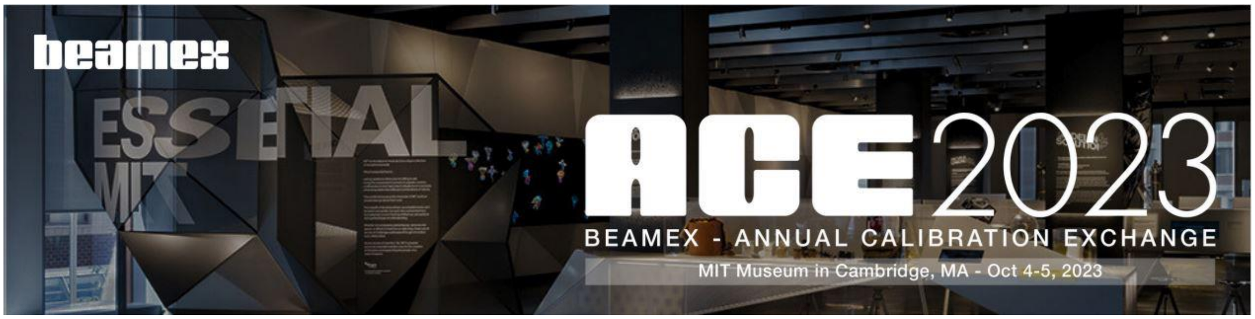
INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

BEAMEX ACE 2023- I'M KEYNOTE SPEAKER

I'm speaking again!
I'm thrilled to share that I'll be a featured speaker at the **2023 Beamex Annual Calibration Exchange –** two days full of guest speakers, industry experts, workshops, and more!
I invite you to join me and other liked-minded professionals on October 4th & 5th at the MIT Museum in Cambridge, MA to connect, exchange insights, and enhance your skill set.
View the full program here: https://resources.beamex.com/.../annual-calibration...


beamex
ESSENTIAL MIT
ACE 2023
BEAMEX - ANNUAL CALIBRATION EXCHANGE
MIT Museum in Cambridge, MA - Oct 4-5, 2023

The IT/OT Argument Again

Back in the early 2000s, when cyber security in the industrial environment became important, there was a big discussion about the differences between IT security and what we chose to call OT security.

IT security has always been around computers, networks, network appliances and other devices. The watchwords of IT security were Confidentiality, Integrity, and Availability. *In that order.* That means that the critical responsibility of IT security was to keep the data in the computers and running on the network confidential, safe from intrusion or theft, The second most critical responsibility is the integrity of the data. Tail-end is availability—the data has to be able to be accessed and used.

It was clear from the very beginning that the Operational Technology industries did not work that way in the process plant or on the manufacturing line. They could not. A typical response to a suspected cyber intrusion in an IT environment was and is to shut down the network and bring it back up piece by piece making sure that the attacker is gone and there is no malware left behind. Think for a minute what would happen if an oil refinery's control network was shut down without warning to protect the data. It would be, and has been, a huge disaster. Imagine shutting down a PLC controlling a packing plant or a car manufacturing line because the network it is connected to is potentially corrupted. You certainly can kill people by doing that.

We have many more cyber security experts who, honestly, have never been to a refinery or packing plant, or paper mill, or whatever. Many of them are part of companies designed to apply mostly IT-derived solutions to the problems of OT networks.

So, we thought that we needed to have a different acronym for the critical responsibilities of OT networks. We started to use AIC. Availability, then Integrity, then Confidentiality. Keeping industrial networks up and operational is the most important responsibility of industrial or OT cybersecurity. Keeping the data integrous is next, and, frankly, confidentiality of the data is a long third. Why? Because most of the data in an industrial network is time series data used for control. Rarely is this data extremely valuable in and of itself. It *can be* of course, so the confidentiality of the data is part of the OT Holy Trinity.

We knew that availability was king, and this caused major problems when IT engineers descended on the plants determined to use their highly developed bags of tricks on the OT networks in the plant. I am not aware that it ever came to blows, but it came close a few times. I ran a survey, back when I was editor of Control magazine asking how the relationship between IT and OT was going. The response I really remember was the OT plant engineering manager who said, "It's going great, now that I run both departments!"

So why am I bringing up this ancient discussion? It appears that the argument is raging once again. We have many more cyber security experts who, honestly, have never been to a refinery or packing plant, or paper mill, or whatever. Many of them are part of companies designed to apply mostly IT-derived solutions to the problems of OT networks.

