

BOOK SEVEN

The Power Plant Had a Second Network

How a private cellular network became a path into a power plant's controls, and how to catch it in time.

NetOpsIQ™

Eldad Matityahu

Published October 7, 2026



Soly Moses / Pexels · Illustrative photograph

Inside the second network.

A Letter Before We Begin	03	06 Three Questions Before You Touch Anything	14
Four Ideas to Carry	04	07 Close the Path, Keep the Plant Running	16
01 The Plant Has More Than One Network	05	08 The Alarm Still Has to Work	18
02 Eleven Quiet Days	07	09 Ten Minutes With the Energy Leader	20
03 The Damage Is Not Always a Blackout	09	A Closing Word: Before Next Winter	21
04 Seven Doors Into the Energy Operation	11	Notes	22
05 The Trail They Left	12		

PHOTOGRAPHS ARE ILLUSTRATIVE. IMAGE SOURCES APPEAR AFTER THE NOTES.

A Letter Before We Begin

To the people who keep the heat and the power on.

Ask any plant manager how the site is protected, and you will hear a good answer. A firewall. A segmented control network. A security team that watches the corporate side.

Then ask a harder question. How many networks does the plant actually have?

Most people count one. The real number is usually higher. There is the cellular router in a cabinet that a vendor installed years ago. There is the private mobile network the grid operator uses to read your equipment. There is the remote link a contractor still has. Each one is a road into the plant, and most of them never made it onto the diagram.

In December 2025, an attacker used one of those roads. They crossed from a wind farm to a heat-and-power plant through a private cellular network, spent days learning the plant, and then stopped its turbine.

This book tells that story using only what investigators have published. Then it asks what your team would have seen, and when.

The goal is simple. Find the second network before someone else does. Watch it. And when something goes wrong, close the unsafe path while the plant keeps running.

Eldad Matityahu Founder and CEO, NetOps IQ

Four Ideas to Carry

1. A plant has more than one network. The wired control network is the one everyone draws. Cellular, radio and vendor links are the ones attackers look for.

2. Private is a setting, and settings can be wrong. A private mobile network can still let every device on it talk to every other device. In Poland, that one setting connected a wind farm to a power plant.

3. Attacks are loud on the plant side. Before a turbine stops, controllers start doing new things and strangers start talking to them. Someone has to be listening.

4. Close the path. Keep the plant running. Prove both. A fix that stops the attacker and also stops the heat has failed. Every response needs a security check and a service check.

01 The Plant Has More Than One Network

The plant has wires. The operation also has air.

Walk through any modern energy site and you will find the network everyone knows. Cables run from the control room to the controllers that open valves, spin turbines and pump water. A firewall guards the edge. The security team has a map of it.

Now open a few cabinets.

Inside one, a small cellular router with a SIM card blinks quietly. A vendor put it there so they could check the equipment without driving out. Inside another, a field controller reports to the grid operator over a mobile link. At the wind farm down the road, every turbine phones home the same way.



Shameer Vayalakkad Hydrose / Pexels · Illustrative photograph

None of that traffic crosses the plant's firewall. It travels through the air, through a mobile carrier, to wherever it was set up to go.

What a private APN is, in plain words. An APN, or access point name, is the door a SIM card uses to get onto a mobile data network. A public APN leads to the internet. A private APN leads to a closed network that a carrier sets aside for one organization, often the local grid operator. Operators use it to read and control equipment spread across many sites.

It sounds like a private line. In practice, it can work more like a shared hallway. Every site with a SIM on that APN is a neighbor. If the hallway lets neighbors knock on each other's doors, one broken lock anywhere puts every door at risk.

Why it stays off the map. The plant often does not own this network. The grid operator does, or a vendor, or a carrier. So it rarely shows up in the plant's own security review. Nobody is careless. The road simply belongs to someone else.

That is the second network. The rest of this book is about what happened when someone used it.

02 Eleven Quiet Days



Syrena Carver / Pexels · Illustrative photograph

Independent evidence. Every fact in this chapter comes from CERT Polska's findings as reported by the outlets listed in the Notes.

The warning came first. CERT Polska says this was likely the first time attackers used a private cellular network as a way in, and that the same weak setup is common in Poland and worldwide.

