INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Your key to the latest industrial automation and process control information

VOLUME 22
NUMBER 1
ISSN2334-0789
January 2018

Inside this issue:

Special Report Issue!

The Future of Automation in the Age of the Internet of Things

The Future of Automation in the Age of the Industrial Internet of Things
By Walt Boyes

A PERFECT STORM IS COMING

We are experiencing a perfect storm in manufacturing and automation. There are so may inflection trends nearing the tipping point that it is possible for several of them to give at once, causing a cascade of new technologies, new uses, and new opportunities. Along with, of course, new challenges, new fears, and new complexities.

The next five to ten years will bring huge changes to process, discrete and energy industries and automating them across the entire value chain. These will include changes in demographics, changes in social interaction, changes in sensors, analysis and control technology, changes in the architecture and use of control systems themselves, changes in work practices and preferences, and changes in the way plants are designed, built, controlled, operated and maintained. Some of these changes will be driven by demographics, some by increasing security concerns, and some by the globalization of the industries that use automation.

THE WORKFORCE IS CHANGING

The automation workforce is going through the greatest change in its history. The generation that helped to build the majority of the existing process plants, and run them, is retiring or has already retired. This is the generation that absorbed their situational awareness by operating the plant manually, or with minimal control. In contrast, the incoming generation of engineers and operators has no such wide-angle view of the plant. They've never operated the plant in manual mode, and they never will, because it is no longer possible to run plants in manual. This is also equally true for factory automation operations. Just try building a car using manual means.

So, the new generation has been limited in their view of the plant to what is being shown on the control room screens. They are unlikely to be able to tell what is wrong with the plant, or what is right, by observation. They require readouts and alarms to tell them what is wrong. They use the tools, but they don't always understand them. This new generation of operators and engineers want to be taught differently, and to work differently. They see the use of mouse-keyboard-display technology as mostly limiting. They want to be able to use mobile devices, and they want to learn by doing, rather than being taught step-by-step and mentored.

The Future of Automation... (continued)

The software and capabilities of the basic process control system will undergo radical changes. The software will have more in-built intelligence and be able to run the plant in steady state with almost no intervention from the operator. The software should be able to automatically go to pre-set failure states, and recover from them, once the conditions of failure have changed, without much intervention from the operator. Loop tuning will be automatic and only need intervention when the loop cannot be tuned. Diagnostics and maintenance requests will be automatic, and not require to be initiated from the operator station.

Industrial automation systems will move to integrated, intelligent model based solutions integrated with the control platform. The model becomes the integration mechanism as well as the application server.

Safety systems and Safety Instrumented Systems will also have significant native intelligence, and will be able to put the plant into pre-programmed failure states and recover from them. The safety system will initiate its own diagnostics and maintenance requests without intervention from the operators. Safety Instrumented Systems will also be required to have in-built and inherent security to prevent the type of malware attacks that have recently been used against Triconex systems in the Middle East.

The combination of new sensors, more sensors, higher computing power and the concept of Big Data and its associated analytics will permit much better use of APC software in real time, and may even permit the use of business data to operate the plant directly.

The trend toward much higher computing power in the sensor and transmitter and in the final control element will permit true distributed control for the first time. As digital plant networks like Foundation fieldbus and Profibus/Profinet proliferate, even in brownfield plants, the system architecture of a process DCS will begin to look more like a SCADA system, and less like “big iron” in the control room. Local control in the field will become commonplace, with the ability to override from the control room as needed. Because the operator interface will be both stationary and increasingly mobile, the concept of the control room as nerve center will become obsolete.

Software will be considerably more collaborative, and permit business variables to be used in the control of the process. The concept of open, secure automation will be key to the future of automation.

The concept of the “Automation App Store,” pioneered by Inductive Automation, and the modular building block concept of software design will significantly change the way asset owners see and use control software. A control system will be made up of the software required for operation, like interlocking “Legos” that are added in or removed as necessary, and the hardware necessary to run it.

As we have noted previously, the new generation of engineers and operators wants more mobile HMI applications, for smartphones, for tablets, for laptops and for new devices such as the augmented reality replacements for the failed Google Glass™. HMI will move past the EEMUA and ASM Consortium designs and will become intelligent and role based. HMIs will deliver the required information and visual representations to the operator or engineer depending on who is looking at the data, and whether the information is required. HMIs will be capable of deciding what information should be presented to the operator for the operator to make decisions. As operators become more mobile and are not tied to the control room, HMI design will change to adapt to mobile visualization platforms. This will be more than just making the standard graphics small or large.

Part of this trend in HMIs will be a decoupling of the HMI itself from the control system. HMIs that are application based and not necessarily produced by the company that designed the control system are currently being discussed, and implemented. Formerly common in SCADA systems, this will be a feature of all control system architectures.

Alarm management will change drastically, as it becomes a standard part of a procedure-controlled automation system. Alarms will become more like notifications and less like demands for operator intervention.

As high definition three-dimensional simulation becomes affordable, training of new generation operators will become more like participating in a video game. Operators can walk through the process plant, still being in charge of the plant, and make notifications and changes while doing so. This may lead to a completely new type of HMI where the operator is immersed in the HMI rather than just looking at it.

The Future of Automation... (continued)

There are not enough people in the workforce, or who will be entering the workforce, for the traditional automation operations to function. Operators and engineers will perforce be required to operate many more functions, and even many more lines or plants than has ever been required of them before, because the lack of trained people has become acute. This is true all over the globe. There are automation engineering and operations jobs going begging in China and India, for lack of trained workers.

THE ARCHITECTURE OF CONTROL SYSTEMS

Control systems will have to be able to compensate for the lack of trained operators by being smarter. AI control systems are not too far off. This means significant changes in the way control systems are architected, from the ground up.

The typical Purdue model of the process plant is flattening, and will become a two-layer model: the plant layer and the enterprise layer. Some industries will have a cloud-based layer between the plant and the enterprise.

Sensors, analyzers and transmitters will become a more significant element of automation as the Industrial Internet of Things becomes an actuality. We will need to measure many more physical properties, compositions and conditions of plant assets. This is only two or three design cycles away, and is a design imperative. New sensor technologies and new sensor designs, influenced by MEMS, Lasers and nanotechnology, will make these simpler, cheaper sensors possible.

Sensors and transmitters will become field controllers in themselves, and will be capable of datalogging, and historicizing, as well as providing diagnostics and calibration for themselves. It is now possible to make a relatively simple sensor with 64 Gigabytes of memory. That is enough memory to store once-per-second readings for the estimated life of the sensor and beyond.

Sensors will be designed that can be linked into large sensor arrays, providing higher accuracy and repeatability than a single sensor and transmitter can today.

Safety instrumented systems will benefit from better sensor technology and sensor cost, as well as better diagnostics. The concept of “soft sensors” will continue to grow, and make possible more control from virtual measurements. Sensors will no longer be linked by analog output. Sensors will increasingly become fully digital, either wired, or more commonly wireless. Analyzers will become simpler, and more field capable. They will divide into “laboratory analysis” and “online analysis.” The concept of “at line” analysis will disappear.

Whatever the hype and perceived value of the Industrial Internet of Things, the use of orders of magnitude more sensors and the use of data analysis tools (Big Data… ubiquitous data from many sources) will change the way control systems are architected.

Virtualization has become ubiquitous in the process industries in just a few years. It will become the norm. This will make it easier for asset owners to continue to run obsolete and outdated software, so vendors will have to make upgrading to new software compelling and of significant added value. The one compelling and value-added feature that will be required is security.

The large number of sensors, and the huge amount of data they will produce, will necessitate storage of the data in, first, private cloud servers on the plant site, and then more public clouds such as Microsoft’s or IBM’s. Data not immediately necessary to run the plant will be cloud stored until needed. Cloud storage demands redundant networks both on the plant and in the server farm. Cloud storage also requires bullet-proof security, in the cloud, and during data transfers into and out of cloud storage.

Control systems will need to become much more automated. Operators with limited situational awareness and limited experience will become more common in the next five to ten years. The importance of ISA 106 and procedure-controlled automation for both batch and continuous processes cannot be overstated. Control systems will need to be stateful, and have failure states with recovery modes as standard practice. Insurance companies may well insist on this before writing policies that cover loss-of-business due to accident.

The hardware of the basic process control system in five years will be redundant systems stored on blade servers, with display architectures ranging from huge flat or curved screen LCD/LED displays to mobile phone and tablet displays, and augmented reality capabilities.

The Future of Automation... (continued)

It is clear that eventually all the field device networks will become Ethernet using IPv6 addressing, so that every device in the plant will have its own IP address. This simplification of plant networking will also make it easier for data to travel from the device level to the enterprise level in real time, without being collected in an historian and sent to a transaction-based ERP system.

Eventually, even wireless field networks will be subsumed to the IEEE802.11s standard, and its successors. With each device having its own IP address, having a specific wireless network will be duplicative and unnecessary. And with the massive increase of wireless sensors and transmitters predicted by the use of Big Data, having a single, standardized wired/wireless communication protocol will become imperative.

WiFi as it is currently constituted is not optimum for the level of sensors and data to be carried in a plant. New capabilities for systems and backhauls will need to be developed so that the data flows aren't choked or limited at the plant level.

These data flows will need to connect both to the control system and to the enterprise, especially if business variables are used for control in the field. Connectivity technologies like OPC and OPC-UA will be treated like electrical receptacles—nobody thinks about them, they just plug devices into them and get power and information.

FIELD DEVICES AND CONTROL SYSTEMS MUST BE INHERENTLY SECURE

The Industrial Internet of Things haS brought cyber security in industrial control systems to the forefront. Control systems must be designed to be inherently secure, with defense in depth and other techniques from the ISA99 playbook. But even more importantly, the hardware on which the control system exists and operates must also be inherently open and secure, by design.

