INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

The Problems of Aging in the Workforce

On November 10, my wife and business partner, Joy Ward, 65 years old, had a health incident in Portland OR, where we were attending Orycon 43, a science fiction convention. She wound up in the hospital, had (another) heart attack, an angiogram with a stent being placed, and spent a week more in the ICU and stepdown ICU. Eventually, she was allowed to come home. She is recuperating, nearly a month later. I reported our travails on LinkedIn and Facebook and received over 4000 impressions on my reports. That's more than most of my posts receive.

What this means is that people are interested, perhaps not entirely in Joy's journey, but in the way that her aging and health issues are affecting both our work. We are NOT retired! Luckily, neither Joy nor I am digging ditches for our living. We write and edit, and that is easier to do than physical labor.

I am thinking about the rest of us, automation and manufacturing workers. The median age of an automation worker is variously listed at somewhere in the mid-40s, while manufacturing workers in general are getting older too-- depending on which source you read, from 42 to 45 years old. Looking at other demographics, the average age of software developers is between 25 and 34 years old.

The median age of an automation worker is variously listed at somewhere in the mid-40s, while manufacturing workers in general are getting older too-- depending on which source you read, from 42 to 45 years old. Looking at other demographics, the average age of software developers is between 25 and 34 years old.

One of the issues this aging demographic raises include the ability to physically do the job. People in their forties and older have illnesses of aging like arthritis, damaged knees and hips, significantly poorer eyesight, and sometimes heart and weight problems that lead to diabetes and other diseases of aging. In the 1950s, the median age for manufacturing workers and automation and controls workers was in the mid- to late twenties. Young people can do jobs easily which older people simply can't. How we work is very often driven by what we can do, not by what has to be done. Older workers cost more, too, and not just in salaries. They get hurt more, and they have higher insurance rates, and they have more lost time incidents than younger workers do.

ISSN: 2334-0789

Of course, the better side to this is that the demographic provides a cadre of experienced and knowledgeable workers who understand what the job is, know how to do the job, and can be used as fonts of knowledge for younger workers as they enter the workplace. That's assuming any younger people want to enter the industrial automation and process control industry. Sometimes, uncharitable as it may be, it seems to us older people that younger workers don't really want to do the things we did or the jobs we did to get where we are.

This is probably true if you think about it. Using advanced sensors and AI-enabled software, we don't need to know all the things we learned. In fact, this may be a case of "learning what to learn" rather than learning all the things.

On the other hand, we may need to know more about the "why" of things to help us figure out when the advanced sensors and AI-enabled software may be leading us down the primrose path instead of helping us run plants and factories. You have to know what you need to know.

So it goes. My wife's illness showed me that the underpinnings of modern control systems and manufacturing may be just a little bit less robust than we think. Especially for those of us who are aging.

Cyber Attacks: We Told You So!

For many years, we have been warning that cyber attacks on infrastructure could be dangerous and deadly. We have argued about what infrastructure actually means, and whether having two of something (like a power plant) means you don't have to protect them. We have been told that there really wasn't a physical component of cyber security—until Aurora vibrated a generator apart and Stuxnet destroyed centrifuges.

Most of the cyber attacks that have gotten the attention of both the public and the authorities have been centered around the financial sector. Ransomware, denial of service attacks, phishing scams, and stealing large sums of money have been much more interesting to talk about and write about than destroying a water system, shutting off the power grid or blowing up a refinery.

Some time ago, I happened to share an elevator with a deputy Director of Homeland Security, and I told him that way back in the 1970s I had been approached by a now-defunct group of political terrorists for information on how to bring down the electrical grid in the eleven Western states. Their idea would work. I told the DDHS what the idea was, and he simply said, "For G_d's sake, don't tell anybody else!" Protection by obscurity, much? It didn't work then and it doesn't work now.

ISSN: 2334-0789

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

We have a set of standards for cybersecurity, and people keep trying to not use them. But let them lose money or oil or cryptocurrency or have the power shut off to hospitals and other important infrastructure, and stand back and wait for all the screaming and crying.

