SUGGESTIONS FOR REVIEW. NOTHING IN THE EXISTING DOCUMENTS HAS BEEN CHANGED.

Maintenance is Operation

Beyond Purdue suggestions on isolation, lockout and permit to work in the levels of authority

Suggestions V0.1 | 2 November 2026 | Petr Roupec, BM Global | Site names anonymised as plant.example

Maintenance is a plant state, not an exception. The lock outranks the screen.

Why it belongs in the core

Around 10 to 15 percent of fatal accidents at work in Europe are related to maintenance [1], and accidental start is one of the most common causes of serious maintenance accidents [2]. On Piper Alpha the pump was restarted because the permit for its missing relief valve was filed elsewhere and the night shift could not see it [3]. The standards agree on the physical sequence: isolate, lock, dissipate stored energy, verify [4][5][6]. What fails in practice is mostly information: who is inside, what is open, which permit touches which equipment.

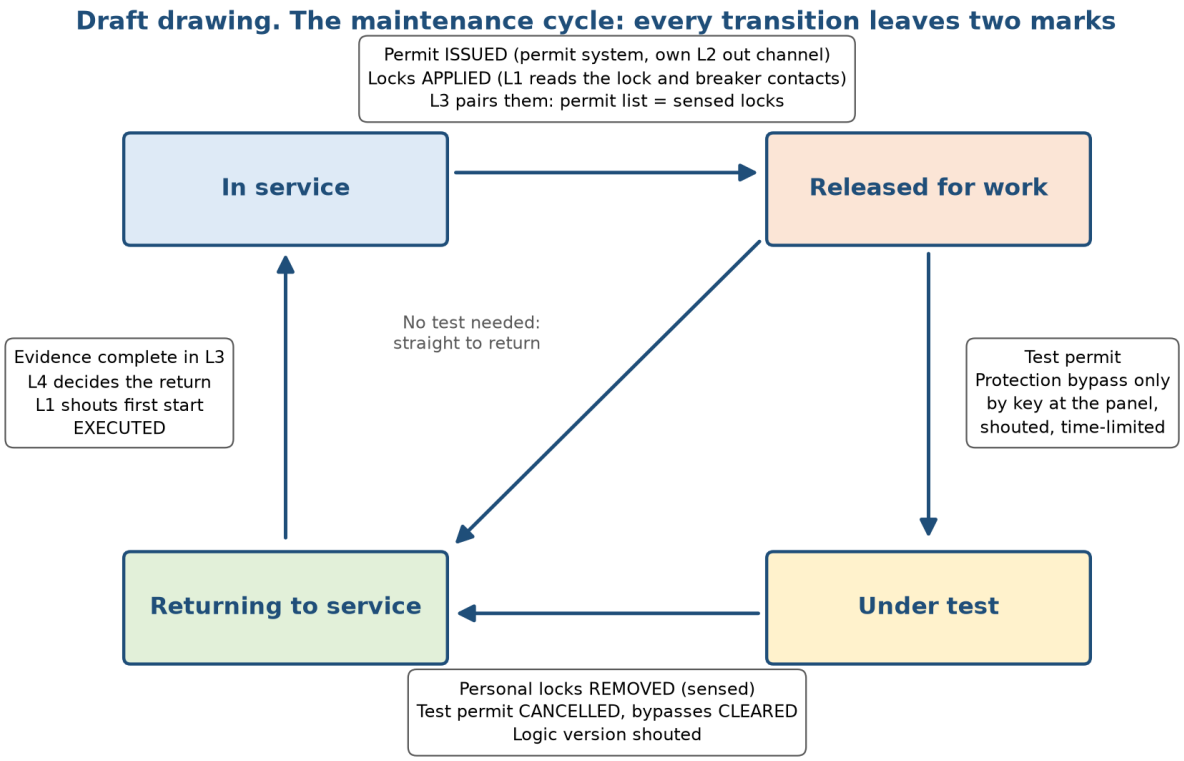
A plant spends its life in mixed states. One unit runs while another is in outage. A pump is released for work while its twin carries the load. Old plants have parts that have never been instrumented for isolation at all. The authority model has to describe all of this, all the time, not only the clean running plant.