While it is true that control system security is only partly based on hardware and software, the control system should have substantial error trapping to warn against "social engineering" like putting an unknown USB stick into the control system processor. Most cyber training currently is on the IT level, and Network Security based. Security of edge devices and field controllers must be assured. Sensors must be inherently secure, their connection to field controllers or gateways must also be inherently secure. The controllers and gateways, such as those produced by Bedrock Automation, must be designed *ab initio* to be both safe and secure, instead of having safety and security stuck on later.

Within the next five years, this must change so that Industrial Control System security is its own discipline, and has the budget and tools to operate successfully in the modern environment. The architecture of control systems must change to include security devices and software that emphasizes security, but not at the expense of control capability.

NEW METHODS OF DISTRIBUTING AND INTEGRATING CONTROL SYSTEMS

Within the next five years, we will see a growing concentration on field services and professional service offerings by vendors to asset owners. Asset owners and vendors alike are faced with the inability to hire enough trained capable workers to operate and maintain plants. Asset owners have already decided that they would prefer to hire vendors to help them with these tasks. Remote optimization and maintenance will be followed by remote operation and management services, to the extent that a vendor can find the trained and capable workers to accomplish these services. It will be difficult for both asset owners and Vendors, and may require a considerably higher expenditure on training by both parties. This is dependent, of course, on the level of security the vendor can provide for both hardware and software that is being managed remotely by the vendor.

We will see an even larger emphasis on the MAC/MIC/MEC (Main Automation Contractor/Main Instrumentation Contractor/Main Electrical Contractor) concept as Asset Owners lose their last remaining in-house engineers with the capability to design and manage construction and modernization or upgrade projects. Only the very largest of the supermajors will continue to have in-house project management capability. Even EPC companies will want to use a MAC, MEC or a MIC in combination with their own overall project management. Some EPC companies may elect to ally with forward thinking and state of the art controls companies, as well as forward thinking system integrators. An example of this is Bedrock Automation's recent partnership

The Future of Automation... (continued)

with Jacobs Engineering.

System integrators will continue to grow, and will provide competition for MAC/MIC/MEC projects with the automation system vendors themselves. System integrators will also need to make alliances with vendors such as Inductive Automation, whose system integrator corps has been co-opted by the vendor into producing apps and templates for the Ignition! software system; vendors such as Bedrock Automation, which has made alliances with Inductive Automation and other vendors to more effectively acquire new system integrator partners.

THE INDUSTRIAL INTERNET OF THINGS

The Internet of Things (IoT) is past the height of its hype cycle, along with its associated buzz word, Big Data. It is instructive to look at the hype, and see how IoT will be used outside of manufacturing, and what issues and problems will be seen in the general use area, and then relate those applications, issues and problems to an *Industrial* Internet of Things, which will be quite different and have different applications than the general Internet of Things may have.

The Internet of Things was originally called M2M (Machine to Machine), now M2M is considered a core part of the IoT. However, the number of sensors and other nodes that will have to be connected together to form an Internet of Things, or an Internet of Everything is so large that it will require wholesale adoption of IPv6 (Internet Protocol version 6). To date, IPv4 stubbornly continues to be the protocol version in use, even though there are no new IP addresses. A variety of workarounds have been established to make it possible to continue to use IPv4.

In order to produce the IIoT devices, the same trends that have been discussed in this paper will apply: very low power radio networks, very inexpensive "lick and stick" sensors, and intelligent final control elements. The sheer numbers of these devices required for the IoT will feed back into the design and availability of these sensors for the Industrial Internet of Things, exactly the same way as advances in design and economies of scale for automotive sensors have reduced prices for many devices used outside of the automotive environment.

The Industrial Internet of Things, working with Smart Manufacturing systems, will be able to produce a revolution in the way manufacturing is done, especially in discrete manufacturing and batch processing, but also effect a considerable change in process manufacturing as well. Based on the way the Internet of Things is designed, an "app-based" design approach may well produce the agile, limber process environment and process control systems that have been called for in the past ten to fifteen years.

The aggregation of sensors and data in the Industrial Internet of Things will first be able to revolutionize the process control lifecycle. Completely automating maintenance work orders, diagnostics and calibration will be among the first major effects of the IIoT. Connecting to vendor purchase networks automatically, for replacement and repair will be another major effect. This will permit maintenance and operations personnel to concentrate on causing the control system to work in an optimized fashion, and not spend time collecting and aggregating data and inputting data into dissimilar systems.

Using RFID and other identification technologies, inventory can be made entirely automatic. Delivery of raw or intermediate materials using robot-guided vehicles can also be made practical and will improve time to market and agility. RFID technologies can also be used to improve worker and asset safety, by providing location services both of personnel and critical assets such as fire trucks and safety gear. Integrating and automating the supply chain will provide another layer of inherent security for control systems and will finally reduce the huge amount of counterfeiting that happens now.

The IIoT will also affect how simulation and modeling can interact with the real-time process. Models can be much more detailed, with the huge amounts of data available from the IIoT, and simulation can be morphed into ways to meta-control the process in real time.

AND YET MORE SECURITY!

Increasing drastically the number of sensor and controller nodes on a control system network and extending the network beyond the physical boundaries of the plant to include suppliers and supply chain networks, increases the potential for threat to the system in a topologically complex way. Increasing the number of sensors and controllers, as well as other network nodes, increases the threat surface available to

The Future of Automation... (continued)

invaders of the system. It also opens the network and the control system to physical and cyber-physical attack, not just cyber-attack.

The control systems of today cannot be made safe with the number of sensors and controllers and the limited complexity of industrial networks currently in existence or in design. In order to operate safely within the Industrial Internet of Things, control systems and industrial networks must be re-designed from the beginning to enhance safety and security and prevent both accident and cyber-intrusion. This will require an entirely new class of control system, and Bedrock Automation has made an excellent start with security built in from the power supply and the backplane to the operating modules of the controller. In fact, Bedrock's Black Fabric backplane also prevents cyber-physical attack by being immune to pin-sniffing—because the backplane has no pins.

What Will the IoT and IIoT Mean for Vendors?

The implications of the Internet of Things, Big Data, and the Industrial Internet of Things are enormous. They will create a completely different vision of control systems and how to control process plants based on the amount of data and the availability of data, and the ability to mine and refine that data into usable information.

The theory of Big Data brings to process control and manufacturing not only the concept of complex systems, but the complex systems themselves in practice.

The IIoT will make the entire sensor network, including final control elements, and the safety instrumented system, and the control system into a single complex system. Adding to the complexity will be the integral interconnections to the supply chain, and to the enterprise. This will especially be true if, as is predicted, it will become commonplace for the business systems, and especially the supply chain, to be seamlessly connected to the control systems.

This clearly has implications for the design and operation of plant control systems. Control systems have always been somewhat isolated from the business systems of the plant, as the Purdue model and its many variants have shown. The Industrial Internet of Things will force the control system to be a part of a "network of networks," and be capable of interfacing easily and in an agile manner, with all the other networks that surround it in the business enterprise, however large.

The automation system vendors, as some like Bedrock Automation already have, must embrace the IIoT by whatever name the vendor wants to call it. The vendor must also embrace the theory of Smart Manufacturing, again, by whichever of the many names currently in use the vendor prefers to use.

The IIoT will finally do for sensors and networking what the PC did for control systems. The introduction of the PC produced a COTS (Commercial Off the Shelf Systems) platform onto which the control system software could run. IIoT will provide the COTS sensors and networks that will be usable with no or minor modification in the industrial environment. The reason for this is that the sensors and networks will have to be more robust, not less, than the current technologies for sensors and sensor networks because they will be used in electric grid, building automation, and home automation systems where the level of training and support will be significantly lower than the standard in process automation.

IT CAME FROM OUTSIDE

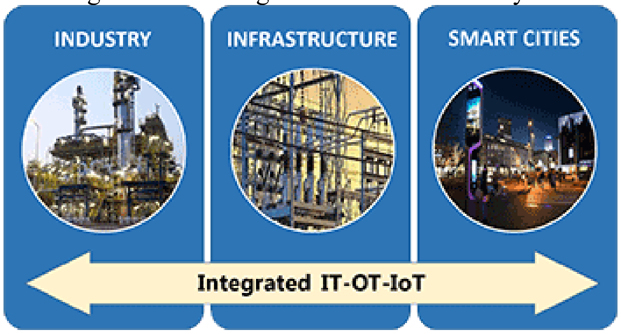
One of the significant trends making up this perfect storm is the continuing insertion of companies, competition, and concepts from entirely outside the mainstream automation vendors. This has been going on for some time. The use of Windows completely destabilized the hardware based DCS market in the 1980s. The use of virtual machines made possible the use of antiquated control systems, and the instantaneous backup and switchover of control systems in the event of disaster or accident. The use of Cisco's invention of managed Ethernet switches made possible the deltaV DCS and all of its clones. The use of Silicon Valley-designed dedicated chipsets has made, and will continue to make, sensors drop in price while increasing in performance and durability. Companies like Bedrock Automation (Silicon Valley), Inductive Automation's Ignition! products, and SEEQ (Microsoft), with roots outside the standard automation vendor space are the tip of the spear, as companies and inventors move from other areas, such as medical instrumentation, network instrumentation, and aerospace instrumentation and controls.

The ARC Orlando Forum Is Coming!

Presenting the 22nd Annual ARC Industry Forum: Digitizing and Securing Industry, Infrastructure, and Cities

February 12-15, 2018 - Orlando, Florida

It's happening fast. Everywhere we turn, things and processes are becoming more connected and intelligent. Streetlights, cars, gas turbines, and thermostats stream data. Buildings, refineries, oil platforms, mines, and wind turbines are optimizing asset and operating performance. Parking meters and distributed power grids deliver value to both consumers and operators. Design software can link to additive machines to print parts directly. And it's only the beginning.



