INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Smart Field Devices Just Are Not Secure.

In this issue:

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."

It used to be an article of faith that nobody would even try to hack field devices. Flow meters, pressure sensors, control valves, level transmitters, and field analyzers were "too stupid" to be worth hacking. By that, they meant the amount of machine intelligence, memory, processor size, and all that jazz were tiny and were hard to connect into the plant from. The received wisdom ran that anybody with any hacking chops at all wouldn't waste time on hacking a field device.

And as long as field devices had tiny processors, were programmed in assembler, and were connected to the plant control system by an analog two- or four-wire (4-20 mADC) connection, they were right. That changed years ago, and apparently nobody noticed, or nobody thought deeply about what it meant.

Flow, level, pressure, temperature, and other analytical measurements are being taken outside the plant, and outside the security cordon of the traditional plant proper. And these devices have little or no cyber security built into them.

By the early 2000s, smart field devices were being made with higher powered processors, large memory stores, and digital communications capabilities. By the 2020s, many smart field devices had built in wireless (WiFi, Bluetooth, LoPan, etc.) signal capability, and either fieldbus or ethernet communications, or both. And many of these devices were being located outside the plant gates.

Places like pipelines, remote pumping stations, tankage in storage facilities all were being fitted with smart field devices. Flow, level, pressure, temperature, and other analytical measurements were being taken outside the plant, and outside the security cordon of the traditional plant proper. And these devices have little or no cyber security built into them. The old attitude continued: "Nobody would try to hack a flow meter. It has no importance and would be a waste of time."

ISSN: 2334-0789

But the old attitude was based on antiquated and faulty logic. Let's look at what actually IS available as a field device in 2023. There is a specific field device owned by one of the major field device manufacturers. It has 64 gigabites of RAM, 256 gigs of storage with battery backup, four analog inputs, one digital input, and digital outputs as HART and Ethernet. If you wanted to, it could run Windows while it measured flow. And it has almost no protection against cyber intrusion.

The thing that makes this device so critical is that it can be used as a way into the control system, and into the operating system of the plant. And nobody will ever know, until it is far too late to do anything about it, that it was used as the entry point for a cyber attack on a {insert type of plant here} either in the US proper or anywhere else in the world. We have learned nothing from Maroochyshire in 2000. But technology has rapidly increased and field devices are much smarter than they were two decades ago.

But the old attitude was based on antiquated and faulty logic. Let's look at what actually IS available as a field device in 2023. There is a specific field device owned by one of the major field device manufacturers. It has 64 gigabites of RAM, 256 gigs of storage with battery backup, four analog inputs, one digital input, and digital outputs as HART and Ethernet. If you wanted to, it could run Windows while it measured flow. And it has almost no protection against cyber intrusion.

Why are field devices so smart? There are a number of reasons. One is that engineers like to do what they can do. Another reason is that instrumentation piggybacks on other industrial design. In the old days, we had 8086 processors with maybe 8 Kb of RAM, and virtually no digital communications. Now, the inside of your favorite flow meter more resembles something you'd use for a laptop. It is cheaper to make them out of commercially available components, and so they are. As other devices get smarter and more powerful, instrumentation does too, whether it needs to or not. This is the reason why control systems migrated to Windows operating systems from proprietary ones. It just is cheaper to build them that way.

So when anybody tells you that field devices and their data are quite safe because nobody would attack through that vector, just know that the person you're talking to doesn't know what they are talking about.

And if they come back with, why hasn't it been done yet? Well, the answer is two-fold. First, how would you know if penetration had been done that way, and perhaps it is just waiting on the appropriate moment to do it. After all, we have known several cyber/physical means to bring down the electric grid in the 11 western states since the middle of the 1970s, and the only thing DHS has ever said about it is, "Well for God's sake, don't tell anybody else."

ISSN: 2334-0789

Consolidation/Deconstruction

Over the past 100 years, the automation and controls industry has been through a continuing cycle of consolidation and deconstruction. That is, companies consolidate by acquiring smaller companies and trying to injest them. Then, after a while, the same companies deconsolidate by selling off those smaller companies and laying off perfectly good employees. They keep doing this because they have no choice, even though they are rarely successful at it.

The great Clayton Christensen of Harvard explains why this cycle doesn't work. Companies look for smaller companies that have concepts and products that the larger company wants. They buy the company, and then immediately try to force the smaller company into the corporate mold. The acquisition company loses the agility and excellence they had before the acquisition. This loses the reasons the company thought their acquisition was attractive, and so they are not successful acquisitions. So, after a bit, the acquiring company divests the shell of the aquired company, and goes looking for another acquisition (read: victim).

Currently, due to a combination of founder deaths or retirements, and Covid-initiated company failures, the market for consolidation is large. Lots of companies are for sale. Unfortunately, the acquisition will have to go through the grinder Christensen described. Personally, I've been through several of these. You have to use the accounting system of your new parent. You have to use the MES system of your new parent. You have to use the engineering and change management system of your new parent. In one case I was personally involved with, it took almost two years for the acquisition to once again ship "first article." It never achieved the targets the parent company expected and was eventually sold off for basically scrap. In another case, it took four months to ship standard products because the BOMs needed to be changed to be used with the specific ERP system of the new company. Every model number and every part number in the BOMs needed to be changed.