Remember, too, that there are devices on OT networks that have no intrinsic security. Last month I wrote about the fact that data from field devices is treated as trusted, no matter what. Joe Weiss and I have been screaming ourselves hoarse since 2000 about how wrong this is. We are still screaming, and it is still wrong. These are the true "edge devices."

Then too, there is the matter of safety. IT networks rarely if ever blow things up or burn things down. In the OT network space, the acronym probably should be SAIC—Safety, Availability, Integrity, Confidentiality. But without security from the field device throughout the network and control systems, you have no safety at all.

ISSN: 2334-0789

The reason that some nation state actors, and some revolutionary terrorist organizations have not used the glaring holes in OT networks is that they are afraid it will unleash a purely physical response. But let them think they will not be nuked into a hole in the ground and you will see the level of attack ramp up.

We can dependably decide on the strength of our security responses and how well we are ensuring safety and security by the fact that 23 years after the Maroochyshire cyber attack, somebody has done it again in Northern California. We are not doing very well.

IS AI WONDERFUL?

Look, anybody can be a Luddite. It's easy to decide that if something is new it must be bad. Lots of the reaction to artificial intelligence and machine intelligence is just that—unthinking Ludditism.

So here's the point. Artificial intelligence and machine intelligence are already here. They will be used, and there will be unprecedented disruption in jobs, careers, both manufacturing and service industries, and commerce in general.

If you are a C-Level executive, you probably don't have much to worry about, but if you're filling most of the jobs in the world, you should be worried.

Robots will be able to do many physical labor jobs now being done by humans. AI will take over customer service completely, with the occasional uber-manager sitting in. Most service jobs, from slinging burgers to warehouse employees will vanish for human beings. Robots don't need breaks, nor do they need wages and benefits.

You've heard the litany already many times, including in this magazine. So I won't do a full rehearsal.

The real issue is not whether AI will be used, and how deeply it will penetrate into the culture and commerce of the world, but what will happen to people afterward.

The famous example of the "Star Trek Universe," in which there is no reason to work unless you want to is one potential outcome, but remember that it is set after a period of violent revolutions and at least one nuclear war.

No matter what, the next few years are going to be filled with disruption. Workers and other people are already exhibiting signs of what Joy Ward has called “TechnoTrauma” and they’ve been doing so for years.

If you have some ideas about how to make the near future less disruptive, post them on LinkedIn or Facebook.

I don’t know what to do about what I see in the future. If you have some ideas about how to make the near future less disruptive, please post them on LinkedIn or Facebook at @waltboyes. Otherwise, try to be kind to people.

INDUSTRIAL STORYTELLING, PART 9: TELLING THE TRUTH

A long time ago, I met a man named Jacques Werth. He was selling a strange brand of what I thought was snake oil. He was saying that *disqualifying* prospects was more important than qualifying them. That you should be willing to take no for an answer, and at the first sign of “no” you should end the call or meeting. For him, “no” meant anything other than “yes.” “I’ll think about it” meant “no.” So did “I need more information,” “I like it but it isn’t in the budget,” and all the other excuses. They all were ways the customer was saying “no” without saying it. Jacques believed in, and practiced a philosophy called “Ruthless Honesty.” He taught that if you were honest about everything with your customers, they would see you as a person of integrity. He taught that if they were saying “no” however they said it, and you didn’t keep trying to “close the deal,” they would be much more willing to deal with you when they did want something you had to sell. He called his system High Probability Selling, and it works.

He proved the system in industry verticals from car dealerships to distributorships to real estate sales firms. His acolytes (of which I consider myself one) spread the word about selling with integrity and complete honesty. And you know what? It works. It really does. You don’t have the stress of pushing where the customer doesn’t want to buy, and you don’t have the nasty bad taste in your mouth from telling stories (lying, as Jacques would say) to get the order and then explaining why you couldn’t deliver or why the specifications weren’t quite what you said.

So what would happen if your entire company only told the complete and unvarnished truth about yourselves, your company, and your products? Would sales wither and die? Would people who weren’t sure about you think again and trust you?

Specification shaving, as I call it, is endemic in many industries. For example, flow meter specifications often mis-state deliberately the accuracy of the device. There was a time a few years ago when Japanese and EU manufacturers were “spec’ed out in many bids, especially municipal bids, because they reported their specifications accurately while many US manufacturers inflated theirs. It probably didn’t matter in the applications, but it made a difference in the perception of honesty and integrity that the customers had of the vendors in question.

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.