Challenges continue to grow for the industrial cybersecurity community. Broader deployment of operational technology is expanding the use cases requiring protection. Resource shortages are undermining the effectiveness of established defenses. Blurring boundaries between IT, OT, and IoT are increasing the need for more integrated, collaborative cybersecurity strategies.

How will disruptive technologies change existing products, plants, and cities? Can cybersecurity threats be overcome? When will machine learning and artificial intelligence transform operations? Will open source solutions impact traditional software and automation domains? How will a digitally-enhanced workforce stem the loss of tribal knowledge? How do connected products create opportunities in aftermarket services? What steps can organizations take to foster innovative thinking?

There are countless ways to conduct your digital transformation journey, too many technologies and suppliers to evaluate, and endless choices to make along the way. Embedded systems, networks, software platforms, augmented reality, and machine learning may play a role as you begin to improve uptime, optimize operating performance, enhance service, and re-think business models.

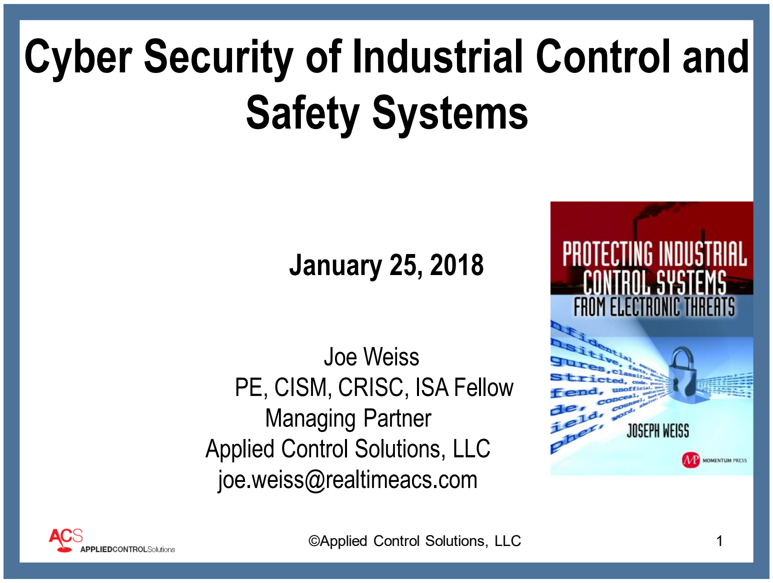
Join us at the 22nd Annual ARC Industry Forum in Orlando, Florida to learn more about how digitizing factories, cities, and infrastructure will benefit technology end users and suppliers alike. Discover what your peers are doing today and what steps they are taking in their respective journeys.

For more information, or to register, visit:

https://www.arcweb.com/events/arc-industry-forum-orlando

Joe Weiss Keynotes TAMU Instrumentation Symposium 2018

[Editor's Note: Many years ago, I arranged for Joe Weiss to become the "Unfettered" blogger at Controlglobal.com. I am excited to report that Joe has given me permission to print the keynote speech he gave on January 25 at the Texas A&M Instrumentation Symposium in College Station, Texas. We welcome Joe to these pages!]



Cyber Security of Industrial Control and Safety Systems

January 25, 2018

Joe Weiss
PE, CISM, CRISC, ISA Fellow
Managing Partner
Applied Control Solutions, LLC
joe.weiss@realtimeacs.com

ACS APPLIEDCONTROLSolutions

©Applied Control Solutions, LLC

1

PROTECTING INDUSTRIAL
CONTROL SYSTEMS
FROM ELECTRONIC THREATS
JOSEPH WEISS
MOMENTUM PRESS

Welcome and thank you for the opportunity to address a very important but not well-understood issue - cyber security of industrial control and safety systems from the perspective of an instrumentation and control system engineer.
The title of my book provides a good summary of the issues: Protecting Industrial Control Systems from Electronic Threats [Figure 1].

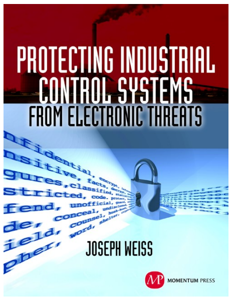


Figure 1 Protecting Industrial Control Systems from Electronic Threats

The term "Protecting" is used rather than the term "Hacking" because it is not that difficult to hack control systems but it is "rocket science" to protect them. This is due to the trade-off between reliability, and security where reliability MUST win. The term "Industrial Control Systems" is used because control systems are more than just SCADA or DCS but encompass a wide range of industrial automation including Remote Terminal Units, Programmable Logic Controllers (PLCs), sensors, actuators, drives, analyzers, Intelligent Electronic Devices, etc. Finally, the term "Electronic Threats" is used instead of "hacking" because past incidents include non-malware cyber induced events. For example, a Navy destroyer performing radar testing off the coast of San Diego inadvertently impacted SCADA Systems of San Diego Gas and Electric and the San Diego Water Authority. Another Naval radar testing incident in the Netherlands caused a pipeline to rupture. Consequently, Electromagnetic and Radio Frequency Interference are also cyber considerations in addition to malware.

Industrial control systems consist of process sensors connected to controllers, actuators, and HMI's (effectively the control system network). The sensors and actuators operate almost exclusively in near real-time (micro-seconds to milliseconds) whereas the HMI provides an operator information on the order of seconds to minutes. The sensors and actuators can operate, and in most cases were designed to function, without the IP network.

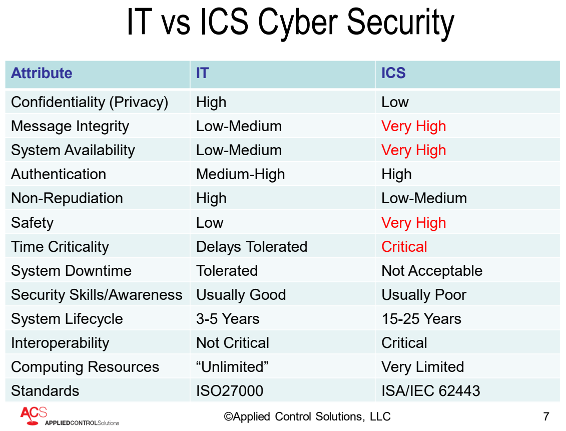
The unofficial IT definition of a cyber incident is the system is connected to the Internet, is using Windows, and the attacker is maliciously compromising the data. Effectively this is Information Assurance. This also implies that all cyber vulnerabilities are important and need to be expeditiously addressed regardless of process system impact. However, the most important factors for plant operations are (1) reliability, and (2) safety. The NIST definition of a cyber incident in FIPS PUB 200 is: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies". This definition is more relevant to the ICS community with one critical modification. The definition needs to add the letter S (Safety). It is also important to note that the term "malicious" is not mentioned in the NIST definition. Effec-

Joe Weiss Keynotes TAMU Instrumentation Symposium 2018 (continued)

tively, this is Mission Assurance which means cyber vulnerabilities are only important if they can impact the mission. The additional reason for not using the term malicious is the lack of adequate ICS cyber forensics as well as lack of sufficient ICS cyber security technologies. In many cases the only difference between an incident being malicious versus unintentional is the motivation of the individual involved. An example of this event was the cyber impact at a bottling facility (Figure 2).

Figure 2 Bottling Plant Cyber Incident

The plant engineer thought the company's bottling systems were secured until someone with access logged in and "inadvertently" changed a timer for a maintenance device on a filler. It was supposed to squirt grease into the bearing every 20 minutes and it was changed to once every eight hours. The bearing soon froze. The line that fills 1,200 bottles per minute ground to a halt. The damage created a $100,000 loss. According to plant management, "With well-intentioned engineers monkeying around in the automation system, who needs terrorists or disgruntled employees?" Or was it? Why would a knowledgeable insider make such a major change without knowing the potential impacts?



IT vs ICS Cyber Security

Attribute	IT	ICS
Confidentiality (Privacy)	High	Low
Message Integrity	Low-Medium	Very High
System Availability	Low-Medium	Very High
Authentication	Medium-High	High
Non-Repudiation	High	Low-Medium
Safety	Low	Very High
Time Criticality	Delays Tolerated	Critical
System Downtime	Tolerated	Not Acceptable
Security Skills/Awareness	Usually Good	Usually Poor
System Lifecycle	3-5 Years	15-25 Years
Interoperability	Not Critical	Critical
Computing Resources	"Unlimited"	Very Limited
Standards	ISO27000	ISA/IEC 62443

ACS APPLIEDCONTROLSolutions ©Applied Control Solutions, LLC 7

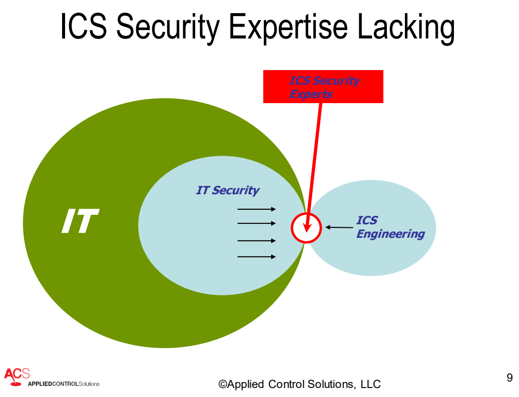
Figure 3. Differences Between IT and ICS

The IT idea of prevention may not be adequate for the ICS environment and consequently, resilience and recovery become very important. An interesting adjunct is the concept of a Cyber Pearl Harbor. Will there be one? Possibly. However, because of the lack of ICS cyber forensics and adequate training, we may not know it is cyber-related.

