Beyond Purdue: Data Diodes as the Enabler

Suggestions V0.1 | 3 November 2026 | Petr Roupec, BM Global

The data diode is the enabler. Light travels one way, so data and commands cannot mix. The levels hold because the diode holds.

This paper records the suggestion for adding data diodes to the works. It is principles only: it describes what a diode does and how it is named, not how it is built.

Why the diode belongs in the model

The laws give each level what it is allowed to do. Those laws hold only if the paths between levels are one way where the model says one way. A data diode makes that a physical fact rather than a setting. Data and records go out; commands come in on their own lane. Nothing can travel back on either.

The NIST glossary defines a data diode as a device that enforces one-way flow. IEC 62443-3-3 asks for restricted data flow between zones and conduits, and NIST SP 800-82r3 describes unidirectional gateways for OT networks.

Predictability earns authority

A passive diode has no power, no firmware and nothing to configure. It is as predictable as a relay or a padlock. That is why the L2 gate can be trusted with the direction of every message: the gate cannot be talked into anything, because it does not listen.

Every diode is a named asset

Each diode is an L3 node like any other asset, with a DNS-style name and aliases, for example:

- dd01.u1.plant.example: the node
- dd01.l2.u1.plant.example: alias by level
- asset-4711.cmms.plant.example CNAME dd01.u1.plant.example: alias by asset number
- cab-12.room-e1.u1.plant.example: alias by cabinet location

The node records:

- **Type:** passive or active. Passive by preference.
- **Direction and channel:** out carries data and records; in carries commands.
- **What it carries:** the groups and the levels it joins.
- **State:** one of the four plant states. Replacing a diode is maintenance, released for work like any other equipment.
- **Proof of emission:** the sending side records what it sent. Principles only.

Only the sending side writes to the record. An out diode and an in diode are never linked in one record.

Where it goes in the works

Document	Change
One Pager	L2 Standards cell: data diodes, passive by preference.
Drawings	Diodes labelled with their names on A to D; new Drawing M, The enablers.
Statement	Fourth Law basis: IEC 62443 and NIST SP 800-82.
Data Plane Concept	Section: The diode as a named node.
Implementation Plan	Diode inventory with names, and a one-way test at commissioning.
Video	Scene: the data diode, the enabler, with the diode name shown.
Overview and web page	The diode named as the enabler in the explanation order.
Eight Questions and UCS	One phrase each.

Defaults chosen

Tag format: DNS name plus aliases, the same as every other node. No KKS codes are invented for diodes. Wording: data diode, passive by preference.

Sources:

NIST glossary, data diode: https://csrc.nist.gov/glossary/term/data_diode
NIST SP 800-82r3, Guide to OT Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final
IEC 62443-3-3, system security requirements: https://webstore.iec.ch/en/publication/7033
RFC 1034, domain names and CNAME aliases: https://www.rfc-editor.org/rfc/rfc1034