The elegant core: three voices must agree

The data plane already records every command twice: GIVEN by L4, EXECUTED by L1. Maintenance uses the same pattern. A permit is a human instruction to the plant to stay still, so it leaves two marks as well.

- The permit (a person declares): issued, suspended, cancelled, with its isolation list. Shouted by the permit system through its own L2 out channel.
- The lock (hardware confirms): breaker racked out and earthed, valve locked closed, personal locks present in the lock box. Read by L1 from contacts and shouted as data.
- The record (L3 reconciles): pairs the permit list with the sensed locks, per equipment. A mismatch is an alarm, never a correction.

Humans declare. Hardware confirms. L3 reconciles. Nobody else is allowed to change the state of a machine with people inside it.



Humans declare. Hardware confirms. L3 reconciles. A mismatch is an alarm, never a correction.

Twelve suggestions

1. State is a meaning tag of every equipment node. Each equipment node carries one of your four decided states (In service, Released for work, Under test, Returning to service) and shouts it with its values. A value without its state is not trusted for operation. Why: the HMI, the historian and the AI all read the same state from the same place.

2. The lock is sensed, not typed. Isolation points report their own position: breaker position and earthing contacts, valve lock switches, lock-box counters. Where an old plant has no contacts, the state may be entered by hand but is marked "declared, not sensed". Why: honest about brownfield plants; the screen never pretends to know more than the hardware.

3. One key, two locks. Use trapped-key interlocking [7]: the key that locks the isolator can only be released from the remote-enable switch of that drive. Taking it opens the L2 in channel for that equipment physically. The switch position is shouted. Why: the command path closes by construction, so "no restart under a lock" does not depend on software.

4. Permits are nodes, linked to equipment. Every permit is its own node in the data plane, linked to every equipment node it touches, including connected items such as a pump and its relief valve. Any equipment view shows every live and suspended permit on it. Why: this is the Piper Alpha lesson; permits are found by equipment, not by trade or location [3].

5. The plant knows who is inside. Personal locks are counted per isolation, including contractors. The equipment node shows how many people hold a lock on it and since when. Why: contractors carry the highest maintenance accident rates [2], and they are the people least known to the control room.

6. Commands meet the lock, and the attempt is recorded. A command GIVEN to equipment under a lock raises an alarm in L3 at once. Whether L1 also refuses it belongs to the command authorization topic you deferred. Either way the refusal is a second barrier, never the isolation.

7. Protection is never bypassed from the system. A protection bypass for test is made only by key at the protection panel, under a test permit. It is shouted, logged, time-limited, and its expiry raises an alarm. IEC 61511 already requires every bypass to have authorization, indication and a log entry [8][9]. Why: keeps L0 independent while giving the operator full visibility.

8. Logic maintenance follows the same rule. Changing controller logic needs a permit, Management of Change and a physical key switch at the controller. The controller shouts its logic version before and after; L3 shows any change without a matching permit.

9. The record is the shift handover. On demand, the control room sees by area: live and suspended permits, sensed locks, bypasses, and isolations that must be re-proved because they have stood longer than a shift [6]. Why: handover failures are a classic cause of maintenance accidents [3].

10. Returning to service is evidence, then a human decision. L3 assembles the evidence: permits cancelled, every personal lock sensed clear, bypasses cleared, logic version matching. It shows "ready" or exactly what is missing. L4 decides. L1 shouts the first start as EXECUTED.

11. AI checks, never signs. L5 can flag overlapping permits, isolation lists that do not match the drawings, re-proving that is due, or bypasses near expiry. It is never allowed to issue, sign, suspend or cancel a permit, or to clear a lock.

12. Unit modes are derived, not set. The state of a unit (for example operating, operating with parts released, outage, commissioning) is derived in L3 from its equipment states. Nobody switches a unit into "outage" on a screen; the outage is the sum of real isolations. Why: covers plants that are partly in maintenance, partly running, for years at a time.

Authority in each state

Suggested content for the per-level table in your checklist. "In service" follows the existing laws and is not repeated.