There are many differences between IT cyber security and ICS cyber security including the basic premise of each. IT is focused on detecting vulnerabilities, generally new, in the network regardless of process system impact. Operations (and safety) focus on what can happen to the process and ask if cyber can cause that problem regardless of the sophistication of the cyber threat (Figure 3).

The recent computer chip cyber security vulnerabilities – Meltdown and Spectre – demonstrate the issues of computing resources. Several vendors have published advisories to inform customers they are assessing the impact of the Meltdown and Spectre exploits. The list includes Siemens, Schneider Electric, ABB, Rockwell Automation, and medical technology company Becton Dickinson (BD). ICS-CERT published an advisory directing users to the advisories of their vendors.

There is a lack of technically capable ICS cyber security experts. The staffing issue needs to start at the community college and university level and move to industry (Figure 4).



ICS Security Expertise Lacking

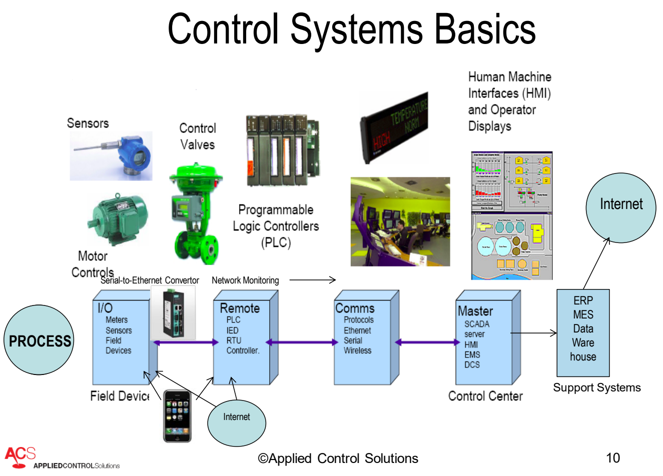
ACS APPLIEDCONTROLSolutions ©Applied Control Solutions, LLC 9

Figure 4. Lack of ICS Cyber Security Expertise

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

That is, both educational domains should be required to take a course that covers the “Principles of Security” and “Principles of Engineering” that overlay application to various domains (e.g. IT and OT). This is not to make students in either discipline experts in the other discipline but to understand there are differences that need to be considered. At the industry level, there is a need to have IT security and Operations share key performance indicators. That is, IT security needs to have some metrics tied to Plant Operations (reliability and safety) and Operations have metrics tied to cyber impacts affecting plant operations. The imperative is that the two organizations (IT and Engineering) have an ongoing cooperative relationship.

Cyber security has traditionally focused on computer-related vulnerabilities (e.g. Windows and Linux platforms) in networked systems. As can be seen from the following slide, as you move from right to left, there is less security but higher physical impacts (Figure 5).


Control Systems Basics

©Applied Control Solutions 10

Figure 5. Control System basics

In fact, the far-left devices (Level 0,1 in the Purdue Reference Model) have not even been considered for cyber security. Yet these are the devices that directly affect process reliability and safety. As a result of Level 0,1 security, in December 2017 the ISA99 standards committee established a new working group to focus on the security of Level 0,1 devices.

Control systems have always been designed to address known threats including environmental, temperature, load, etc. The only threat not previously considered is cyber. Consequently, cyber needs to be addressed in the context of process risk. Risk is defined as Frequency (F) x Consequence (C) where F is based on mean-time between failures (MBTF) and C is based on…(to be defined). In many cases, vendors installed backdoors in the control system devices to obtain the MBTF data. Many of these backdoors still exist. As far as C is concerned, if an attacker takes control of a system, what can be the consequence? The real question is can a cyber event exceed the design basis. Risk can be reduced by mitigation … if it works. Other traditional aspects for estimating risk such probabilistic risk assessments don’t work as they cannot account for malicious events. ICS cyber risk can be temporal and potentially universal. Stuxnet is a good example. Prior to Stuxnet, the probability of changing controller logic without the operator being aware and then modifying operator displays to camouflage the logic change would have had a very low probability. Additionally, considering this type of attack as being universal and applicable to any industry using the particular vendor’s products would not have been conceivable or at least had a very low probability. However, after the publicity surrounding Stuxnet, the probability of another similar event would have a much higher probability. That is, the risk equation of FxC went from very low to high. Another unique aspect of ICS cyber risk is that it can have an organizational (damage to an individual facility) as well as societal risk (damaged facility impacting the public)

Unfortunately, there is a lack of imagination by the “good guys” that the “bad guys” don’t share. If the event is taken out of context, the security implications are too often ignored.

The March 2007 Aurora test at the Idaho National Laboratory (INL) is an example (Figure 6).

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

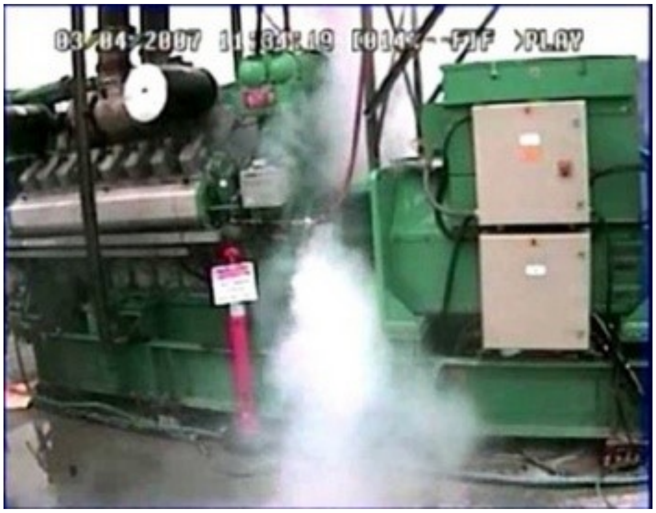
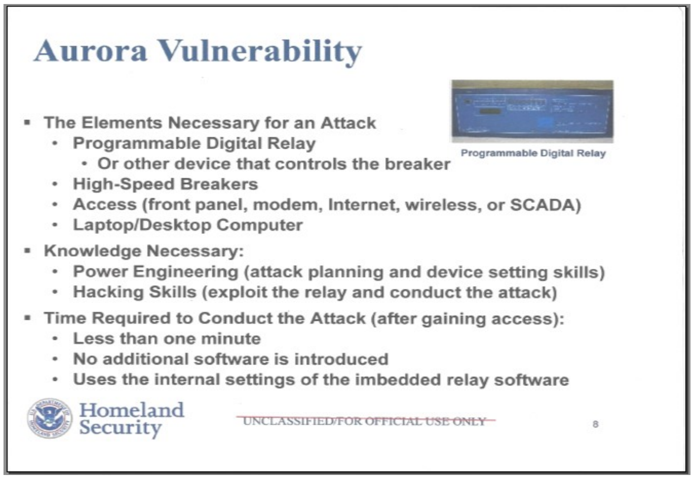


Figure 6 INL Aurora Test

The Aurora vulnerability is based on a vulnerability that electrical engineers are taught – don't restart Alternating Current (AC) equipment out-of-phase with the grid or the generated torque will damage the equipment. The Aurora vulnerability is simply remotely opening breakers and then reclosing them out-of-phase with the grid and letting the torque of the grid cause the damage – no malware involved (Figure 7).



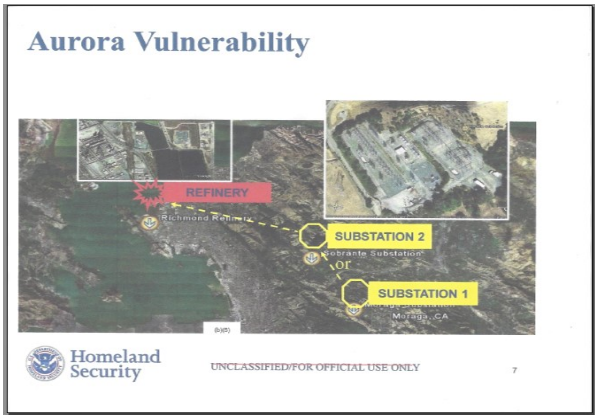
Aurora Vulnerability

- The Elements Necessary for an Attack
  - Programmable Digital Relay
    - Or other device that controls the breaker
  - High-Speed Breakers
  - Access (front panel, modem, Internet, wireless, or SCADA)
  - Laptop/Desktop Computer
- Knowledge Necessary:
  - Power Engineering (attack planning and device setting skills)
  - Hacking Skills (exploit the relay and conduct the attack)
- Time Required to Conduct the Attack (after gaining access):
  - Less than one minute
  - No additional software is introduced
  - Uses the internal settings of the imbedded relay software

Homeland Security ~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~ 8

Figure 7 Aurora Vulnerability

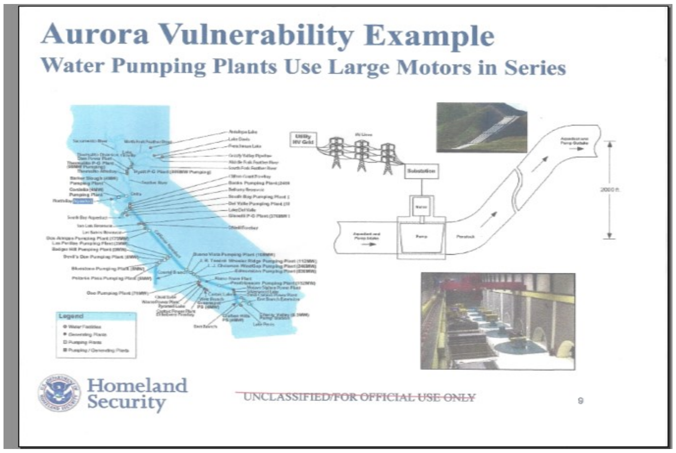
This is a gap in protection of the electric grid as the torque occurs in milliseconds – too fast for any ordinary breaker to respond and damaging all AC equipment and transformers connected to that substation. This vulnerability is very disconcerting because it uses the protection as the vulnerability initiation and it affects all equipment connected to the affected substation (Figures 8, 9, 10)



