ring around them. Every level talks to every other level only through an L2 channel.

Protection sends its records through a one-way diode into the data plane, and from there they reach the operator and anyone else who needs them. The operator sends commands through an L2 in channel, with its own diode, down to the controller. Remote access, vendors and the enterprise also enter only through L2. Nothing has to pass through the level above it to be seen. 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].

This gives two planes. The record plane is wide and flows out only: everything is recorded. The command plane is narrow and flows in only: few paths, every command stamped with who issued it and from which level, never in the same channel as data.

Every command leaves two marks

A command is the most consequential thing a plant does, so it is recorded twice. When the operator gives a command, L4 shouts it as GIVEN to L3 through its own diode. When the controller carries it out, L1 shouts EXECUTED. The data node pairs the two. A command that was given but never executed raises an alarm, and so does an execution nobody gave.

This changes what the record is for. It is not only a history of values. It is an account of authority: who asked for what, and what the plant actually did. Data are just data. Everyone is allowed to read them; very few are allowed to command.

Maintenance is operation

People work inside the plant. Between 10 and 15 percent of fatal accidents at work in Europe are linked to maintenance [21]. So maintenance is not a pause in operation; it is part of it, and their safety is designed in from the start, not added later. Isolation is there because of maintenance: the lock holds a machine still while someone is inside it, and a lock outranks every level. When equipment is released for work, the data plane hears it as a shout, for example 11MBN12AP001 released for work, and L3 records the permit, the lock and any bypass. The emergency stop stops a machine; only the lock keeps it stopped [18]. The lock outranks the screen.

Enforced by construction

Asimov wrote his laws to show how they fail; nearly every story is a loophole [1]. So these laws must not live only in software. Protection is enforced by copper. Channels are enforced by light and direction. Names are enforced by signatures. Credentials carry a level of authority, and the controller checks the stamp on every command, not only the login screen. Names identify; they never authorize.

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

A law that lives only in software is a wish.

What this is, and what it is not

This is V1.0 of a statement, not a standard and not a certified safety architecture. The standards named in the table are the basis for each level; whether and how they apply to a given plant is a question for that plant's own safety and security studies. Several points are open by design, among them how a controller confirms a command's authorization before it obeys. They will be developed in later issues.

Your turn

The laws are published one by one in the Beyond Purdue newsletter so practitioners can challenge them [15]. Which law would you break first, and how would you stop it from being broken?

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

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=L3B1Yi9wZGYvcHJldmlldy9pbmZvX2llYzYyMDYxe2VkMi4yfWVuLnBkZg==

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