INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

CYBERSAFE INSTRUMENTATION

In this issue:

- **Cybersafe Instrumentation**
- **AI Again**
- **Industrial Storytelling, Part 8: Getting Customers Back**

Joe Weiss, who is an OG Cybersecurity expert and a longtime pundit and gadfly, has been saying ever since I can remember that unless your instruments are cybersafe, your plant is not.

"As process sensors do not contain any cybersecurity features," Weiss noted in his blog last week, "authentication, or cyber logging capabilities, and yet are the input to all OT networks, this should be recognized as a major cybersecurity, reliability and process safety gap."

Even as long ago as the cyber-stone-age when I was editor of Control magazine and I gave Joe his blog space to begin with, it was clear he was right. It was also clear that all the manufacturers and asset owners were sticking their fingers in their ears and saying loudly, "Na, na, na!"

…all the manufacturers and asset owners were sticking their fingers in their ears and saying loudly, "Na, na, na!"

There seem to be three issues here. First, the manufacturers and asset owners don't believe Joe (and I) are right. Second, they don't understand why any attacks would come through this attack vector. Third, they don't want to incur the cost to fix the problem.

So, let's talk about the first issue. Joe and I have been saying this all along, and he has some serious proof of what he's saying. His paper**, "Challenges in Federal Facility Control System Cyber Security, Including Level 0 and 1 Devices,"** published by the National Academies of Science, points out the lack of cyber protections in field devices and final control elements. In his June 20, 2023, *Unfettered* blog post, **Critical infrastructures cannot be secured when process sensors are not secure,** Joe quotes a 2021 DOE report: "…cybersecurity threats are increasing, and sensor data delivery could be hacked as a result. How hacked sensor data affects building control performance must be understood. A typical situation could include sensor data being modified by hackers and sent to the control loops, resulting in extreme control actions."

If the process sensors, and final control elements, are not cyber secure, they cannot be 100% trusted devices. They are individual attack vectors. Ironically, the older and dumber the device, the less cyber-attack capable it is. So, your 50-year-old pressure transmitter is probably safe. Your brand new one, equipped with an IP address is probably not safe.

ISSN: 2334-0789

In addition, there is the serious presence of counterfeit devices. In 2019, Yokogawa warned their US customers about the potential presence of counterfeit devices. Yokogawa isn't the only one. I personally have seen counterfeit instruments in the field from at least four different manufacturers. Who knows what little easter eggs can be in a counterfeit HART or Fieldbus transmitter, or in a smart relay? Years ago, Schneider Electric warned that there were more Square D products being sold than they were making. I haven't heard anything to make me believe that this situation has improved.

The second issue is that manufacturers, asset owners, and even many cybersecurity workers, cannot understand why some hacker would use a field instrument or final control element as an attack vector. But look at it this way: cybersecurity is focused on the industrial and office networks, and it stops at the field devices. If you have at least one Internet-enabled field device or final control element on your plant, it is an invitation to try to invade the OT network from a place from which nobody is looking for an attack. If all your instrumentation is old and worn out, you need to think about this when you are replacing your instruments and final control elements. Would a hacker who is after cyber ransom do this? Probably not. Phishing scams seem to work just fine, and they are easier to do. So, who should we be looking at? Nation state actors, or domestic terrorists are the prime suspects. Would they? Would *we?* Of course, they would, and we have. Can such attacks happen? Yes. Have they happened? Joe Weiss says they have, and I believe he is right. There is no more time for "na, na, na!"

Can such attacks happen? Yes. Have they happened? Joe Weiss says they have, and I believe he is right. There is no more time for "na, na, na!"

The third issue is even more insidious. The asset owners and equipment and instrumentation manufacturers simply don't want to incur the cost of fixing the problem. They are depending on security by obscurity to defend their plant networks. Nobody would attack an Ethernet-enabled flow transmitter, or an Ethernet-enabled smart control valve, now, would they? Or would they? We have known since the early 1990s that security by obscurity hasn't worked in business networks, or industrial networks, so why would it suddenly start to work with field devices?

Have any manufacturers taken up the challenge of making cyber secure instrumentation and controls? I know of two. ACS, led by Phillip Hunt and Bruce Thompson, was sold to Schneider Electric. ACS made a complete line of cyber-secure intelligent transmitters. As far as I know,

ISSN: 2334-0789

Schneider has done not very much with them. (Full Disclosure: I participated in the company and in the sale to Schneider). And Bedrock Automation (also Full Disclosure: I worked as a consultant to Bedrock) tried to intensely cyber protect its PLCs even cyber protecting its power supplies. Bedrock, unfortunately, was buried by its parent company. The amazing thing was that NOBODY wanted to buy Bedrock and keep it going. Another case of "na, na, na!"

So, here's what is going to happen.

Some process plant is going to be penetrated through its device network, and something bad will happen. Maybe the plant will explode. Maybe the plant will oscillate wildly out of control. Maybe…maybe…who knows? But this isn't a time for "Nah, never happen." Because it will.