This is how it played out.

A campaign, and a small plant. The plant heats about 50,000 homes. It was the second facility hit that day, in a campaign that also struck about 30 wind and solar sites and a larger heat-and-power plant, where equipment was destroyed beyond repair. The campaign was linked to the Sandworm group.

The route nobody drew. The attack started at a wind farm. The attacker broke into its firewall, then used a cellular router to reach a private network run by the local grid operator. That network was built so the operator's control center could talk to equipment in the field.

It had one setting wrong. Devices on it could talk to each other. So a wind farm could reach a power plant. The two sites shared nothing except a mobile network they both trusted.

Day 1. December 18. The attacker searched that network and found a controller at the plant with its admin page open and the factory password still set. That controller became the doorway into the plant's control systems.

Day 8. December 25. By Christmas, the attacker was sending commands to the Siemens controllers that ran the plant.

Day 12. December 29. At about 5:30 in the morning, someone logged into the plant's control system and switched the controllers to STOP. The turbine and the water-treatment system shut down, and the controllers were locked with a new password. The crew began recovering while the attacker was still inside.

Then the attacker wiped the routers and erased the logs on the way out.

03 The Damage Is Not Always a Blackout



Dave Meckler / Unsplash · Illustrative photograph

The most dangerous attack can be the one that stops just enough.

When people imagine a cyberattack on energy, they picture a city going dark. That picture makes the problem feel rare and distant.

The Polish plant tells a quieter, more useful story. The turbine stopped. The water-treatment system stopped. Cogeneration, the plant's whole reason for existing, was interrupted. And the controllers were locked with a password the operators did not have, so they could not simply switch them back on.

The crew started recovering while the attacker was still inside. Picture that morning. You are restoring a plant you can no longer fully trust, against someone who may still be watching.

Then the attacker erased the trail. Routers were reset. Firewall logs were wiped. The controller used as a doorway was damaged. Investigators started with less evidence than they needed.

Elsewhere in the same campaign, the damage was worse. At about 30 wind and solar sites and a larger heat-and-power plant, equipment was destroyed beyond repair.

What the cost really looks like. It is the hours of not knowing. It is crews sent to check every cabinet. It is the choice between restarting fast and restarting safely. It is the regulator's questions, and the ones from the public.

Resilience in this world comes down to one thing: how fast you know what is happening, and how precisely you can act on it.

04 Seven Doors Into the Energy Operation

Five of these doors were open in Poland. All seven are open somewhere today.

1. The forgotten cellular router. The attacker reached a cellular router at the wind farm after the firewall fell. Its default password had been changed. It still became the bridge to the private network. One good fix is a start, never the finish.

2. The private network no one inventories. The grid operator's private APN let devices on it reach each other. That single setting turned a wind-farm breach into a power-plant breach.

3. The vendor connection that never closes. Remote access set up for one repair often stays open for years. Every always-on link is a road someone else can drive.

4. The exposed management interface. The doorway controller at the plant showed its admin page to anyone on the private network. That page let the attacker turn on remote login.

5. The flat path from renewables to plant controls. Nothing stopped traffic from a wind farm from reaching a heat-and-power plant's controller. Two sites, two owners, one shared path.

6. The device with default or shared credentials. The doorway controller still used its factory password. Every week of the attack rested on that one login.

7. The fix nobody checked. After a change, teams often confirm the system works and move on. Nobody checks whether the risky path is actually gone, or whether it quietly came back.

05 The Trail They Left

Findavi could not have seen the wind-farm break-in or the grid operator's network. Those sit outside the plant.

Inside the plant, the attack was loud, for days.

A controller learned a new trick. The doorway controller had one job. Then remote login appeared on it. If that login traffic crosses the switch Findavi watches, Findavi flags a device running a service it has never run. If it arrives only over the cellular side, the next two signals are where Findavi sees the attack.

New paths opened inward. Traffic flowed from that controller to parts of the plant it had never reached. Findavi flags new paths into operational systems.



Sergei Starostin / Pexels · Illustrative photograph

A stranger spoke to the turbine controllers. On Christmas Day, commands reached the Siemens controllers through the doorway controller, a device that had never sent them before. Findavi flags that source as unfamiliar.

