Episode Book

EPISODE #6580

How One-Way Data Diodes Protect Power, Water, and Rail

PUBLISHED	14 November 2026 at 02:23 UTC
DURATION	20:48
LISTEN	myweirdprompts.com/episode/one-way-data-diodes-52968/
HOSTS	Corn, Herman, Larry, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
SOURCES	25 cited by the research (listed at the end)
BOOK GENERATED	14 November 2026 at 06:47 UTC

SYNOPSIS

A data diode enforces one-way network traffic with physics: a fibre link with a laser on one end and no laser on the other. Originally a classified defence tool, these unidirectional gateways are now mandated in nuclear plants, used by municipal water utilities and rail operators, and required by France's ANSSI where firewalls are forbidden. This episode unpacks how protocol breaks keep TCP working, who builds the hardware—including Waterfall, Owl Cyber Defense, and OPSWAT—and where the security guarantee falls short.

TRANSCRIPT



Corn

What if the safest network device on earth is the one you couldn't break even if you tried? Not hardened, not patched — incapable. That's the corner of the security world Daniel wants us in today. He's asking about the data diode, or unidirectional gateway: hardware that lets data flow one way only, usually enforced with a fibre link where one end has a laser and the other end has no laser at all. Who actually uses these things, does anyone outside the military and intelligence world use one instead of a firewall, power plants, water utilities, rail, even ordinary businesses, and who builds them.



Herman

And it's a good time to ask, honestly, because the answer has been changing. Ten years ago this was a classified-world curiosity. Now it's mandated kit in nuclear plants and showing up at municipal wastewater pump stations, which is quite the journey for a box whose main feature is doing less than a firewall.



Corn

It refuses. That's the product.



Herman

It refuses, and it sells. Before we get to who's buying, though, we should be precise about what the box actually does, because the name is the mechanism. A data diode is named after the electronic diode — the component that lets current flow one way and blocks it the other. The network version does the same thing physically. You take a bidirectional fibre link and you strip it: the transmitter module has the laser, the receiver module has the optical receiver and no laser. There is literally nothing on the far side that could emit light back down that fibre.



Corn

So the guarantee is made of absence.



Herman

Absence, exactly. Waterfall, one of the big vendors, describes their own hardware in exactly those terms — transmit module with a laser, receive module with an optical receiver, no laser — and says the gateway is physically incapable of propagating any virus, denial-of-service attack, human error or cyber attack at all back into the protected network. Which sounds like marketing until you look at the hardware and realize the marketing is a parts list.



Corn

My kind of advertising. "Contains nothing."



Herman

But here's the complication that turns this from a clever cable into a real product, and it's the single most important technical point in this whole episode. A bare diode breaks the internet. TCP, the protocol almost everything runs on, is connection-oriented — the receiver has to send acknowledgements back. If nothing can come back, no connection ever completes. So a real diode product is hardware plus software: proxy servers on each side that terminate the connection, throw away all the session state, and re-originate the data fresh on the far side. It's called a protocol break.



Corn

So the box that can't be reconfigured is surrounded by software that absolutely can.



Herman

That's the honest tension in the whole category, yes. The unidirectionality is physics; everything usable about it is engineering. And there's a second distinction Daniel's question brushes against without naming. There are two models here. The classical, defence-and-intelligence model protects confidentiality — secrets can't leak out of the classified network. The alternative, industrial model protects availability and integrity — a control system publishes its data outward while being immune to anything coming in. The dam example people use: the public downstream needs current outflow data, and the floodgate controllers need it too, but the floodgate controllers do not need to hear from the public internet.



Corn

One-way for different reasons. The spy wants nothing to leave; the plant wants nothing to arrive.



Herman

That's the cleanest framing of it. And almost every civilian deployment — nuclear, water, rail — is the second kind. Keep that in mind, because it explains most of what follows, including where the guarantee is narrower than people assume.



Corn

Then let's get to who's buying. Nuclear first, I assume, since you're already leaning toward it like a man at a buffet.



Herman

I am, because nuclear is the beachhead. Waterfall's co-founder, Lior Frenkel, told Forbes that by the end of twenty-ten the company had sold to half the nuclear power plants in the United States. Half. And the go-to-market story is almost comically direct — they had a basic product by two thousand seven, some customers in Israel, and instead of doing what the textbooks said and going to Europe, they built a direct sales force pointed at North American nuclear generation.



Corn

Skip the channel, knock on reactor doors.



