MY WEIRD PROMPTS

Podcast Transcript

EPISODE #139

The Vanishing Air Gap: IT vs. Operational Technology

Published January 03, 2026 • Runtime: 17:19

https://myweirdprompts.com/episode/industrial-ot-vs-it-security/

EPISODE SYNOPSIS

In this episode of My Weird Prompts, Herman and Corn dive into the hidden world of Operational Technology (OT)—the systems that keep our lights on and water flowing. They explore the critical differences between the IT world’s focus on data and the OT world’s obsession with physical availability and safety. From the legendary "air gap" and the Purdue Model to the risks of connecting legacy hardware to the 2026 cloud, the brothers break down why a software update in a factory is often viewed as a threat rather than a feature. Whether you're curious about the future of industrial cybersecurity or looking to bridge the gap between "graybeard" technicians and modern IT pros, this deep dive reveals the high-stakes reality of the machines that run our world.

DANIEL'S PROMPT

Daniel

I’d like to talk about the operational internet, or OT. How interoperable is the OT network with the regular internet? Could you connect a browser to the network in a power plant, or is there a hard divide between OT and IT networks for safety reasons? Also, what is the industry like for people who manage these networks? Are there separate degrees, courses, or certifications for OT, similar to those in the regular IT world?

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts! I am Corn, and as always, I am joined by my brother, who is looking particularly ready to dive into some technical weeds today.

Herman

Herman Poppleberry at your service, Corn! And you are right. This prompt from our housemate Daniel really struck a chord. He was asking about operational technology, or OT, which is basically the nervous system of the physical world. It is the stuff that makes sure when you flip a switch, the lights actually come on, or when you turn a tap, water actually flows.

Corn

It is funny because we spend so much time talking about the internet we see on our screens, the IT side of things, but we rarely think about the industrial side. Daniel mentioned he worked for an industrial internet of things company, so he has seen this firsthand, but he wanted us to dig into how separate these worlds really are. Like, could you actually pull up a web browser on a console in a power plant and watch cat videos?

Herman

Well, the short answer is that you probably could, but you absolutely should not. In fact, if you did, you would likely have a very angry security officer at your desk within about thirty seconds. This is where we get into the concept of the air gap, which is this legendary, or perhaps mythical, hard divide between the regular office network and the industrial control systems.

Corn

Right, and as we move into twenty twenty-six, that air gap is feeling more like a screen door than a brick wall. Remember back in episode two hundred forty-one when we talked about missile defense alerts? That was all about real-time systems where milliseconds matter. OT is very similar. It is not just about moving data; it is about moving physical matter.

Herman

Exactly. In the IT world, we care about the CIA triad, which stands for Confidentiality, Integrity, and Availability. We want our emails kept secret, we want them to be accurate, and we want to be able to read them when we need to. But in the OT world, they flip that on its head. They care about the AIC triad. Availability is king. If a cooling pump in a nuclear reactor stops working because of a software update, that is a catastrophic failure. Integrity comes second, making sure the sensor says ten degrees when it is actually ten degrees. Confidentiality is actually often the lowest priority.

Corn

That is such a fascinating shift in perspective. If my email is down for five minutes, I am annoyed. If the city's water pressure regulation system is down for five minutes, pipes start bursting. So, Daniel asked about interoperability. Are these systems using the same protocols we use to browse the web?

Herman

They are starting to, but it is complicated. Historically, OT used very specialized, proprietary protocols. You had things like Modbus, which was developed way back in nineteen seventy-nine, or Profibus and BacNet. These were designed to be very simple and very fast, running over serial cables. They did not have any security because, back then, the only way to talk to the machine was to be standing right next to it with a physical cable.

Corn

But now we have Industrial Ethernet, right? That was one of the things Daniel mentioned.

Herman

Yes, Industrial Ethernet is basically the ruggedized, high-performance cousin of the Ethernet we use at home. It uses the same physical connectors, mostly, but the protocols on top of it are designed for determinism. In a regular office, if a packet takes an extra fifty milliseconds to arrive, nobody notices. In a factory where a robotic arm is moving at three meters per second, fifty milliseconds is the difference between a perfect weld and a hole in the floor.