Aurora Vulnerability

Homeland Security ~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~ 7

Figure 8 Aurora Vulnerability Affecting Refinery (oil/ gas/chemical) Facilities



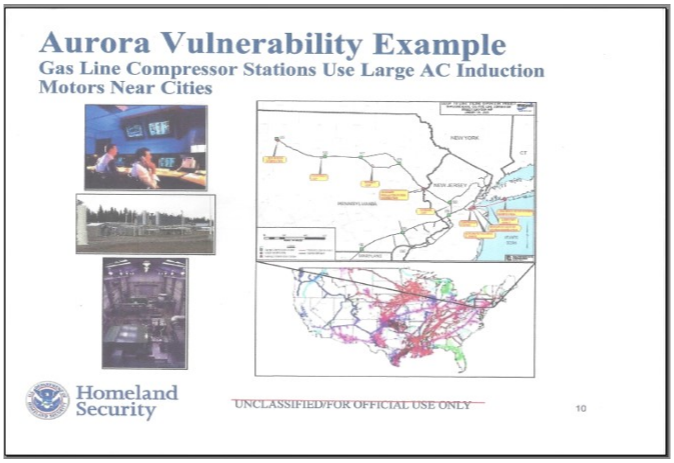
Aurora Vulnerability Example

Water Pumping Plants Use Large Motors in Series

Homeland Security ~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~ 9

Figure 9 Aurora Vulnerability Affecting Water Facilities

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...



Aurora Vulnerability Example

Gas Line Compressor Stations Use Large AC Induction Motors Near Cities

NEW YORK
NEW JERSEY
PENNSYLVANIA
CT
MARYLAND

Homeland Security

UNCLASSIFIED/FOR OFFICIAL USE ONLY

10

Figure 10 Aurora Vulnerability Affecting Gas Compressor Stations

There is a hardware fix, but very few utilities have adequately implemented it.

Siemens contracted INL to evaluate the Siemens PSC7 product line for cyber vulnerabilities in the 2008 time frame (Figure 11).

2008 Automation Summit
A Users Conference

ID#: 2481
Title: Control System Security Assessments
Track: Industrial Security

Presenters: Marty Edwards
Idaho National Laboratory

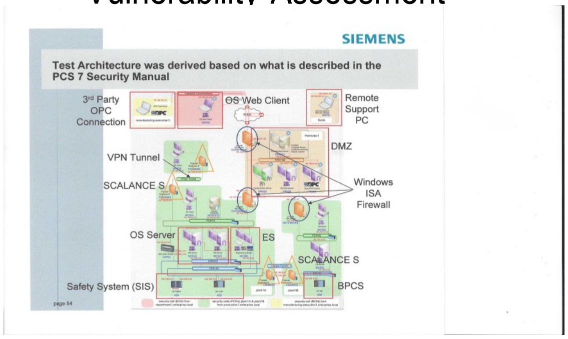
Todd Stauffer
Siemens

Figure 11 Siemens/INL PCS7 Presentation

INL gave a presentation at the 2008 Siemens International User Group Meeting in Chicago on the results of the testing. Why would Siemens ask DHS to perform a security assessment on PCS7? The intent was to validate and improve the PCS7 security concept; leverage INL's unique skillsets (e.g., Aurora), enhance the security posture of PCS7 control systems, knowledge transfer to members of the PCS7 Security lab, expand DHS/INL body of knowledge for protecting control systems that control US critical infrastructure, help Siemens customers comply with new government regulations, and produce input for certification which did not exist at the time of the testing.

The test architecture was derived based on what was described in the PCS7 Security Manual which included firewalls, VPN tunnels, DMZ as well as the Basic Process Control Systems (BPCS) and the Safety Instrumented Systems (SIS). The Targets of Evaluation were selected to stress key parts of the system and to leverage INL's expertise gained from the Aurora testing. The testing assessed the vulnerability of DMZ servers for the attacker to gain control of a server inside the DMZ as gaining control of a server inside the DMZ would be a stepping stone for getting into the BPCS. The DMZ servers included WSUS, Virus Scan, and Certification Authority servers. The next step gained unauthorized access to the Engineering Workstation with the goal to gain interactive login to the PCS7 Engineer's Workstation as the Engineer's Workstation is used for the development, maintenance, and troubleshooting of the BPCS and the SIS. The next step performed protocol fuzzing to find vulnerabilities with a goal of causing a communication disruption/overload. The communication paths included TUV certified safety system communication, controller-to-controller, Plant Bus, and Terminal Bus. Creating a communication overload scenario is a common hacker method for attempting to take

Figure 12: Siemens/INL PCS7 Vulnerability Assessment



SIEMENS

Test Architecture was derived based on what is described in the PCS 7 Security Manual

ACS APPLIEDCONTROLSolutions ©Applied Control Solutions 20

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

down a control system. The next step obtained unauthorized access to the Configuration Database to modify the PCS7 Engineer's Workstation configuration. The objectives were to access/modify the control system configuration WITHOUT BEING DETECTED to compromise the controller configurations in the BPCS and SIS! This was essentially a description of Stuxnet in 2008. However, the attendees didn't recognize what this really meant. Think of the industry reaction to Stuxnet in September 2010 when Ralph Langner first started publishing his results. It should also be noted the Siemens presentation was on the web for all to see until about 2012 when it was removed (Figure 12).

the first sophisticated cyber attack against ICSs that also included the SIS. Stuxnet was an engineering attack on a process which cannot be patched or prevented by AntiVirus (there was an Iranian paper to this affect). Stuxnet was not identified for well over a year despite the damage to the plant equipment (centrifuges). The attack defeated 2-factor authentication despite the Certificate Server that was part of the PCS7 design. The methodology can, and has been, used to attack many IP network-based ICSs (not just Siemens) as demonstrated by the Triconex hack (Trisis) disclosed in December 2017 (Figure 13).

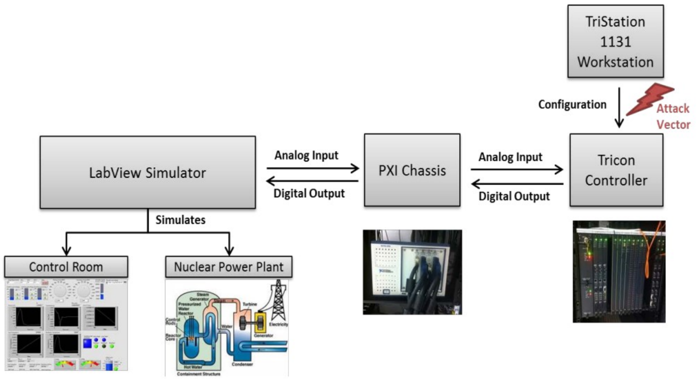


Figure 6. Test Bed Setup for Cyber Security.

Figure 13 Triconex Test Setup

Trisis leveraged a zero-day vulnerability in Schneider Electric's Triconex Tricon safety-controller firmware. The vulnerability allowed for privilege escalation, which would allow hackers to manipulate emergency shutdown systems during a targeted attack. In addition, there was a remote access trojan (RAT) within Trisis, providing attackers with a wide array of options, including the ability to turn off industrial equipment or sabotage the safety controllers in order to create unsafe conditions. The RAT is the first designed to specifically impact SISs, allowing for someone to access the highest privileges available on a targeted machine. In this case, the RAT was injected directly into the computer's memory, making it more difficult to capture and analyze. According to the May/June 2015 DHS Monitor, "Some asset owners may have missed the memo about disconnecting control systems from the Internet. Our recent experience in responding to organizations compromised during the BlackEnergy malware campaign continues to bring to light this major cybersecurity issue—Internet connected industrial control systems get compromised. All infected victims of the BlackEnergy campaign had their control system directly facing the Internet without properly implemented security measures. The BlackEnergy campaign took advantage of Internet connected ICS by exploiting previously unknown vulnerabilities in those devices in order to download malware directly into the control environment. Once inside the network, the threat actors added remote access tools, along with other capabilities to steal credentials and collect data about the network. With this level of access, the threat actor would have the capability to manipulate the control system." Despite DHS's admonitions, there are more than 2 million ICS devices connected directly to the Internet and more being configured in part because of IIOT applications.

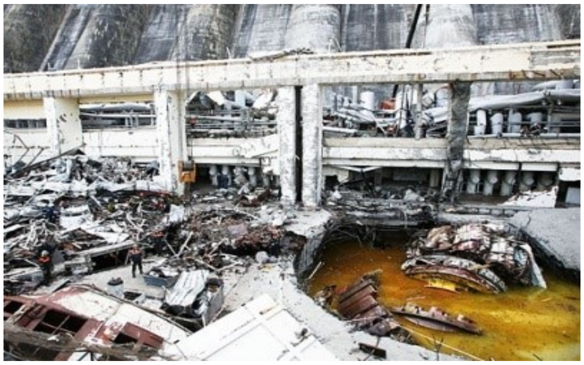
The Ukraine suffered a series of electric grid cyber attacks in December 2015 and 2016. As with Stuxnet, many people were surprised. As with Stuxnet, this should not have been a surprise as the attack scenario was identified six months before the first attack.

