The Laws of Authority

A Beyond Purdue statement on machines, people and AI | V1.0 | 3 November 2026 | Petr Roupec, BM Global

In 1942 Isaac Asimov gave his robots three laws, burned into their positronic brains. Our plants have been full of robots for decades: turbines, pumps, breakers, valves. They do not walk, but they can kill, and people work inside them every day. 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.

From Purdue levels to levels of authority

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

A level is not a network segment. A level is a grant of authority, and every level must state who is allowed to vote on what.

The principle of 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.

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 communicates only through L2. Out channels carry data and records out; in channels carry commands in.	Originate a command. Mix data and commands.	Data diodes, passive by preference. IEC 62443-3-3
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)

AI has a voice, not a vote.

The laws

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

Meta-law. The Law of Laws. No level is allowed to act unless its action is subject to these laws. Basis: Clarke's meta-law extension of Asimov [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. Basis: Asimov's Zeroth Law [1]; IEC 61508 and IEC 61511 safe state [3][4]; ISO 14118 and IEC 60204-1 clause 5.3: when an isolator is locked, remote as well as local closing is prevented [17][18].

First Law. Independence. Protection stands alone. If every level above fails at the same moment, protection still acts. Basis: IEC 61511-1 clause 11.2.4 [5]; API 670 separation of overspeed detection from speed control [9][10].

Second Law. Obedience. The controller obeys the operator, except where the command would break Law Zero or the First Law. Basis: Asimov's Second Law [1]; IEC 62061 / ISO 13849 safety-related control [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. Basis: Asimov's Third Law [1]; API 670 machinery protection, IEC 60255 protection relays [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. Basis: Beyond Purdue [15]; restricted data flow between zones and conduits, IEC 62443-3-3 [26]; unidirectional gateways and data diodes, NIST SP 800-82r3 [25][24].

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. Basis: DNSSEC [12]; open standards such as OPC UA [11] or MQTT [16]; IEC 61511 clause 16.2 bypass log [21].

Sixth Law. The human decides. The operator can always ignore, override, reverse or stop any advice, and must never be made dependent on it. Basis: EU AI Act Article 14(4) [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. Basis: Beyond Purdue [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. Basis: Beyond Purdue [15].

Data lives in independent nodes

Independent nodes. The second idea follows the laws. Data does not live in one big database. It lives in many small, independent nodes, the L3 Data nodes of the data plane: one tag, one node, with its own name, IPv6 address, history, description and meaning. Everything that follows is a result of this. The levels are not stacked like Purdue; each stands on its own around the data plane. The technology is technology people already know: DNS, IPv6, multicast and OPC UA.

Names and aliases. Naming and asset management is always the big issue. Every node has a DNS-style name, because people already read names like these. A name is updated automatically when a node is born, by a person, or by a shout. DNS aliases let one node be found by all its names: KKS code, vendor tag, HMI name, asset number and OPC UA name [12][23].

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

L2 is the ring. Every level communicates with the others only through L2 channels. Protection sends its records through a data diode into the data plane, and from there they are available to the operator and other systems. 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. The data diode is the enabler: light travels one way, so data and commands cannot mix. A passive diode has no power, no firmware and nothing to configure, so it is as predictable as a relay or a padlock, and it is named like any other asset [24][25].

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

Who is allowed to act, not who is allowed to see. Data are just data. Everyone is allowed to read them; very few are allowed to command. Everything stays on site. An external database is one more reader on an out channel.

Built for obsolescence. Because each level stands on its own, an obsolete part is replaced without touching the rest, and proven equipment that still works stays in place.

Built for the people inside it. Maintenance is part of operation, and people work inside the plant. Their safety is designed in from the start, not added later. Each piece of equipment is in one of four states: in service, released for work, under test, or returning to service. 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. The lock outranks the screen. [17][19][20][22]

Statements of authority

- **Users carry their level.** Every user, device and application holds a level of authority, and a credential grants only what that level is allowed to do. Authority is checked where the action happens: the controller checks the stamp on every command, not only the login screen.
- **Roles follow the levels.** Viewer: reads data nodes. Engineer: changes L1 logic offline, every version recorded. Operator: issues L4 commands. Permit issuer: releases equipment for work and returns it to service, an L4 role; the lock stays with the person at work. AI service: reads only, L5. Nobody receives protection authority through the system; protection settings are changed only at the protection equipment, under its own procedure.
- **Assets are nodes.** Every asset, from a transmitter to a controller or a server, has a name and a network address, so asset management lives in L3. Each asset node holds its own type, firmware, location,

maintenance and obsolescence status. The register is not a separate database: asking the names lists what exists.

- **Names identify, they never authorize.** A DNS name or an address tells who and where. Only the level of authority tells what is allowed to be done.

Enforced by construction, not by programming

Asimov wrote his laws to show how they fail; nearly every story is a loophole. So these laws must not live only in software. Protection is enforced by copper, channels by light and direction through data diodes, names by signatures, credentials by a level of authority on every one. A law that lives only in software is a wish.

Ideas to develop

- **Authority in the name.** Each Meaning Tag carries its authority level and owner in its DNS records, signed with DNSSEC, so any device can check who is allowed to write it before it obeys.
- **Remote access through the ring.** Vendor and remote access treated as one more L2 in channel: time-limited, stamped with the level of the person, recorded in the L3 Data nodes.
- **Authority ledger.** Every vote, veto and override is written into the Plant Diary as a plain sentence an engineer can read.
- **Pull-the-plug test.** Before commissioning, prove the First Law: disconnect every level above L0 at once and watch protection still trip.
- **Beyond Purdue for the AI world.** One law per newsletter issue, opened to practitioners for challenge and extension.

Changes from V0.4

Reordered to follow the explanation: the laws first, then data in independent nodes, then names and aliases, then everything else. New paragraphs: names and aliases; at least two copies. The data diode named as the enabler, with its basis under the Fourth Law. References 23 to 26 added. No law changed.

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 (API 670 separation of overspeed 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. IEC 60204-1, Electrical equipment of machines, clauses 5.3 to 5.6 (supply disconnecting and isolation): https://eclass.uniwa.gr/modules/document/file.php/IDPE391/%CE%A0%CE%A1%CE%9F%CE%A4%CE%A5%CE%A0%CE%91/EN%2060204-1-2018.pdf
19. EN 50110-1:2023, Operation of electrical installations, the five safety rules: https://standards.iteh.ai/catalog/standards/clc/1b0a0556-70ff-4d0f-a322-ca2d7d05af90/en-50110-1-2023
20. ISO 13850:2015, Safety of machinery, emergency stop function: https://www.iso.org/standard/59970.html
21. IEC 61511 ed.2, clause 16.2, bypass authorization, indication and bypass log (ABB summary): https://library.e.abb.com/public/52dc61cd2284462c8f66bdcafb1fefcb/11%20C%20Bratt%20ABB%20changes%20in%20IEC61511.pdf
22. IEC 62682 / ISA-18.2, alarm management, out of service and maintenance stage (ISA): https://www.isa.org/getmedia/55b4210e-6cb2-4de4-89f8-2b5b6b46d954/PAS-Understanding-ISA-18-2.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
25. NIST SP 800-82r3, Guide to Operational Technology Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final
26. IEC 62443-3-3, System security requirements and security levels: https://webstore.iec.ch/en/publication/7033