The STOP command arrived. Findavi recognizes a STOP command to a Siemens controller when it sees one. But by then, the damage is underway. That is why the earlier signals matter most.

The factory password was a signal too. Findavi can flag devices likely still on factory defaults by make and model, while only listening. A login is actively tested only with the customer's approval.

Findavi sits beside the plant's network switch, on a mirror (SPAN) port or a network tap. It sees everything that crosses that switch and touches nothing. So placement matters: it belongs on the control-network switch where the doorway controller connects.

This is the step CERT itself recommends: watch traffic between the control network and the private cellular network, and flag anything unusual.

In Approve mode, each signal goes to a named person with one recommended action, such as blocking a single connection, while the grid operator's normal data keeps flowing. Then two checks: is the unsafe path closed, and is the plant still running?

The honest line. No public report shows any monitoring at this plant, and we don't claim Findavi would have stopped this attack. We claim the attack left eleven days of plant-side signals, and those are the signals Findavi is built to catch.

06 Three Questions Before You Touch Anything

What can it reach? What does it support? Can we restrict it without an outage?

In an office, the safe move during an attack is often to pull the plug. In a power plant, pulling the wrong plug can do the attacker's job for them. The private network that carried the attack also carried the grid operator's legitimate data. Cut it all, and the people balancing the grid lose sight of your plant.

So every response starts with three questions, asked about the specific device in front of you.

Asset	The real question
Cellular router	Can it reach only approved remote systems, or can it scan and connect across the whole private network?
Controller	What equipment or process depends on it, and what happens if its network path is restricted?
Vendor link	Is access time-limited, approved, logged, and limited to the one device it needs?
Control-network gateway	Does it bridge renewable sites, plant controls and business systems?
Operator screen or engineering workstation	Can it still monitor and safely manage the process after the risky path is closed?

If you cannot answer these questions before an incident, you will be guessing during one. Answering them is most of the work of being ready.

07 Close the Path, Keep the Plant Running

Contain the connection. Leave the generation alone.

The right response is narrow. You want to shut the one road the attacker is using, while every approved road stays open. Findavi works through it in seven steps.

1. Spot a device talking outside its normal pattern, such as a gateway controller that suddenly accepts remote logins.
2. Check the customer's own operating rules for that device.
3. Send the finding to the right owner, with a plain summary and one recommended action.
4. Wait for that person's approval, in Approve mode.
5. Act narrowly: block one connection, isolate one port, or push one configuration change.

6. Confirm the unsafe path is closed, and confirm the approved traffic still flows.

7. Record every step, with the time and the approver's name.

The customer chooses the mode for each agent. Observe only watches and reports. Approve acts after a named person says yes. Autonomous acts on rules the customer has already signed off. Any agent can be stopped, rolled back or switched off at any time.

Observed: a live water site. Pilot result, confirmed by NetOps IQ's CTO. Different sector, same kind of control system.

During a pilot at a live water site, the team ran a simulated attack on the plant's controller screens, the screens operators use to run the process. Findavi blocked the attacking connection and isolated a port. Then it ran both checks. The security check passed: the attacking path was closed. The service check passed: the controls kept running for the operator.

A water plant and a power plant run on the same kind of equipment: controllers, operator screens and remote links. The lesson carries over. You can close the dangerous path while the people running the plant keep working.

08 The Alarm Still Has to Work

Closing the door is half the job.

Every action Findavi takes ends with two questions.

The security check. Is the unauthorized path closed? Findavi confirms the blocked connection no longer carries traffic.

The service check. Is the plant still working? Findavi confirms that the approved traffic it can see still flows: operator screens still talk to their controllers, and the grid operator's data still arrives.

Both must pass. A fix that stops the attacker and silences an alarm has traded one risk for another.



Bulat843 / Pexels · Illustrative photograph

Where the network stops and people take over. Findavi sees the network. It does not stand next to the turbine. The process itself, steam pressure, water quality, a running motor, is confirmed by the operator on site. The best response pairs the two: the network check from Findavi, the physical check from the crew.