There are many approaches to hacking control systems depending on the ultimate goal. If the ultimate goal is denial-of-service, network manipulation is generally the choice. However, if the intent is to cause equipment damage or destruction, manipulating physics is a more effective approach for a number of reasons: Cyber security considerations are generally not adequately consid-

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

ered during system design such as lack of mechanical interlocks, etc. Consequently, systems can be more susceptible to damage. Another example would be cycling power supplies to cause mechanical damage from thermal cycling internal electronic components. Additionally, manipulating physics can cause cascading failures affecting other systems. Once started, “unstable” electrical or mechanical operations in forbidden operating zones may be impossible to stop. This can be electrical instabilities or operating in resonance frequencies (Figure 14).

Figure 14 Sayano–Shushenskaya Dam Failure



Many “physics” scenarios such as Aurora are not network-related so they cannot be identified from network monitoring. It is often difficult to detect the difference between operational anomalies and cyber attacks. The first 20 times the Australian sewage plant discharge valves were opened, the wastewater operations personnel felt it was a mechanical or electrical problem, not a cyber attack (Figure 15).

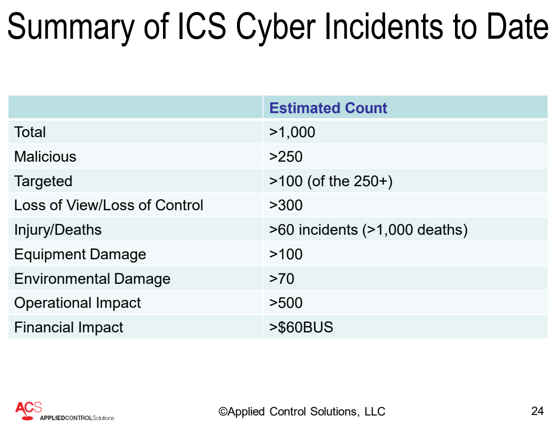
Figure 15 – Maroochyshire Sewage System Cyber Attack

Manipulation of physics can apply to any physical-cyber system.

As noted from the discussions above, ICS cyber incidents are real. There have been more than 1,000 ICS incidents to date. Impacts ranged from trivial impacts, to significant environmental discharges to significant equipment damage, to widespread electric outages, to deaths. The impacts are international in scope and have affected multiple industries, defense facilities, hospitals, transportation, etc. A summary is given in Figure 16.

Figure 16 ICS Cyber Incident Summary

As mentioned, cyber security has been focused on networks. Consequently, most of the discussions are on the ISO 7 layer stack rather than the Purdue Reference Model. Cyber security also has a focus on identifying MAC addresses, Internet Protocol (IP) addresses, and network hardware devices and effectively excludes all non-Ethernet data. Many ICS network monitoring solutions provide non-intrusive asset discovery, network anomaly detection, micro-segmentation of networks, and network visibility all of which is very important. What is missing, however, is view and understanding of what is happening with Level 0,1 devices BEFORE their data is converted to Ethernet communications via serial-to-Ethernet converters (gateways) as identified in Figure 5. If you are a doctor and you can’t trust the



Summary of ICS Cyber Incidents to Date

	Estimated Count
Total	>1,000
Malicious	>250
Targeted	>100 (of the 250+)
Loss of View/Loss of Control	>300
Injury/Deaths	>60 incidents (>1,000 deaths)
Equipment Damage	>100
Environmental Damage	>70
Operational Impact	>500
Financial Impact	>$60BUS

ACS APPLIEDCONTROLSolutions

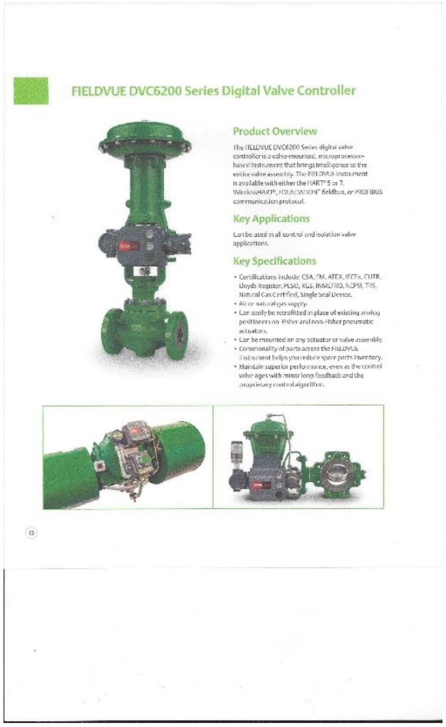
©Applied Control Solutions, LLC 24

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

temperature or blood pressure readings, how can you make a diagnosis? Why did this Level 0,1 gap occur and why is it important? IT views cyber security as the network and is focused on the Ethernet packets. However, Level 0,1 devices are viewed as engineering systems and start as analog devices. Consequently, cyber security was (and continues) to not be part of the design process for Level 0,1 devices. Additionally, Cloud providers assume sensors are authenticated and secure. Sensor standards including Namur 43, ISA108, etc.do not appear to adequately address cyber security whereas security standards such as IEC62443-4-2 do not appear to adequately address Level 0,1 devices. Additionally, sensor protocols are cyber vulnerable including wired and wireless HART -- Highway Addressable Smart Transducer, Profibus, and Fieldbus. As an example, January 23rd, 2018 DHS ICS-CERT issued a vulnerability disclosure on Siemens devices using the PROFINET Discovery and Configuration Protocol.

Both Wired and Wired-HART communications have been demonstrated to be cyber vulnerable and can be used as a vehicle to get access to reconfigure sensor configuration such as span, range, and damping. This can result in loss of safety and yet not be detected by network monitoring.

Level 0,1 devices include controllers and drives as well as instrumentation. Figure 17 is of a digital valve controller that can use any of the aforementioned cyber vulnerable communication protocols.



FIELDVUE DVC6200 Series Digital Valve Controller

Product Overview

The FIELDVUE DVC6200 Series digital valve controller is a valve-mounted, microprocessor-based instrument that brings intelligence to the entire valve assembly. The FIELDVUE instrument is available with either the HART® 5 or 7, WirelessHART®, FOUNDATION™ fieldbus, or PROFIBUS communication protocol.

Key Applications

Can be used in all control and isolation valve applications.

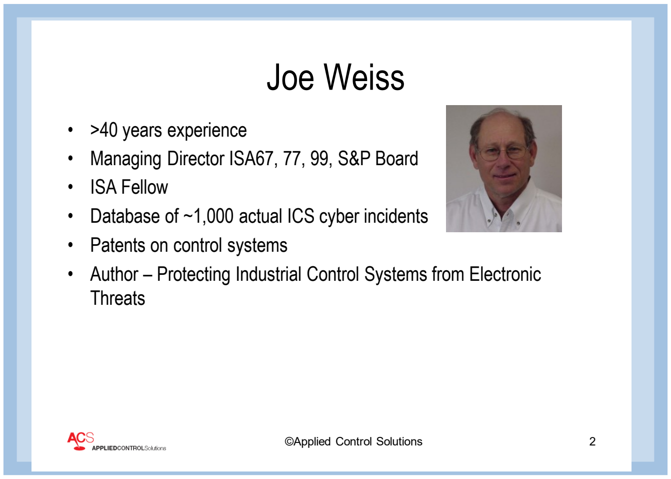
Key Specifications

- Certifications include: CSA, FM, ATEX, IECEx, CUTR, Lloyds Register, PESO, KGS, INMETRO, NEPSI, TIIS, Natural Gas Certified, Single Seal Device.
- Air or natural gas supply.
- Can easily be retrofitted in place of existing analog positioners on Fisher and non-Fisher pneumatic actuators.
- Can be mounted on any actuator or valve assembly.
- Commonality of parts across the FIELDVUE instrument helps you reduce spare parts inventory.
- Maintain superior performance, even as the control valve ages with minor loop feedback and the proprietary control algorithm.

13

Figure 17 Digital Valve Controller

Cyber considerations occur with the addition of microprocessors to conventional 4-20 milli-amp sensors that can perform calculations, produce diagnostics, and allow remote communication capabilities using protocols such as HART. The design features of smart transmit-



Joe Weiss

- >40 years experience
- Managing Director ISA67, 77, 99, S&P Board
- ISA Fellow
- Database of ~1,000 actual ICS cyber incidents
- Patents on control systems
- Author – Protecting Industrial Control Systems from Electronic Threats

ACS APPLIEDCONTROLSolutions

©Applied Control Solutions

2

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

ters and I/O devices that allow the instruments to communicate bidirectionally which inherently precludes an "air gap". A smart transmitter doesn't simply measure the output analog signal but needs to be able to communicate with the transmitter and read the digital signal.

The need for process sensors (and other level 0,1 devices) to communicate with a Windows-based HMI requires a Serial-to-Ethernet Convertor (gateway). Several issues arise affecting gateways and cyber security: Many of the gateways have identified cyber vulnerabilities which is an issue not just for BPCS but also for SIS. Another issue is that process noise is used to perform diagnostics of the process and the sensors. However, gateways filter out the process noise which preclude the ability to identify certain sensor and process issues including sensing line issues, flow-induced vibration, etc. (Figure 18)

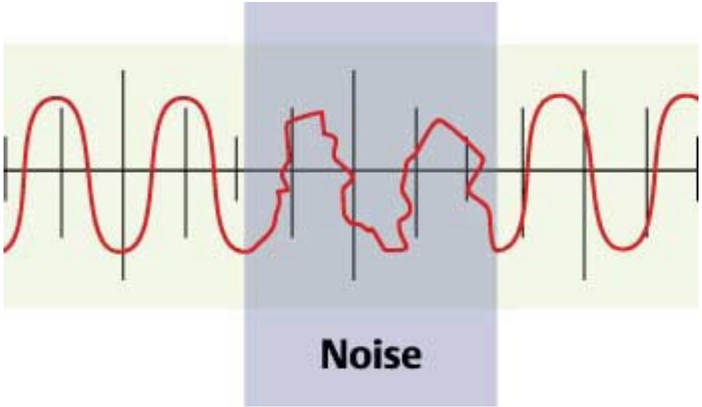


Figure 18 Sensor/Process Noise

Other Level 0,1 issues include the need to redefine Level 0,1 in 2018 terms, the lack of ICS-CERT addressing level 0,1 devices, etc. The 2016 ICS CERT Annual Assessment Report identifies Potential Network Attack Scenarios in Figure 19 but only goes as far as Level 3. There is no mention of any Level 0,1 issues.