Level	Released for work	Under test	Returning to service
L0 Protection	Stays active. Allowed to trip. Never bypassed to make work easier.	Bypass allowed only by key at the panel, under a test permit, shouted and time-limited. Never bypassed remotely.	Allowed to confirm all bypasses cleared. Never returned with a bypass active.
L1 Controller	Holds the safe state and shouts lock and isolator contacts. Never allowed to start or energise.	Allowed to run only the test scope of the test permit; every test command shouted EXECUTED.	Shouts locks clear and logic version. Allowed to start on the L4 decision only.
L2 Channels	In channel for the equipment closed by the trapped key. Never carries a command to it.	In channel opened only for the test scope, by key.	In channel reopened when the key returns to the remote-enable switch.
L3 Data nodes	Holds permit, isolation and lock records; reconciles; alarms. Never releases or cancels.	Records the test and the bypass timer; alarms on expiry.	Assembles the evidence; shows "ready" or what is missing.
L4 Operator	Sees and plans around. Never allowed to command released equipment or remove a lock.	Commands only within the test permit.	Decides the return. Never allowed to return while a lock is sensed.
L5 AI	Checks conflicts and re-proving. Never allowed to sign or cancel.	Watches test limits and bypass time.	Summarises the evidence. Never allowed to decide.

What this means for the laws

Suggestion: no new law. Two small changes carry everything, because a lower-numbered law already overrides every higher one.

- Law Zero, second clause (the lock): "A lock outranks every level. No level is allowed to energise, start or move equipment that carries a lock. Only the person who applied it, or the site's formal removal procedure, is allowed to remove it."
- Fifth Law, the record, gains one phrase: "...and they record every command given and executed, and every permit, lock and bypass."

Because the Second Law already makes the controller obey the operator only where Law Zero is not broken, the lock automatically limits obedience. The Sixth Law stays as it is: the human decides, and the lock is a human decision held in the hand.

A tag that lives only on the screen is a wish. The lock outranks the screen.

What stays outside the system

- Issuing and cancelling permits remains the site's permit-to-work process and its competent persons. The system shows and reconciles; it never issues.
- Proving dead and verifying isolation stays a physical act by the person doing the work [4][5]. The system records that it was done.
- Isolation standards (single or double block and bleed, spading, positive isolation) are chosen by the site's risk assessment [6].

Decisions for you

- Is "three voices must agree" (permit, lock, record) the core idea, or would you frame it differently?
- Sensed isolation as the default, with "declared, not sensed" allowed for old plants?
- Trapped key on the remote-enable switch as the reference design?
- Unit modes derived from equipment states: keep, rename or drop?
- Law Zero second clause and the Fifth Law phrase as above, or another placement?
- Wording: this paper uses "allowed", as in the article. Your checklist uses "authorised". Which applies everywhere?

References

1. EU-OSHA, Maintenance and OSH: a statistical picture: https://osha.europa.eu/en/publications/maintenance-and-occupational-safety-and-health-statistical-picture
2. EU-OSHA, Overall safety management of maintenance work (accidental start; contractors): https://osha.europa.eu/sites/default/files/Overall-safety-management-of-maintenance-work.pdf
3. The Chemical Engineer, Piper Alpha: the disaster in detail: https://www.thechemicalengineer.com/features/piper-alpha-the-disaster-in-detail/
4. OSHA 29 CFR 1910.147, Control of hazardous energy (lockout/tagout): https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.147
5. ISO 14118:2017, Prevention of unexpected start-up (preview): https://cdn.standards.iteh.ai/samples/66460/62a3ecd66eab46b6ae004bf557c660dc/ISO-14118-2017.pdf
6. HSE HSG253, The safe isolation of plant and equipment: https://www.hse.gov.uk/pubns/priced/hsg253.pdf
7. ISO 14119:2024, Interlocking devices, including trapped key systems (Annex K): https://www.iso.org/standard/75942.html
8. ABB, Changes in IEC 61511 edition 2 (bypass log, authorization and indication, 16.2.7): https://library.e.abb.com/public/52dc61cd2284462c8f66bdcafb1fefcb/11%20C%20Bratt%20ABB%20changes%20in%20IEC61511.pdf
9. IEC 61511-1, Safety instrumented systems for the process industry sector: https://webstore.iec.ch/en/publication/24241
10. OSHA, Control of hazardous energy, overview and training: https://www.osha.gov/control-hazardous-energy