Proof that lasts. Every alert, approval, action and check lands in an audit trail with a time and a name. When the regulator, the insurer or your own board asks what happened, the answer is already written down.

All of this runs on the Findavi appliance inside your site. The analysis happens on the device, and your plant's data stays there.

09 Ten Minutes With the Energy Leader

Speak the language of the plant.

The person who runs a power plant does not lose sleep over protocols. They lose sleep over a turbine that will not restart, a town without heat in January, and a phone call from the regulator.

So the conversation starts there. Will generation stay available? Will heat and power keep flowing? Is the equipment safe? How much work lands on the field crew? How fast can we recover, and how sure can we be? What does a broad precautionary shutdown cost us, compared with a precise one?

The Polish case answers the first question for them. A private network shared with a wind farm became a road to their turbine. Investigators say that setup is common. The honest next step is to find out whether it exists at their plant.

The first ask is small. Start with one plant, one renewable site, one private cellular network, one fleet of cellular routers, or one vendor remote-access path.

That is the Blind Spot Assessment. The Findavi appliance connects to a passive port and listens. It touches no device and needs no internet connection. Within days, the team sees which devices exist, who they talk to, which ones are likely still on factory passwords, and which paths lead somewhere they should not.

Then the leader decides what to close, and in which mode. Nothing moves without their rules.

A Closing Word: Before Next Winter

The attacker in Poland needed eleven quiet days. Every one of them happened on equipment the plant owned, on a network the plant could have watched. Winter is when heat matters most, and it is when this attack landed. Before the next one, ask your team three things:

1. **Is our private cellular network shared, or ours alone?** Can devices on it reach each other?
2. **Which devices connect that network to our control systems?** Do any still use factory passwords?
3. **Is anyone watching the traffic between the two?**

If the answer to the third one is no, you have a second network nobody is watching.

Notes

- [Circuit Magazine: Polish CHP plant private APN OT attack](#)
- [SecurityWeek: Novel Private APN Pivot Let Hackers Sabotage Second Polish Energy Facility](#)
- [Infosecurity Magazine: Russian-Linked Hackers Accessed Polish Power Plant OT Network Through Private APN](#)
- [The Hacker News: Hackers breach Polish power plant](#)
- [EveryWAN: Carrier private APN, who else is inside](#)

Sources checked October 12, 2026. Equipment named in CERT Polska's findings: Teltonika RUTX50 router, WAGO PFC200 controller, Siemens S7-300, S7-1200 and S7-1500 controllers.

The photographs.

These are illustrative stock photographs of other sites and equipment. They do not show the Polish incident, a Findavi deployment, or the people involved. No endorsement is implied.

Cover / industrial power plant at night

[Soly Moses / Pexels](#)

Chapter 1 / electrical control room

[Shameer Vayalakkad Hydrose / Pexels](#)

Chapter 2 / winter wind turbines, Howard, New York

[Syrena Carver / Pexels](#)

Chapter 3 / historic Georgetown Steam Plant, Seattle

[Dave Meckler / Unsplash](#)

Chapter 5 / network connections

[Sergei Starostin / Pexels](#)

Chapter 8 / technician inspecting equipment

[Bulat843 / Pexels](#)

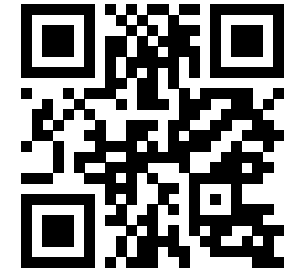
[Pexels License](#) · [Unsplash License](#)

Start with one plant.

The first ask is small. Start with one plant, one renewable site, one private cellular network, one fleet of cellular routers, or one vendor remote-access path.

That is the Blind Spot Assessment. The Findavi appliance connects to a passive port and listens. It touches no device and needs no internet connection. Within days, the team sees which devices exist, who they talk to, which ones are likely still on factory passwords, and which paths lead somewhere they should not.

Then the leader decides what to close, and in which mode. Nothing moves without their rules.



Visit netopsiq.com

REQUEST AN ASSESSMENT

netopsiq.com/assessment

info@netopsiq.com

The blind spot, secured.
NetOpsIQ™

netopsiq.com