Corn

So, let's get back to the browser question. If I am sitting at a Human-Machine Interface, or an HMI, which is basically the touchscreen or computer that operators use to watch the plant, am I on the internet?

Herman

Usually, no. If the system is designed correctly, you are sitting in what we call the Purdue Model. This is a framework that divides the industrial network into levels. Level zero is the actual hardware, the motors and sensors. Level one is the controllers, like the PLCs or Programmable Logic Controllers that Daniel mentioned. Level two is the supervisory control. By the time you get to Level four or five, you are in the corporate office network.

Corn

And there is supposed to be a DMZ, a Demilitarized Zone, between those levels.

Herman

Precisely. A proper OT setup has a very strict firewall between the office and the plant. Information should only flow one way if possible, or through very tightly controlled gateways. You might have a web-based HMI where the interface looks like a website, but it is hosted on a local server that has never seen the public internet. If you tried to go to a search engine or a social media site, the firewall would just drop the request.

Corn

But we know this is changing. With the rise of the Industrial Internet of Things, companies want that data in the cloud. They want AI to analyze their power consumption or predict when a bearing is going to fail. That means they are punching holes in that firewall.

Herman

And that is exactly why cybersecurity in OT is the fastest-growing part of the industry right now. We have seen attacks like Stuxnet or the more recent ones on power grids in various parts of the world. When you connect a nineteen eighties water pump controller to a twenty twenty-six cloud platform, you are asking for trouble if you do not know what you are doing.

Corn

It feels like a clash of cultures. The IT people want to patch everything every Tuesday, and the OT people want to never touch a working system for twenty years.

Herman

You hit the nail on the head. I once talked to a plant manager who said that a firmware update is a threat, not a feature. To them, "new" means "untested."

Corn

Speaking of people who manage these things, let's take a quick break to hear from our sponsors. Larry: Are you worried about the invisible rays coming out of your toaster? Do you feel like your neighbor's Wi-Fi is slowly rewriting your DNA? You need the Lead-Lined Liberty Hat. It is not just a fashion statement; it is a personal fortress for your brain. Each hat is hand-forged from recycled car batteries and lined with a proprietary blend of tin foil and beeswax. It is heavy, it is uncomfortable, and it smells faintly of honey and despair. But can the government read your thoughts while you are wearing it? Probably not! Get your Lead-Lined Liberty Hat today and start living in a world of silent, heavy safety. Larry: BUY NOW!

Corn

Alright, thanks Larry. I think my neck hurts just thinking about that hat.

Herman

I am pretty sure wearing a lead hat is a health hazard in itself, but let's get back to the much safer world of high-voltage power grids and industrial automation.

Corn

Daniel also asked about the industry and the career path. Is this something you can just jump into if you have a Computer Science degree, or are there specific certifications?

Herman

It is actually a very different path. If you want to work in OT, a standard Computer Science degree is helpful, but it is often not enough. You see, in IT, if you break a piece of code, the program crashes. In OT, if you break a piece of code, a crane might drop a five-ton crate. Because of that, the industry heavily favors people with backgrounds in Electrical Engineering, Mechanical Engineering, or specialized Mechatronics.

Corn

So you need to understand the physics as much as the logic.

Herman

Exactly. You need to know what happens to a motor if you suddenly reverse its direction at three thousand RPM. But as the worlds converge, we are seeing new certifications. The big one is the GICP, which stands for the Global Industrial Cybersecurity Professional. There are also certifications from the International Society of Automation, or the ISA. They have the ISA ninety-nine and the IEC sixty-two four forty-three standards, which are basically the bibles of industrial security.

Corn

I have noticed that a lot of people in this field actually start as technicians or electricians. They are the ones who were out on the floor fixing the machines, and they learned the networking side of it as the machines got smarter.