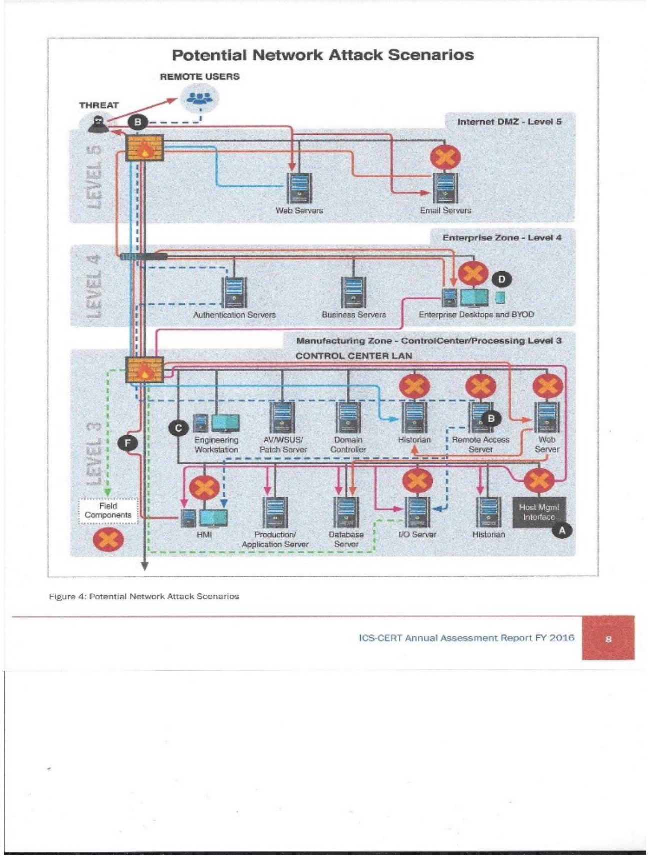


Figure 4: Potential Network Attack Scenarios

ICS-CERT Annual Assessment Report FY 2016 8

Figure 19 2016 ICS CERT Annual Assessment Report

Examples of actual process sensor cyber-related incidents include:

Dam failure when sensors pulled away from wall providing erroneous low readings resulting in pumps overfilling the reservoir.

A sensor on a valve malfunctioned and resulted in the release of millions of gallons of untreated wastewater.

A pressure transmitter sensing line clogged causing a plant trip in a fossil power plant.

A safety relief valve in a nuclear plant did not lift because the pressure sensor never reached its setpoint.

PLC automatically opened the reject bin chute door based on faulty sensor data dropping10 tons of material on the truck cab resulting in a fatality.

The level sensor failed to identify the rising level of petrol, so the 'final alarm' did not sound and

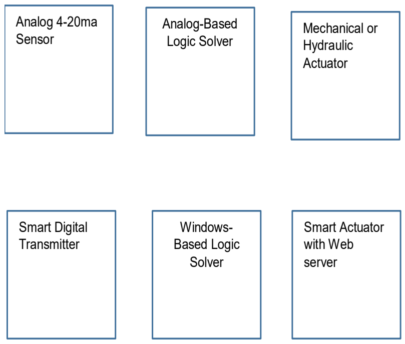
Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

> the automatic shutdown was not activated. By the time the explosion occurred, over 250,000 liters of petrol had escaped from the tank injuring more than 40. The ensuing fire, the largest seen in peacetime UK, engulfed over 20 fuel tanks on the tank farm and adjacent sites and burned for several days.

There are non-malicious events but could be done maliciously. As an engineer, it should not matter.

Safety is well understood and accepted throughout the enterprise whereas ICS cyber security is not. The relationship between process safety and cyber security is not necessarily clean. Safety Integrity Levels (SIL) are not the same as Security Levels (SLs). SIL is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function (SIF) whereas SLs focus on prevention of unauthorized information disclosure.

As safety and security are related but not the same, it raises questions about the term “risk”. As an example, in one plant, the installation utilized hardwired certified trip amplifiers to connect the analog sensors to the safeguard analog final elements. In the second plant, the installation utilized a certified programmable electronic logic solver utilizing a broadly utilized computing operating system to connect intelligent sensors to the safeguard final elements with built-in webservers. From a safety perspective, the risk to both are the same, but from a security perspective, the risk would be different (Figure 20).



Analog 4-20ma Sensor	Analog-Based Logic Solver	Mechanical or Hydraulic Actuator
Smart Digital Transmitter	Windows-Based Logic Solver	Smart Actuator with Web server

Figure 20 Differences in Safety Systems

Safety standards including Namur 163 (Security Risk Assessment of SIS), ISA84, and IEC 61511 do not adequately address Level 0,1 issues. In addition, they allow a mix of BPCS and SIS systems. Based on hacking experience and DHS ICS-CERT vulnerability notifications, how can gateways and HMIs be allowed in SIS applications without being isolated from BPCS and the “outside world”?

The Bellingham, WA Olympic Pipeline Rupture (Figure 21) was an ICS cyber incident that also had safety issues.

Figure 21 Bellingham, WA Olympic Pipeline Gasoline Pipeline Rupture

Immediately prior to the pipe rupture, the SCADA system which had a nominal 3-7 second scan rate increased to 30 seconds to 400 seconds to totally unresponsive (Figure 22).

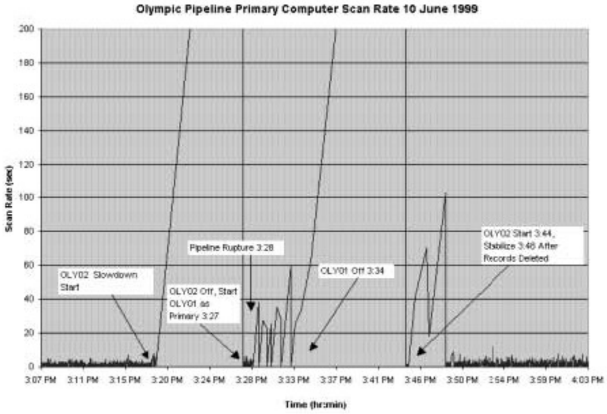


Figure 22 SCADA Scan Rate

When SCADA became unresponsive, the logic was to set all sensors to average values which led to loss of safety. Additionally, because the sensors were set to average values, traditional sensor monitoring would not have identified a problem as the sensors were not out-of

Joe Weiss Keynotes TAMU Instrumentation Symposium (continued)...

-band. The Olympic Pipeline case was arguably the first case where a cyber event can be directly connected to a loss of safety event.

As mentioned, gateways can be cyber vulnerable. Namur 163 segments the SIS but allows communication between the zones (Figure 23)

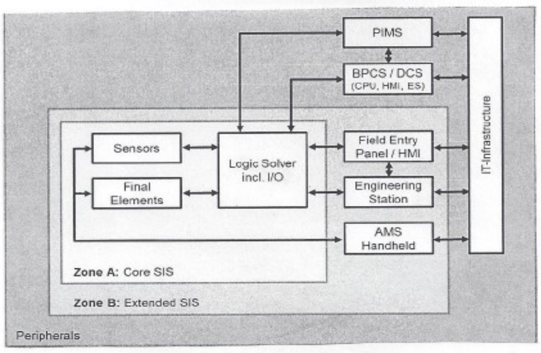
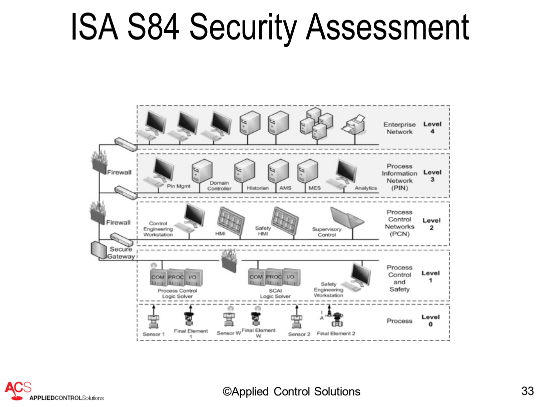


Figure 23 Namur 163

ISAS84 offers seven architectural examples from a fully isolated SIS to various combinations of interconnected SIS and BPCS (Figure 24).


ISA S84 Security Assessment

©Applied Control Solutions 33

Figure 24 ISAS84 Security Architecture Assessment

Achieving the appropriate security levels is largely dependent on the specific controller, networking, and countermeasures chosen for a given application (notice the Level 0 is not addressed). Therefore, the analyses focus on the high level impact the selection of architecture has on the ease or difficulty with respect to achieving the overall cyber security objectives for the Safety Control Alarms and Interlocks -SCAI. In each example architecture, it is assumed that ALL safety functions, including safety controls, safety alarms, and safety interlocks are executed on the safety controller. As a result, the safety security zone must include all the hardware (including the safety HMI) necessary to execute the safety functions. What should be evident from Stuxnet and Triconex is any approach that is less than fully isolated can be a cyber threat which would include sharing of sensors from the BPCS with the SIS.