If you are a small, agile company with some extra money, keep watching because the deacquisitions have already started.

INDUSTRIAL STORYTELLING, PART 10: Customer Relationships

Every so often I receive a contributed piece for the INSIDER. Las month I received one from a longtime acquaintance, Roger VanNuis. Roger had a long and successful career as an executive in the industrial automation space, and, along with Brian Gardner of salesprocess360.com, has been thinking deeply about how to improve relationships with customers. Mostly, Brian and Roger have been thinking about how poorly CRM does in most implementations.

ISSN: 2334-0789

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Last month we looked at how to get back lost customers. It is far better to keep them than to lose them and have to work overtime to get them back. Way cheaper too. So, let's take a fresh look at your CRM in three critical areas to improve functionality and increase overall performance. Here's Roger's take on it.

Almost everyone has invested in a CRM, but studies show less than 20% of companies believe they are getting an acceptable ROI out of CRM. Getting ROI from CRM is about process, not just technology. Most companies have processes and visibility at the back end of the sales cycle for order processing, inventory tracking and more. However, most lack the processes and visibility for the front-end, sales-generating portion of their businesses, which is critical for growth. Common mistakes can be avoided through experience and up-front planning. General mistakes include:

- The CRM project is led by IT as a software project. This leads to a lack of support and input from sales and other key stakeholders.
- Technical teams do not understand Sales requirements. Team selling is not facilitated.
- Taxonomy is not properly designed-in up front to ensure future integration with ERP.
- Custom Objects limit expansion and upgrading.
- Onboarding and training are limited and not offered by role.
- Training / coaching is too technical and How-To's are often complex.
- Documentation lacks a custom playbook for continuity.
- Standardized dashboards tend to underdeliver value.

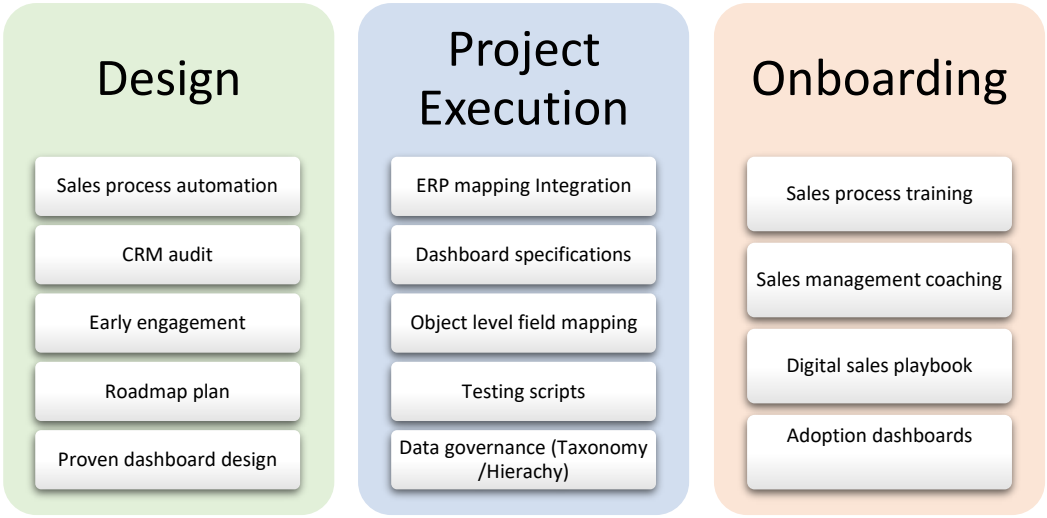
Using proven methodologies, processes, and tools companies can avoid these pitfalls by concentrating on three competencies: Design, Project Execution, and Onboarding.
Getting the design right upfront is critical to achieving your business objectives with a CRM implementation. Therefore, begin with a detailed CRM Audit focused on sales process automation and optimization. Interview each stakeholder to capture the methodologies and processes they are accountable to today and the ones they may follow in the future. Processes are baselined and performance gaps are documented. Functional dashboards are specified to capture KPI and any other critical benchmark data. The data collected presents a cost benefit analysis that concludes with a well-documented road map

ISSN: 2334-0789

including a logical phased in plan for complete and easy adoption.

Most businesses lack the necessary skillset in-house to bridge the core groups. CRM implementation teams try to function effectively as an Architect while implementing a CRM platform. It is important to use the output of the audit, to engineer a working framework for dashboards and other necessary KPI collection points. This is critical to data parsing for the business hierarchy accommodating all entities like PCAT, BU's, division, and major accounts, parent/child relationships, team selling groups, etc. At this point testing scripts are executed proving connections and functionality between CPQ quotation systems and other bolt-ons with the ERP.

With most CRM, implementations and adoption rates for outside salespeople are extremely low. Onboard training is product focused, generic, and not specific to their role. Successful training and onboarding focus on teaching new behaviors and building modern habits that salespeople and management should adopt to make CRM a useful tool. Coaching services focus on modern in-field habits to leverage mobile tools, dashboards, KPI's and other performance metrics for continuous improvement. High-fidelity digital playbooks by role featuring a day in the life scenarios, FAQs, and How To training are all created.



Roger can be reached at roger.vannuis@salesprocess360.com

ISSN: 2334-0789

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

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