Herman

It worked. And there's a concrete deployment worth naming: August twenty-eleven, Iberdrola installed Waterfall gateways at the Cofrentes nuclear plant in Valencia, Spain — about a thousand megawatts — to create a real-time replica of their PI historian on the corporate side while blocking any data flow back toward the control networks. That's the model in miniature. The engineers get their data. The control room gets its quiet.



Corn

And the regulator's role in this? Because I suspect the buying wasn't purely driven by engineers lying awake at night.



Herman

No, and that's the uncomfortable question. The Nuclear Regulatory Commission now mandates data diodes — mandates, not suggests. On the electric side, NERC issued a compliance notice in December twenty-eleven recognizing hardware-enforced unidirectional paths as strong non-routable security under the CIP standards. And then the vendors took that ball and ran. OPSWAT markets its diode as, and this is their actual phrase, "Your Fast Pass to Compliance" — arguing the device helps meet CIP-005-8 and can exempt utilities from several CIP requirements entirely. Waterfall made the same case to FERC in written remarks: unidirectionally protected systems don't count as bi-directional external connectivity, so the compliance burden shrinks.



Corn

"Buy our box, skip your audit."



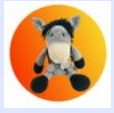
Herman

That's roughly the pitch, yes. Which doesn't make the box bad — it makes the buyer complicated. Some diodes are installed because an engineer was frightened, and some are installed because an auditor asked a question that this device makes disappear. You'll never get a clean count of which is which.



Corn

I'd guess the ratio follows the paperwork.



Herman

France is where this stops being encouragement and becomes law. ANSSI, the French national cyber agency, published a classification method for industrial control systems, revised last December to version two, four classes now, with Class 3 as high impact and Class 4 as catastrophic. The rule is startling: the most sensitive industrial networks are forbidden from using firewalls to connect to less critical networks. Not "firewalls plus something." Forbidden. Only hardware-enforced unidirectional gateways are permitted between network classes.



Corn

They banned the firewall.



Herman

Banned it for the top classes. Railway switching networks, chemical plant safety systems — the societally sensitive stuff. Andrew Ginter, who's been in this space forever, wrote that the French standards are the strongest in the world on exactly this point. ANSSI even published a formal protection profile for an industrial diode, defining the target of evaluation as equipment that permits communication in one direction only, with no return channel whatsoever. They wrote a specification for absence.



Corn

Certification of a vacuum. The French would.



Herman

So to Daniel's actual question — does anyone outside military and intelligence use one in place of a firewall — the answer is yes, but with two caveats. The users are power plants, water utilities, rail, oil and gas. And the placement is always the boundary between operational technology and the corporate network. Never general internet connectivity. No ordinary business swaps its firewall for a diode so the office can browse. The cost alone forbids it, which we'll get to.



Corn

And the selling point, really, is that it cannot be reconfigured. Nothing to misconfigure, nothing to get wrong.

L

Larry

Somewhere between silence and certainty, there is a diode. The Diora One Way. It lets the good things leave and nothing, nothing at all, come back. Your data, your light, your signal, flowing out into the evening like breath into cold air. The Diora One Way. It cannot be reconfigured. Neither can you.

L

Larry

Ask for the Diora One Way at the counter of any participating pharmacy. One way. That is the only way it goes.



Corn

"Flowing out into the evening like breath into cold air."



Herman

Please don't read it back in the slow voice. I'm asking you as your brother.



Corn

Fine. Supply side, then. Who builds these?



Herman

A small and oddly shaped market. One recent analysis puts Owl Cyber Defense, Waterfall, BAE Systems, Advenica and Fox-IT at roughly half of global revenues between them — about fifty-two percent in twenty twenty-five. Beyond that it's a long tail of specialists across a surprising number of countries: Naonworks in South Korea, Infodas and Siemens in Germany, Link22 in Sweden, VADO in Israel, Oakdoor in the UK, Stratign in the UAE, ST Engineering in Singapore, Chipspirit in India.



Corn

Every country with a defence ministry and a machine shop.



Herman

That's close to the pattern. The archetypes matter more than the list. Owl, out of Columbia, Maryland, is the defence-and-intelligence incumbent — decades of classified deployments. Waterfall, from Rosh Ha'ayin in Israel, is the OT specialist, the nuclear-and-rail people, with actual patents on the gateway architecture. Advenica in Sweden sells Common Criteria certified kit into European defence programmes. BAE wraps a diode into a broader cross-domain portfolio. And OPSWAT, after acquiring a



Herman (continued)

small company called Fend, sells the MetaDefender Optical Diode, which leads us to what I find the most interesting recent thread: water.