Based on my experience, the following can, and should be done today:

- Obtain senior management buy-in specifically for ICS cyber security with adequate resources and priorities.
- Establish a cross-discipline team reporting to the C-Level consisting of Operations, Maintenance, Engineering, Safety, IT, Telecom, Forensics, Risk, and Crisis Management with adequate resources and priorities.
- Implement a “living” ICS cyber security program.
- Develop ICS-specific cyber security policies and metrics including for Level 0,1 devices;
- Perform risk assessments based on critical needs such as safety, reliability, regulatory compliance, etc;
- Implement appropriate ICS cyber security technologies including process and network anomaly detection;
- Develop a configuration/control program that includes control systems, safety systems, and cyber security considerations;
- Completely isolate the SIS from BPCS; and
- Develop security requirements for procurement specifications.

Visit Joe Weiss’ blog at http://www/controlglobal.com/blogs/unfettered and his website at [http://www.realtimeacs.com.](http://www.realtimeacs.com)

THE WAY I SEE IT

Editorial

Treat Employees Better If You Want High Performance

Rockwell Automation, Emerson Automation Solutions, ABB and other major automation companies have been touting their efforts to provide training for new entrants in the automation profession. Rockwell started their own automation bootcamp in collaboration with Manpower; Emerson has funded Rankin Tech to provide high level college and technical school education for new automation professionals. ISA has established a scholarship fund in the name of Dick Morley. Festo has established an entire division, Festo Didactic, to provide teaching tools for automation professors.

All that is wonderful. It is great. And unless the lot of automation workers is greatly improved, we are going to have jobs going begging and new entrants into the work force running away as fast as they can from careers in automation and factory and process control.

Now that the President and the Republican Congress has given a huge tax cut to large corporations, there is no excuse for corporations not to allow some of that money to actually trickle down to the hourly and lowly professional worker level— where all the automation professionals are. In China, in India, and in other places, automation workers are a sought-after job category and people want to become automation professionals. In the USA, we should make sure that's true too— even when companies like Carrier and others are closing plants and laying off workers, including automation workers.

Comments? Talk to me!
waltboyes@spitzerandboyes.com

Read my Original Soundoff!! Blog:
http://www.spitzerandboyes.com

In many plants, operators and other low level automation workers are considered hourly workers and not professionals. No special licensing is required to be an operator in either a factory or a process plant. Even the water treatment plant and the boiler plant must have licensed operators. Yet there are no licensing requirements for the operators of assembly lines and process units that are in command of multi-million-dollar trains that produce profits for the company.

ISA failed miserably to get their CCST and CAP certifications required for working in factories and process plants. You don't have to be a Control System Engineer to design and build and operate control systems.

If we are going to raise the skill level and the attractiveness of automation jobs, we need to clothe them in the trappings of professionalism. The CAP and CCST certifications and the companion textbook, *The Automation Book of Knowledge,* are excellent places to start.

It should be a matter of safety and security to make operators and engineers get licenses. Safety and security are going to become much more important in the next few years, as nation state terrorists are going to attack electric grids, oil and chemical process plants, and cause destruction via cyber means and through safety systems that are vulnerable.

Big automation companies, big asset owner companies, and technical schools need to band together and get the governments who oversee manufacturing and process plants to see that a requirement for licensing is necessary.

And we need to make sure that licensing is not a rubber stamp. Instead we need to use licensing as the way forward to create the skills level needed to run plants in the 21st century.

I think the Automation Federation is the best possible vehicle to assume this crusade. We need to give Marty Edwards the funds and the staff he needs to make this happen.

Safety, security, knowledge, experience are going to make automation in the future even more important than it has been in the past. We can get the best and brightest, if we want them.

Walt Boyes

The Industrial Automation and Process Control INSIDER™ is published by Spitzer and Boyes LLC., Copyright 2014-2017, all rights reserved.

The INSIDER is edited by Walt Boyes. Joy Ward is a columnist. Additional reporting is done by David W, Spitzer PE., Rajabahadur V. Arcot, Nick Denbow, and Steven Meyer.

INSIDER INDUSTRIAL AUTOMATION & PROCESS CONTROL SPITZER AND BOYES, LLC

The INSIDER is a subscription based publication and does not take advertising. This means that the INSIDER can be completely independent and unbiased in its reporting and in its analysis.

To subscribe to the INSIDER, please visit http://www.iainsider.co.uk and click the "Become an Insider" button.

Send comments to insider@spitzerandboyes.com. We want to hear from you!

Rajabahadur V. Arcot: Leverage technology but focus on delivering technology to customers

Manufacturing industries for their autonomous, efficient, and safe operations require the production processes to be monitored and controlled and for that purpose invest in industrial automation systems.

Industrial automation systems, which collect information about the various operational parameters and automatically regulate some of them, evolved to meet this demand.

Meeting the needs of the manufacturing industries remained the dominant driver for the growth of the automation industry. Locally mounted mechanical gauges and electrical meters gave place to control room panel mounted pneumatic and electronic instruments and controllers.

Over the years, as the manufacturing industries became bigger and more complex, their needs also changed, and the automation industry began to extensively uses the processing and computational capabilities of microprocessors; convergence of information and communication technologies further contributed to the extensive use of communication protocols in industrial automation systems.

The ongoing rapid developments taking place in the information and communication technologies (ICT) continue to have profound influence on evolution the automation industry. The developments include computer-systems' ability to gather data and analyze the same into information & insight and perform tasks that normally require human intelligence and skills associated with cognition, visual perception, speech recognition, and decision-making.

Until now, automation systems leveraged the ICT to access data from plant, equipment, and machinery and convert them into information which are disseminated, stored, and manipulated according to the manufacturing plant's operational requirements. ICT served as a technology enabler or a tool in the hands of automation suppliers. Recent technological developments in information and communication technologies hold the promise of making automation systems more intelligent and thus capable of performing predictive and prescriptive tasks and get them up to speed to meet the needs of the future manufacturing era, Industry 4.0.

Meeting the needs of the manufacturing industries remained the dominant driver for the growth of the automation industry. Locally mounted mechanical gauges and electrical meters gave place to control room panel mounted pneumatic and electronic instruments and controllers.

The success of manufacturing companies of the future depends on their ability, on one hand, to be agile, flexible, and responsive to customer demands and, on the other, improve material usage productivity, environmental sustainability, supply chain efficiencies, asset performance, lifecycle management, and such others.

This mandates autonomous exchange of real-time information amongst all systems and solutions for managing all associated production and enterprise operations in an integrated manner. This can be achieved by transforming production equipment into cyber-physical systems by embedding computational and networking capabilities and connecting them.

Currently, there is a great deal of discussion on the building blocks of such technology solutions of the future that include Industrial Internet of things (IIoT), artificial intelligence (AI), machine learning, cloud computing, big & fast data analytics, edge computing, and such others.

While companies, such as ABB, Siemens, Rockwell, and GE, are presently some of the

Rajabahadur V. Arcot: Leverage technology but focus on delivering technology to customers (continued…)

leading providers of operating technology (OT) solutions, such as programmable logic controllers, distributed control systems, plant safety systems, sensors and actuators, the major initiatives to enhance the role of ICT in industrial automations systems are triggered by technology companies, such as Apple, Google, IBM, Microsoft, and others, who have competencies in IIoT, AI and such others mentioned above.

While automation supplier companies have intimate understanding of the manufacturing industries' demand for the OT solutions, the challenges of the production processes, and proven track-record in meeting their needs, technology companies are working continually on cutting edge developments in ICT.

> …the major initiatives to enhance the role of ICT in industrial automations systems are triggered by technology companies, such as Apple, Google, IBM, Microsoft, and others…

Technology companies' narrative is more about the enhanced capabilities of the ICT and how they can help enterprises to become seamlessly connected and information driven; and they offer platforms / infrastructure such as Azure (Microsoft), Watson (IBM), Alexa (Amazon), and DeepMind (Alphabet), for others to build applications including industrial automation applications.

They are also making large investments and establishing new centers of excellence to develop and demonstrate their competencies. They have deep financial resources and have been in the forefront in driving the developments in ICT. They have been successful not only in convincing the industrial sector about the expanded role for the ICT in the OT architecture of the future but also in downplaying the drawbacks, such as the cyber security challenges.

On the contrary, automation suppliers provide comprehensive solutions that address the needs of industries by leveraging multidisciplinary technologies including ICT. Automation suppliers recognize, on one hand, the benefits of leveraging the new developments taking place in the ICT and integrating them into their OT architecture and, on the other, the need for collaboration with technology leaders to gain greater access to latest ICT, around which comprehensive solutions can be built.

The recent collaboration agreement between ABB and IBM is the outcome of such an approach. ABB in its joint statement about the agreement with IBM said it would combine its digital offering that gathers information from machinery with IBM's expertise in artificial intelligence – IBM's Watson data analytics software.

Yet another such strategic agreement was signed by ABB with Microsoft. ABB's press release says that the company with a view to drive digital industrial transformation "will leverage Microsoft's Azure services such as Azure IoT Suite and Cortana Intelligence Suite to capitalize on insights gathered at every level from device, to system, to enterprise, to cloud."

We have wait for the future to tell us whether such agreements have paved the way for creating enduring value to all stakeholders.

In this context it may be pertinent to draw some lessons from the recent GE announcement about its decision to operate the software and services including its Predix platform in Amazon Web Services and Microsoft Azure public cloud data centers to save money rather than duplicate efforts.

However, it will be safe to conclude that the future OT solutions will only come from companies who have excellent competencies in both automation and information and communications technologies and when they begin to offer comprehensive and integrated solutions which are cyber secure and deliver demonstrable business benefits to manufacturers. This is what the customers want.

Rajabahadur Arcot is an Independent Industry Analyst and Business Consultant, and Director Asia Operations for Spitzer and Boyes LLC **with 40 years of senior management experience. He was responsible for ARC Advisory Group in India. Contact him at rajabahadurav@gmail.com**