AI AGAIN

Artificial Intelligence has both good and bad sides, long before you get to *Terminator* and to Frank Herbert's "Butlerian Jihad" from *Dune.* If you don't remember that one, that's where all the AIs in the universe are massacred and it becomes illegal to make a new AI.

It seems to be mostly a matter of ethics.

The creators of the Large Language Model and ChatGPT and all the other experimental AIs seem to believe in the basic goodness of the universe, while the greedy and unscrupulous are just slavering over the idea that they can cut their staffing levels by using AIs instead of actual people. How insidious is this? As a Director of the Heinlein Society (www.heinlinesociety.org) I just finished participating in the review of the more than 700 applications we received for the 2023 Heinlein Scholarships. These are four, $4000 scholarships. One is entailed for a woman, and the other three are for any undergraduate in a STEM major in any four-year institution. That was a huge number of applications, many more than we have usually received. Unfortunately, we were forced to reject about half of them because they weren't written by the applicant—they were written by one or more of the LLM AIs such as ChatGPT.

Unfortunately, we were forced to reject about half of them because they weren't written by the applicant—they were written by one or more of the LLM AIs such as ChatGPT.

ISSN: 2334-0789

Other uses of AI are significantly more benign. Machine communications and learning algorithms are using AI to do many things that human beings cannot do easily. I point to a company like UReason, with whose Nicolas Spiegl, I wrote an article in the current issue of *Valve World.* UReason uses AI-based algorithms to predict the Remaining Useful Life of control valves, positioners, and actuators. Other companies are also working with AIs to do similar things.

Then there is the real ethical problem with the Large Language Model. They are seeding this model with language stolen from creators and writers (like me—I confess to having a dog in this fight). The Writers' Guild-West is on strike to, among other things, prevent AIs from taking writing jobs from actual writers. My union, the Authors' Guild, has gone on record as in support of the Writers' Guild and in opposition to creation-by-theft. One of the largest publishing companies in the world has announced that they are replacing thousands of authors and editors with AIs. Why? There is no way that such a use of AI will produce better writing, or more scholarly works. This is simple greed, and nothing else. Last month, I said that unless you have some special and irreplaceable skills, you will likely be replaced, in whole or in part by an AI.

Will you have something else to do? The continuing refrain of those producing "labor saving" devices like AI is that this frees humans up to do something only they can do. Okay, like what?

Perhaps *this* is why we can't have nice things.

INDUSTRIAL STORYTELLING, PART 8: GETTING CUSTOMERS BACK

Many years ago, there was a television commercial about losing a customer. The boss, shirtsleeves rolled up, calls his team in for a meeting. "Our oldest customer just called me and cancelled his account. He said we just weren't easy to do business with anymore." He went on to talk about what the company had to do to get their customers back and handed out airplane tickets to his team. He had one left, when one team member asked, where are you going? "To talk to our oldest customer and see what it would take to get him back."

I don't remember who the commercial was for, but it is still something we should think about. What do you do when you've abused your customers to the point that they leave?

ISSN: 2334-0789

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Abusing your customers is like cooking a frog. Frogs like water, and they'll cheerfully swim around a big pot while you slowly raise the temperature until they are cooked. Like your customers leaving you, the frogs eventually die.

Abusing your customers starts with trying to trim your service. Airlines are famous for making seats narrower, and seat pitches shorter. When was the last time you decided to stop doing something for your customers or make them pay extra for it? The first time, nothing happens, nor does anything happen the second or third times you take something away. Your brand will carry you, you think.

But at some point, your customers will rebel. If you are lucky, and you see what's going on, and you can convince your management to reverse course, you will be able to keep or get back the majority of your customers. If you keep pushing your brand, you will lose your customers because they no longer believe in your brand or your promises, or your products and services, or you.

Getting on airplanes to talk to your customers makes for a great commercial, but it may not get your customers back. The best way to get your customers back is not to lose them in the first place. Your customers may not always be right, but unless you understand why they don't think you are right, you might as well shoot yourself in the other foot.

WALT BOYES is a principal with Spitzer and Boyes LLC. He is a Life Fellow of the International Society of Automation, a Fellow of the Institute of Measurement and Control, a Chartered Measurement and Control Technologist, and a member of the Association of Professional Futurists. From 2003 to 2013 Walt was Editor in Chief of *Control* magazine, and from 2014 he has been Editor and Publisher of the INSIDER. From 2016 to 2022 he acted as Editor of the alternate history magazine, *The Grantville Gazette* and as Editor in Chief of *Eric Flint's Ring of Fire Press*. He recently joined Top of the World Publishing, along with Joy Ward, as SFF/AltHist Editors for their *Novus Mundi Publishing* imprint. Walt "pays it forward" as a Director of The Heinlein Society.
Walt is available for consulting and for speaking engagements both in person and online.
Contact him at waltboyes@spitzerandboyes.com or waltboyes@gmail.com , or by phone at +1-630-639-7090.

ISSN: 2334-0789