Corn

Go on. Water utilities.



Herman

A New England municipal public works department — serving about forty-two thousand residents — replaced an omnidirectional radio tower with optical diodes at their wastewater pump stations. The diodes pull Modbus data off the local controllers and push it over cellular to a cloud dashboard. Part of the driver was regulatory: under America's Water Infrastructure Act these utilities need risk and resilience assessments, which means they suddenly need real-time visibility into systems they'd previously isolated.



Corn

So the isolation that made them safe also made them blind, and the diode is how they get one without the other.



Herman

There's a better one. A large water utility serving close to two million customers had deliberately air-gapped its IT from its operational network — proper air gap, nothing crossing. Every day, someone physically carried disks of performance data from the treatment plants to the office network.



Corn

Sneakernet. For a system serving two million people.



Herman

Daily hand-carried disks, for years. They replaced that with diode transfers every few minutes. And it's not just water — Owl and Trihedral announced an integration this June pairing data diodes with SCADA software for water operators, with deployments in Houston and Nashville. Then rail: Waterfall published a case study of a North American metro and regional operator replicating logs, alert traffic and signal status XML outward, plus a remote screen view so the corporate security operations centre could literally watch the signalling console — all one-way. The stated requirement is blunt: the signalling network contains safety-rated systems and should be physically protected from all outside networks. When you put it that way, in a signalling room, a firewall does sound like a polite request.



Corn

Now the part where you disappoint me. What's the catch?



Herman

Several, and they're worth stating properly. The big one comes from an MIT paper by Hamed Okhravi, and it's bluntly written. It is sometimes claimed that data diodes protect the high network against cyber attacks. This, he says, is not correct. Many exploits need no session and no bidirectional communication — a fast-propagating worm or malware can infect a machine with one packet of data. The diode protects the sending side, not the receiving side.



Corn

One packet. And a one-way pipe is happy to deliver one packet.



Herman

Happy to. If a control system is publishing outward — the industrial model — that's fine, because the thing you care about is the sender. But people hear "no attack can cross" and assume both ends are safe, and the guarantee has never said that.



Corn

Cost?



Herman

Owl estimates thirty to a hundred and fifty thousand euros per diode. Fox-IT puts a minimum certified configuration around fifteen thousand. A SANS paper on industrial gateways says a hundred thousand dollars plus, and calls that not financially viable except for the most critical processes. Plus there's no receipt, no error control — you cannot confirm a packet arrived, because confirming is a return channel. Even the latency claims contradict each other; one source says no latency, another says some transfers run slow and unreliable. Nobody's lying. It depends entirely on the proxy software, which is the part that isn't physics.



Corn

Which is my favourite fact about this market: even the market doesn't know itself. One forecast says it grows at six and a half percent, another at twelve. North America is either a third of it or nearly half.



Herman

Sixteen percentage points apart on the same question. These are estimates wearing lab coats. When two reputable firms disagree by more than a factor of two on growth, what you're learning is that nobody has visibility into actual unit shipments — which itself tells you the market is small, defence-adjacent, and partly classified.



Corn

And there's a line I wanted you to hit — the report saying software diodes can't really be called diodes.



Herman

The Dutch HSD report, drawing on practitioner interviews: software-based data diodes are very hard to protect and cannot be acknowledged as being a true data diode. Same report notes zero reported bypasses of the hardware kind — no diode is known to have been defeated — while conceding, in the same breath, that proliferation is limited. Absence of incidents in a small, guarded population is a weaker claim than it sounds.



Corn

Six thousand diodes, no reported incidents. Call me when the denominator grows.



Herman

The last thing, and to me the most honest one in the whole episode: the diode is a monument to legacy systems. The HSD report points out these devices let operators keep ancient equipment running — going back as far as Windows 3.1-era kit — without an overhaul. Which is the technology's best feature and its most damning one at the same time. It doesn't modernize anything. It buys time.



Hilbert

Which of you said "buying time" like it was a small thing?



Corn

That would be him.



