AEIC GRID ADVANCEMENT PROGRAM · CHALLENGE BRIEF

Securing the Grid: OT/IT Convergence

Challenge 09. The operating problem, why it is hard, and what the cohort will work.

Working session	Tuesday, April 13, 2027, 2:00 p.m. ET
Cadence	Second Tuesday of every month, 2:00 p.m. ET
Eligibility	AEIC members and any electric utility
Join	https://aeicopscenter.org/grid-advancement
Program	AEIC Center for Operational Excellence

The problem

OT and IT are converging whether or not anybody planned for it. Every meter, recloser, inverter, and DER interconnection is a connected device, and every connected device is a way in. The attack surface is not a perimeter on a map anymore. It is the edge of the distribution system, and it grows every quarter.

Meanwhile OT was built for availability and for a thirty or forty year life, not to be patched, and often it cannot be. The relay that has run flawlessly since before your security team existed runs an operating system nobody supports, speaks a protocol that trusts anything on the wire, and sits one hop from a network that touches the internet.

The problem is not that utilities are careless. It is that the only security model anybody knows how to run is an IT model, and it assumes a thing that is not true in operations: that you can take the system down.

Why this challenge

Because it is the one where the standard playbook is actively wrong, and running it anyway is how you cause the outage you were trying to prevent.

The IT team patches on Tuesday. The operations team cannot take a substation down on Tuesday, or any other day, without a switching order, an outage window, a load transfer, and a very good reason. Both teams are right. The gap between them is not a communication problem you fix with a joint standup. It is a real difference in what the system is for.

Every other challenge in this program asks you to see more, connect more, control more. Every one expands this attack surface. This challenge is the bill.

Where utilities actually are

Most utilities are running some version of the same three postures, and none of them are unreasonable.

The perimeter. A hard shell around the OT environment, a firewall, a DMZ, and an assumption that what is inside is trusted. It is a real control, and it fails the moment somebody gets in, because inside the shell the network is flat and the protocols authenticate nobody.

Compliance. NERC-CIP is doing real work, and utilities that take it seriously are genuinely harder to hurt. But CIP draws a boundary around the bulk electric system, and the attack surface growing fastest sits on the distribution side of it. **You can be fully compliant and fully exposed on the same day.** The audit will not fail you for that.

Air gap by memory. A lot of shops still describe their OT network as isolated, and it was, once. Then came a firmware push, a remote support session, an engineering laptop that was on the corporate network last week. The air gap is usually a description of the past, and the honest work is finding out where it stopped being true.

None of these are wrong. They are what you do when the perimeter is the only line you know how to draw.

The hard part

The technology mostly exists. Segmentation, device certificates, OT-aware monitoring, secure remote access, asset discovery. All real, all deployed somewhere right now. The hard part is not the technology. It is these four things:

1. You cannot patch what you cannot take offline. IT security is built on a reboot. Push the update, restart the box, move on. Operations does not have that move. Outage windows are scarce, and half the time the patch does not exist, because the device is fifteen years past support and the company that built it is gone. So the

honest question is not how to patch faster. It is what to do about the thousands of devices that will never be patched and will still be in service in 2040. Compensating controls, not remediation.

2. Identity was built for people, and the things you have to trust are not people. Your identity program has a joiner-mover-leaver process, an HR system of record, and MFA. None of it applies to a recloser. Devices do not get onboarded, they get installed, often with a default credential, and they never leave, because there is no offboarding. And the largest standing trust relationship in most OT environments is not an employee. It is supplier remote access into the equipment they support, which is normal, is usually necessary, and is how that equipment stays healthy. It is also rarely reviewed, because reviewing it is not written into anyone's job.

3. The network is flat, and flat was the point. OT protocols were designed to trust each other. Availability mattered, confidentiality did not. Segmentation is the right answer, and few utilities can say they have finished it, because you cannot segment what you have not inventoried, and you cannot inventory a network you are afraid to scan. That is genuinely hard, and it is a technical problem, not a diligence problem.

4. Compliance is a floor, and the incentive structure treats it as a ceiling. When the metric is the audit, the program is rewarded for the audit. Scope gets managed rather than reduced, and the work that matters most earns no credit with a regulator. Going beyond CIP means arguing for capital against an event that did not happen, the same unsolved business case in every challenge in this program.

If you need one sentence to carry into a board or audit conversation: **we can be fully compliant and fully exposed on the same day, and the audit will not fail us for that.** That is not an argument against compliance. It is an argument for what compliance was never scoped to cover.

None of those four barriers is local to you. In some form, all four show up in all ten challenges in this program: the asset you cannot see, the boundary the data cannot cross, the work that falls between IT and operations, and the value that is an incident that did not happen. If your list looks like this one, you are not behind. You are in the same room as everyone else.

And "we do not know how many OT assets we have" is a legitimate answer here. It is the most common honest answer in this challenge, and it is a finding, not a failure. Bring the estimate and the error bars.

What the cohort will work

Not "which security product should we buy." The room is going to work what actually blocks deployment:

- What do you actually do about unpatchable assets that stay in service another fifteen years?
- Is anybody handling device identity at scale, and who owns and reviews supplier remote access?
- Segmentation: what got finished, what stalled, and what did it cost?
- How do an IT security team and an operations team make one decision together, without one overruling the other?
- What has been tried and did not work? That is the most valuable hour in this program, and it is the one you can only get from peers who have actually tried it.

What to bring

You do not need a solved problem. You need an honest one. Come with:

- One decision you are stuck on
- Your best honest estimate of how many OT assets you cannot patch
- How suppliers get into your OT environment today, and who reviews that access
- One thing you tried that did not work

If the honest answer to any of those is "we do not know," bring that. It is a finding, not a failure, and you will not be the only one saying it.

What you get

- This brief, and a short video briefing, before the session
- The Flight Plan, a working pilot scaffold, inside InnovationWorks
- The session itself, with the utilities living this problem
- A retrospective afterward: what the cohort tried and what happened

Join

Tuesday, April 13, 2027, 2:00 p.m. ET. Recruitment runs per challenge, so your OT security people can come to this one without committing to all ten.

Open to AEIC members and to any electric utility. If you run a utility, you are welcome here.

https://aeicopscenter.org/grid-advancement
Knowledge of one is the knowledge of all.
Sources: this challenge was developed from research of public utility filings. The technology landscape for this challenge is maintained separately inside InnovationWorks.