IT vs. OT: Bridging the divide

Traditional IT is moving more onto the plant floor. OT will have to accept a greater level of integration. Is that a problem or an opportunity?

Peter Welander
08/16/2013

NOTICE
YOU ARE LEAVING THE I.T. SECTOR
DANGER
NO SMOKING IN THIS AREA
WARNING
THESE PREMISES ARE MONITORED TRESPASSERS WILL BE PROSECUTED

You’re a networking person who works in your plant in operations technology (OT), supporting the technology that keeps manufacturing going. An e-mail arrives with a message that strikes terror: Your corporate IT department has been assigned the task of updating networks and implementing new cyber security measures in the plant, and you are to cooperate. In other words, IT is moving into the plant. Is this necessarily bad news? It probably isn't good news, but the question is, why does the thought of combining IT and OT normally draw strong reactions?

"When you take people with an IT background and bring them into an industrial control system environment, there's a lack of understanding from operations why they're there and there is a lack of understanding of the specific controls environment needs from IT," says Tim Conway, technical director, ICS and SCADA for the SANS Institute. He points out that typically IT professionals are trained and driven to perform a task: "They work on a box, a VM (virtual machine), a storage area network, or a firewall. They don't realize that they're a part of a larger control system operation, and how the things that they do can impact others."

Conway's experience came from many years working in networking engineering and management at a mid-sized electric utility. He's seen how difficult it can be to develop IT personnel to realize the larger context: "If they're network guys, they see how a change affects their networks and the inter-dependent IT system functions, meaning active directory or workstation authentication, or monitoring and alerting, and all the other IT functions. But they don't think systemically from an operations perspective. For example, the impact out to the breaker in the substation if the communication path is lost. I compare the development challenge to what we do with our safety programs where we ask people to think about safety from the perspective of their work product. They have to think about how their actions can impact their own safety, impact the safety of the equipment and operation, and the safety of others. We ask them to all walk through the process and say, 'Here's what I work on, and here's how it can impact the safety of the people in the field.' The same applies to networks they support and the control systems that rely upon them."

Needs of industrial networks

Younger IT people likely find a walk through a manufacturing facility to be like a trip to a museum. Engineers used to working with the latest technologies probably find most of the equipment running a process unit quaint, but they have to understand that industrial users are seldom impressed with the newest technologies since a technology is only a means to an end. If it works, who cares how old it is?

"That's one of the biggest issues," says Perry Tobin, senior consultant for Matrix Technologies. "IT people are typically young and don't have 5 or 10 years working in a manufacturing environment and understanding the legacy issues. The IT person comes down and sees Windows 2000 machines that are deployed and will be there for two or three more years, and says, ‘Oh my, we need to get rid of that.’ But you say, ‘No, you can’t just change that machine out. There’s licensing, there are issues with Rockwell, Siemens, and some of the older software that won’t run on a new platform.’

“They’re all about upgrading, bigger, faster. IT people are not impressed with longevity. They’re appalled at how long it’s been static. It hasn’t had an upgrade, it hasn’t had updated firmware. They don’t realize that if something has been running without a reboot for seven years, don’t touch it. OT people tend to be in the same position longer.”

IT people also find themselves largely stripped of their skills and tools when they move into the plant. The techniques that they use routinely to solve problems and secure communication may simply not be available. Conway explains, “IT security people who look at a traditional plant control system, would want to engage a standard security package; switchport security, intrusion detection on the backplane of the VLANs, and SNMP rollups, for example. In many cases, the system vendors would simply say ‘You can’t do it. These switches have custom code and are built for a certain scan rate, certain throughput, and if you screw with that, we can’t ensure the availability and integrity of the controller talking through the switch to the workstation.’ This is a challenging response to IT security personnel who want to provide security defenses, but it needs to be understood and evaluated because a secure system that does not perform its functions as engineered or perform them safely, would not be desirable for anyone. There are approaches working with all stakeholders to achieve a balance.

Dealing with the unknown

When IT people have to take on a problem-solving task in the plant, they often discover many kinds of devices and communication approaches that are much different than they’re used to. Hunting for creative solutions can go in new directions if an engineer has to work with manufacturing to find ways to communicate with a system or piece of equipment to collect performance data. Kevin Price, senior product manager of Infor EAM, has seen many situations where a reliability engineer has to work with IT to extract data from an individual machine or system for performance analysis. As he describes the situation, “The reliability engineers are trying to reach a specific OEE (overall equipment effectiveness) rating. In order to do that, they need to understand how the asset is running from a quality perspective and an availability perspective.

“To do that, they need to be able to monitor it. To do that, they need a meter that can talk to that piece of equipment, whether analog, digital, or a system. All these tell, in real time or batch, the health of that asset. You have to work with IT in order to do those integrations and pull it to a system like ours. Our connection to the system, from an IT perspective, is at that integration layer. Now that we’re moving from analog to digital with some of these controls and systems, it’s becoming more open and the data more readily available. It’s more accessible to the average IT resource. But if you look at some of the systems that were installed in the 1990s, they’re proprietary, they’re analog, they’ve never been rebooted, and they’re running like a champ. The problem is the IT person can’t get any data out of it. So the reliability engineer gets frustrated because he can’t understand how that equipment could be improved because nobody knows how to talk to it.”

Developing an inferiority complex

In most situations, OT is in a weaker position in the corporate pecking order since there are typically fewer of them and they are more isolated at the device level end of the systems. Corporate IT people are better organized and connected. The corporate culture can leave OT feeling like a second banana and forced to do what those up the chain dictate.

Tobin says it doesn’t have to be that way. He suggests, “When everybody gets together and thinks long term, it definitely builds a much better relationship than if somebody says, ‘We’ve been tasked with putting a new network in the plant over the next six months, and here’s what you’re going to get.’ It’s the knowledge of OT understanding more what IT wants to do, it’s the understanding of IT knowing what OT needs, and somebody to coordinate that. There’s an education side to it. Companies that are willing to invest the time and money to bring people together to get that dialog going are the ones that are successful and don’t have a lot of animosity between the two. The right technology has to be there and it’s going to change, but the corporate culture and the communication between IT and OT are the key things to making any success between the two.”

Source:

http://www.controleng.com/single-article/it-vs-ot-bridging-the-divide/db503d6cb9af3014f532cf19b5bf75e8.html