Hilbert

Hm. I ran a one-way feed for eleven years and nobody ever framed it as philosophy. Presses, the old kind. You cannot unbake a print. We had a hatch, you'd send the plate down and that was that. There was a man on the other side, a Lithuanian fellow, Simeonas, who kept insisting we could route a return line for corrections. I told him corrections were what the next edition was for. He left, eventually, went to Vilnius. I still think about him around two in the morning, because he was right, in a way — the return line was the whole business, that was the part worth money. We just called it the morning.



Corn

You're describing an air gap with a schedule.



Hilbert

We called it the dumbwaiter, which I grant you was generous. Everything about it was generous. It cost nothing, it never broke, and it never once came back up with anything useful in it.



Herman

Eleven years of a one-way channel and no complaints about the direction.



Hilbert

Complaints, plenty. About the direction, none. Corn, you'd have liked it. Nothing arrived, and you were never expected to answer.



Corn

That's the most flattering thing anyone's said about my work habits.



Hilbert

Simeonas wrote me a letter once, after Vilnius. I never replied. One way.



Corn

There it is.



Herman

So the question that's been sitting under this whole episode for me is the one the legacy point raises. The diode's pitch is that it cannot be reconfigured — that's the strength, no rule set, no admin, no mistake possible. But the Windows 3.1-era machine behind it doesn't last forever. Eventually someone has to replace the controller, the pump, the signalling box. And then you have to ask whether the diode goes with it or whether it's now permanent scaffolding.

Corn

My money's on scaffolding. Nobody rips out the one component that never caused an incident.



Herman

And there's a second thing worth watching, which is the regulatory split. The French moved to their four-class model last December and banned firewalls outright for the most sensitive networks. The Americans took the recognition-and-encouragement route through NERC — no ban, just credit for going one-way. Two philosophies, same hardware. If the American approach spreads, you get diodes chosen by auditors. If the French approach spreads, you get firewalls legislated out of the top tier entirely. Those markets would look very different.



Corn

One thing to take from this, if you take anything: the diode doesn't protect the network receiving the data. One packet of malware down a one-way pipe is still a delivery. The guarantee covers the sender only.



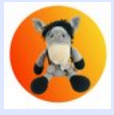
Herman

And the sender is exactly who the nuclear plant, the dam, the signalling room care about protecting — which is why the guarantee works there, and why you should read the marketing of anything else with one eyebrow up.



Corn

Producer credit where it's due — Hilbert Flumingtop, at the desk as always. For more along these lines, there's episode one thirty-nine, The Vanishing Air Gap; and episode eighteen, Beyond the GPU. This has been My Weird Prompts. If the show's earned it, a review on Spotify takes about thirty seconds and helps more than you'd think. We'll be back soon — see you then.



Herman

See you.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Owl Cyber Defense, Why Data Diodes Are Critical to Modern Critical Infrastructure Security [primary]**

   published 2025-07-09, retrieved 2026-11-14.
   https://owlcyberdefense.com/blog/what-is-data-diode-technology-how-does-it-work/

2. **Owl Cyber Defense, Owl and Trihedral Integrate VTScada and Data Diodes [primary]**
published 2026-06-02, retrieved 2026-11-14.
https://owlcyberdefense.com/news/owl-and-trihedral-integrate-vtscada-and-data-diodes/

3. **Waterfall Security Solutions, Protecting Rail Signaling Networks from External Cyber Threats (case study PDF) [primary]**
2022, retrieved 2026-11-14.
https://waterfall-security.com/wp-content/uploads/2022/08/WF_Rail-Signalling_case-study.pdf

4. **Waterfall Security Solutions, Securing the Digital [Nuclear Generation Perimeter] (use case PDF) [primary]**
retrieved 2026-11-14.
https://waterfall-security.com/wp-content/uploads/Waterfall-Nuclear-Use-Case.pdf

5. **Waterfall Security Solutions, NERC CIP V5 Standards and Unidirectional Network Protection [primary]**
retrieved 2026-11-14.
https://waterfall-security.com/ot-insights-center/ot-security-standards/nerc-cip-v5-standards-and-unidirectional-network-protection-whitepaper/

6. **NERC, Security Guidelines for the Electricity Sector: Control System Electronic Connectivity (PDF) [primary]**
retrieved 2026-11-14.
https://www.nerc.com/globalassets/who-we-are/standing-committees/rstc/swg/control_systems_electronic_connectivity_guideline.pdf

7. **OPSWAT, Data Diodes and NERC CIP: Your Fast Pass to Compliance [primary]**
retrieved 2026-11-14.
https://www.opswat.com/blog/data-diodes-and-nerc-cip-your-fast-pass-to-compliance