But, they say, nobody is doing any of those doomsday things. Yes, they are. Joe Weiss reported recently in a LinkedIn post and on his blog on Controlglobal.com, *"CISA's response to Iran hacking control systems in US critical infrastructures is inadequate. People keep saying, wait until there is a real control system cyber incident and then control system cyber security will be taken more seriously. Last Saturday, Iran (IRGC) cyberattacked US critical infrastructure on US soil. Dale Peterson's response on Friday was "I guess I have to include this: the Municipal Water Authority of Aliquippa serving 6615 customers had an attack on their OT. Small water utilities have weak OT and ICS security and need to be able to fall back to manual … which they did. Much more consequential is the ransomware that took out emergency room services at multiple hospitals for multiple days in Texas." Iran (IRGC) is in an undeclared cyberwar against the US and our critical infrastructures. The IRGC targeted Israeli-made Unitronics PLCs including one used in the Aliquippa cyberattack. Attacking the PLC can compromise the near- or long-term operation of the targeted systems. The attack is against the targeted PLCs, not the end-users, making this a nation-state supply chain attack against US critical infrastructure with hundreds of Unitronics PLCs in US applications and more than a thousand installed internationally. To date, none of the CISA OT guidance, including the two Unitronics Alerts, have addressed control system field device issues or device limitations. Moreover, the CISA guidance in the Alerts may not be able to be applied to many control system field devices because of PLC technical limitations. The lack of engineering expertise in preparing the Alerts is an intolerable gap that needs to be changed immediately. As can be seen by Dale Peterson's response, the lack of OT industry response to a non-OT network attack also speaks volumes.*

Iran (IRGC) is in an undeclared cyberwar against the US and our critical infrastructures. The IRGC targeted Israeli-made Unitronics PLCs including one used in the Aliquippa cyberattack.

And every time Joe or I suggest that we need to protect the field devices that have virtually no cyber protection at all, we are told that we are needlessly worried about low priority stuff. No, we are not. Aliquippa shows that this is serious. Cyber attacks? We told you so!

What appears to have happened is that for the past twenty years, state-sponsored hackers have been building a dynamically correct and topologically correct map of the infrastructure of the Western economies. When I was editor of CONTROL, I met with a scientist from Trend

ISSN: 2334-0789

Micro who had designed and built a cyber honey pot that pretended to be a very small water system in southeast Missouri in a very small town. He reported thousands of attacks after only a few hours online. This has been going on for a long time. If this sounds like the aforementioned Aliquippa incident, it should. This honeypot was set up more than a decade ago!

> For the past twenty years, state-sponsored hackers have been building a dynamically correct and topologically correct map of the infrastructure of the Western economies.

Now organizations like the Iranian Revolutionary Guard Corps (IRGC) and Chinese and Russian state-sponsored hackers have begun serious attacks. They are like being nibbled by ducks, but we've all heard the phrase "nibbled to death by ducks."

So how long is it going to take to get asset owners and governments to take this seriously? Is it going to be necessary, as Joe is suggesting, that we wait until a cyber attack is so big, so brazen, so destructive, that we can't ignore it and hope it goes away—and we have to deal with it?

We told you so!

Operating by Walking Around

One of the big differences between the way we operate manufacturing and process plants and refineries today and the way we used to do it is how we gather the information necessary to operate and control the plants.

Now, we have data coming out of our ears. Eli Goldratt called it the data haystack, in which we are supposed to find a needle. We have all the flows, all the pressures, all the levels, all the temperatures, all the outputs from the analyzers, and all the sensors that help us understand what is happening in the plant.

Fifty or sixty years ago, we didn't have all that data in a form we could use. We had our own senses. Operators and engineers relied on their own actual hearing, sight, feeling, and intuition to know what was going on in their plants.

Operators could walk around the plant and listen to the process and know if a pump was having problems, or a compressor was failing, or a valve was suffering from abnormal stiction just from the sounds. Increasing vibration could be felt over a few

ISSN: 2334-0789

hours or days' time, as could temperature excursions by feeling the outside of a pipe or vessel. The change in color of process media, and the density of steam clouds could be estimated by "calibrated eyeball."

In at least one case, I learned it was possible to tell precisely what alloy a piece of metal was…by taste. I met a recycler in Philadelphia who could tell the difference between 300 and 400 series stainless and Hastelloy. He could tell the difference between Hastelloy C and Hastelloy C 276. I watched him do it, and I checked him against an XRF alloy analyzer. He was right ten out of eleven times, and the eleventh time it was possible the machine was wrong.

I learned it was possible to tell precisely what alloy a piece of metal was…by taste.

What this tells me is that plants have a real resource in the minds and senses of their experienced engineers and operators that we have been ignoring in the rush to Big Data and the Cloud and Artificial Intelligence.

If you work in a plant or manufacturing line environment, try spending some time every day just listening to your process. It might make a huge difference in the way you do your job.

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 Vice-President 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