Herman

That is very common. We call them the "graybeards" sometimes, though that is becoming less common as younger people enter the field. There is a huge generational gap right now. You have the older folks who know everything about the physical machinery but might not understand how an IP address works, and you have the younger IT folks who know everything about networking but do not know the difference between a solenoid and a relay.

Corn

The real superstars are the ones who can bridge that gap. The ones who can talk to the IT department about firewall rules and then go out onto the factory floor and troubleshoot a PLC.

Herman

And the demand is through the roof. Because of all the security concerns we talked about earlier, every major utility company, every manufacturing plant, and every city government is looking for OT security experts. They are paying huge salaries because the stakes are so high. If a bank gets hacked, money is lost. If a water treatment plant gets hacked, people get sick.

Corn

It is interesting that Daniel mentioned he never met someone whose career goal was to manage a city lighting network. It sounds mundane until you realize that if the streetlights stop working, the city stops moving. It is invisible work until it fails.

Herman

That is the tragedy of the infrastructure engineer. If you do your job perfectly, nobody knows you exist. It is only when things go wrong that you become the most important person in the room.

Corn

So, if someone is listening and they think this sounds like a cool challenge, where do they start? You mentioned the ISA and specialized degrees. Are there "home labs" for OT?

Herman

You can actually do quite a bit at home! You can buy small PLCs like an Arduino or a Siemens Logo for relatively cheap. There are also open-source simulators like Open PLC. You can learn the logic, which is often called Ladder Logic. It is a visual programming language that looks like an electrical circuit diagram. It is very different from Python or C plus plus.

Corn

Ladder logic is wild. It is literally designed so that an electrician in the nineteen seventies could understand it by looking at it as a series of switches and coils.

Herman

Right! And even though we have more advanced languages now, like Structured Text, ladder logic is still the king of the factory floor because it is so easy to troubleshoot in real-time. You can see exactly which "switch" is not closing.

Corn

I think one of the biggest takeaways here is that the "internet" is not one thing. We have this layer of the world that is increasingly connected but operates under totally different rules and risks.

Herman

Exactly. And the interoperability is a double-edged sword. We want the efficiency of the internet, but we do not want the vulnerability. That is why we are seeing a move toward Zero Trust architecture in OT. In the old days, if you were inside the factory, you were trusted. Now, we are moving to a model where every single command, every single sensor reading, has to be verified.

Corn

It is like what we talked about in episode one hundred ninety-five, about why AI won't talk to us first. It is all about control and boundaries. In OT, those boundaries are literally matters of life and death.

Herman

I think we are going to see a lot more of this in the next year. As we move through twenty twenty-six, the integration of AI into these OT networks is going to be the big story. Imagine an AI that can "feel" a vibration in a turbine that a human would never notice and shut it down before it explodes.

Corn

But then you have the risk of the AI making a mistake and shutting down a city's power grid because it thought a bird landing on a wire was a cyberattack.

Herman

That is the nightmare scenario. This is why the humans in this loop are so important. You need that gut feeling, that experience of being on the floor for twenty years, to know when the computer is being too cautious or not cautious enough.

Corn

Well, this has been a fascinating deep dive. I definitely have a new respect for the people who keep the "operational internet" running. It is definitely not just about cat videos and emails.

Herman

Not at all. It is about the physical reality we live in. Thanks for the prompt, Daniel! It was a great excuse to talk about some of these less-glamorous but absolutely vital technologies.

Corn

And hey, if you are out there listening and you have a weird prompt for us, or if you just want to tell us about your own experience with ladder logic or lead-lined hats, get in touch! You can find us at myweirdprompts.com. We have a contact form there and an RSS feed for all you regular subscribers.

Herman

And if you are enjoying the show, please leave us a review on your podcast app or on Spotify. It really does help other curious people find us. We are at episode two hundred forty-six, and we are not slowing down anytime soon.

Corn

This has been My Weird Prompts. I am Corn.

Herman

And I am Herman Poppleberry.

Corn

We will see you next time! Keep asking those weird questions.

Herman

Bye everyone!