8. **OPSWAT, Data Diode Use Case [primary]**
Wastewater SCADA Cybersecurity Compliance, retrieved 2026-11-14.
https://www.opswat.com/blog/how-opswats-data-diode-solution-strengthens-a-north-american-wastewater-operations-security

9. **OPSWAT, Safer Water Operations with Secure Data Transfers [primary]**
retrieved 2026-11-14.
https://www.opswat.com/blog/safer-water-operations-with-secure-data-transfers

10. **Fend Incorporated, Water and Infrastructure Cybersecurity [primary]**
retrieved 2026-11-14.
https://www.fend.tech/water-infrastructure

11. **ANSSI, Cybersecurity of Industrial Control Systems [primary]**
Classification Method, v2.0 (ANSSI-PA-107-EN), published 2025-12-04, retrieved 2026-11-14.
https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-industrial_control_systems-classification_method_v2-0.pdf

12. **ANSSI, Profil de protection d'une diode industrielle et de ses guichets, v1.0 [primary]**
GTCSI 2015-07-01, retrieved 2026-11-14.
https://messervices.cyber.gouv.fr/documents-guides/20151005_NP_ANSSI_SDE_4067_PJ2_diode_moyen_terme_PJ2.vfp_.pdf

13. **Wikipedia, Data diode**
retrieved 2026-11-14, last edited 2026-10-26.
https://en.wikipedia.org/wiki/Data_diode

14. **Wikipedia, Air gap (networking)**
(networking), retrieved 2026-11-14, last edited 2026-11-03.
https://en.wikipedia.org/wiki/Air_gap

15. **Hamed Okhravi, Data Diodes in Support of Trustworthy Cyber Infrastructure (CSIIRW10), MIT**
retrieved 2026-11-14.
https://web.mit.edu/ha22286/www/papers/CSIIRW10.pdf

16. **PR Newswire, Iberdrola's Spanish Cofrentes Nuclear Power Plant Deploys Waterfall Security's Unidirectional Security Gateways**
published 2011-08-04, retrieved 2026-11-14.
https://www.prnewswire.com/news-releases/iberdrolas-spanish-cofrentes-nuclear-power-plant-deploys-waterfall-securitys-unidirectional-security-gateways-126761743.html

17. **Peter Cohan, Forbes, Waterfall Security Defends Power Plants From Hackers**
published 2013-09-23, retrieved 2026-11-14.
https://www.forbes.com/sites/petercohan/2013/09/23/waterfall-security-defends-power-plants-from-hackers/

18. **TD World, NERC Recognizes Security of Unidirectional Communications**
published 2012-01-12, retrieved 2026-11-14.
https://www.tdworld.com/smart-utility/article/20958390/nerc-recognizes-security-of-unidirectional-communications

19. **FERC, Waterfall Security Solutions remarks on CIP Version 5**
remarks dated 2016-01-28, retrieved 2026-11-14.
https://www.ferc.gov/sites/default/files/2020-08/Ginter-WaterfallSecuritySolutions.pdf

20. **The Hague Security Delta, The Case of Data Diodes for Cybersecurity (PDF, 48pp)**
retrieved 2026-11-14.
https://securitydelta.nl/media/com_hsd/report/246/document/HSD-Rapport-Data-Diodes.pdf

21. **4Secure, Top Data Diode Vendors: 2026 Buyer's Guide**
retrieved 2026-11-14.
https://www.4-secure.com/data-diode-vendors/

22. **MarketsandMarkets, Data Diode Market Report 2026-2031 (Report Code TC 9266)**
published May 2026, retrieved 2026-11-14.
https://www.marketsandmarkets.com/Market-Reports/data-diode-market-36397871.html

23. **MarketsandMarkets, Data Diode Market research insight**
retrieved 2026-11-14.
https://www.marketsandmarkets.com/ResearchInsight/data-diode-market.asp

24. **Fortune Business Insights, Data Diode Solution Market Size & Share (Report ID FBI104770)**
last updated 2026-05-25, retrieved 2026-11-14.
https://www.fortunebusinessinsights.com/data-diode-solution-market-104770

25. **TMC Insight (Rich Tehrani), Global Data Diode Cybersecurity Demand Rising**
published 2026-07-07, retrieved 2026-11-14.
https://insight.tmcnet.com/insight/researchandmarkets-com-adds-new-forecast-highlighting-rising-global-demand-for-data-diode-cybersecurity-mra94jan