Check out the ARC Forum for 2017 ...page 12

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

VOLUME 20
NUMBER 10
ISSN2334-0789
October 2016

Your key to the latest industrial automation and process control information

Four Conferences: More from Inductive Automation, Wonderware, Yokogawa, and Emerson Exchange

Inductive Automation Sells Passes to watch ICC'16 sessions

Inductive Automation's Ignition Community Conference has a new first. For a limited time, you can buy a ticket to watch the sessions on streaming media. This is a response to the fact that the conference was sold out, and that many developers and integrators couldn't take the time to attend. For more information, including pricing, visit https://icc.inductiveautomation.com/register/tickets.

This makes a great deal of sense, since many people who would otherwise not go to a user group meeting can partake in the information, and vicariously in the spirit of the thing. Maybe other companies should take note and follow suit. Schneider Software, which split up their user groups into several differently scheduled meetings, should maybe take note.

Dueling User Group Meetings...Yokogawa, Wonderware and Hurricane Matthew

The Yokogawa USA User Group and Schneider Software's Wonderware Live meeting were both scheduled for the same days in early October in Orlando, about five miles apart. I was very glad that I had rented a car to facilitate covering both conferences, because it turned out that I had to make a mad dash to Tampa to catch a plane after Hurricane Matthew forced the cancellation of my plane out of Orlando. Many others were not so lucky. It was a near thing but the Hurricane simply bumbled up the coast coming ashore in South Carolina instead of right at Orlando, where it was originally aiming.

Wonderware LIVE! was well-attended, with probably 500 people, while Yokogawa's user group was much less well attended, but quite interesting, nonetheless.

This was the first user group meeting for Schneider Software since the abortive attempt to use them as bait to acquire Aveva without paying full price, and it looked like Wonderware was absolutely back on its feet and moving forward, and as near as anybody could tell, Schneider is happy with them and happy to keep the group.

Ravi Gopinath

There were significant product releases, including the ubiquitous cloud apps. Ravi Gopinath and Rob McGreevy tried to put Wonderware's forward-looking plans into perspective. Gopinath noted that Wonderware maintains its lead in automation software because it is relentlessly hardware agnostic, and McGreevy suggested that there were three critical trends that Wonderware is responding to: acceptance of public cloud services (the INSIDER has doubts, but…), tightening the belt on CAPEX, and increasing reliance on short cycle ROI.

Rob McGreevy

Inside this issue:

INSIDER HealthWatch

Waiting for the election or somebody like that
Page 13

Four Conferences: More from Inductive Automation, Wonderware, Yokogawa, and Emerson Exchange (continued)

Wonderware is betting that because of these trends, more users will be looking at applications as a service, or "renting" software to get data— what Wonderware calls "Infrastructure as a Service." This is the basis of Wonderware's IIoT offering.

Wonderware introduced a significant product release in the Infrastructure as a Service, or IaaS, with Wonderware Online InStudio, a secure cloud subscription service that allows System Integrators to "overlay a next-generation infrastructure that is highly available and scalable." InStudio joins Online InSight in Wonderware's portfolio of cloud– and mobile– based apps.

Wonderware also introduced a serialization suite for the pharma and biopharma industries, as well as a new batch solution, which, interestingly, is not compatible with ISA88, ISA95 or ISA106. "The customers aren't demanding it," we were told.

By far the most important release by Wonderware was the launch of "Prometheus." This is a configuration tool for defining, programming, and documenting all components in an industrial control system. It is an open programming environment that automates complex configuration tasks and enables the configuration of control components, regardless of type or brand. At least according to the press release, anyway. How unique it is may be debatable, with PAS and Inductive Automation offering somewhat similar software. Code developed in Prometheus is independent of the target platform, Scott Clark told us, but once it is complete, it is compiled by the vendor's software so it is as hardware agnostic as possible.

At **YOKOGAWA**, Sandy Vasser, recently retired from Exxon-Mobil, gave his "It Just Works" talk that we have all heard so often in the past few years. It would be nice if the industry worked like that. Maybe it will.

Sandy Vasser

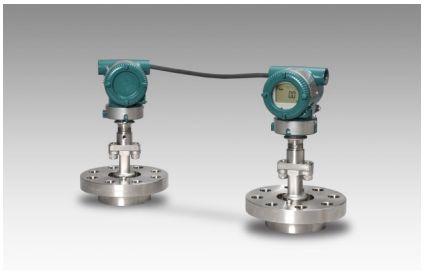
Frank Abagnale

Also keynoting was Frank Abagnale, the anti-hero of the film, "Catch Me if You Can." Abagnale is a reformed con artist who works as a consultant to the FBI and other three-letter agencies.

There were a few product introductions, as well, including the introduction of a new production program of ROTAMASS Coriolis mass flow meters, the ROTAMAS TI. Standing for "Total Insight," these flow meters have new features. Yokogawa has developed a new tool that will assist our customers in selecting the optimal sensor and transmitter combination for specific applications. In addition, an online expert guide and a built-in configuration wizard are provided to ensure quick and error-free commissioning. Yokogawa added a Process Guard function that can be used to select event patterns for the issuance of alarms, configure the trigger-ing of data logging based on alarms or manually set points, and specify whether data is to be backed up to a microSD card for use in root cause analysis.

ROTAMASS TI

A Maintenance Manager function that includes Yokogawa's patented Tube Health Check technology monitors all key sensing elements while the flowmeter is in use, yielding data that can be used to minimize disruptions and thereby reduce maintenance costs. All data can be stored on a microSD card for easy data transfer. A new Feature On Demand (FOD) option is available that allows users to upgrade already installed flowmeters by adding new product functions such as the Tube Health Check and a concentration measurement function.



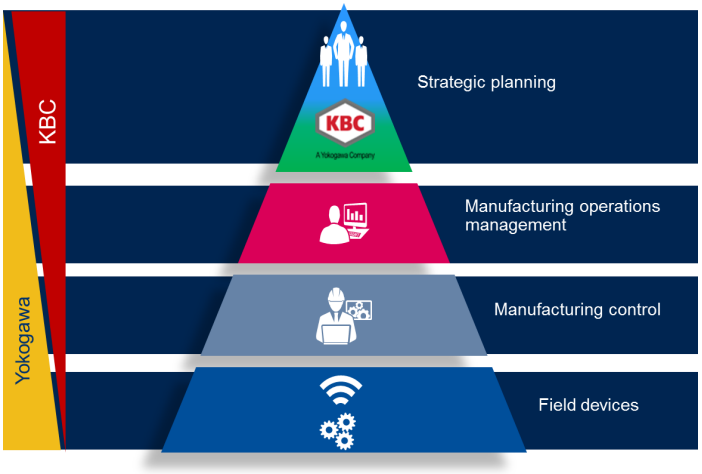
XJC40A Pressure Transmitters

Yokogawa also announced the EJXC40A digital remote sensor, a newly developed DPharp EJX series differential pressure transmitter. Equipped with two pressure sensors that are connected with an electric cable, the EJXC40A offers superior performance in the measurement of liquid levels in large tanks and large differential pressure with high-pressure fluids. This new addition to the DPharp EJX series will meet a wide range of customer needs.

Historically famous for being acquisition-averse, Yokogawa has decided to change that, acquiring a 44.3% stake in Soteica, completing the acquisition of Industrial Evolution, and now the recent acquisition of KBC, all of which are being operated as independent subsidiaries.

Four Conferences: More from Inductive Automation, Wonderware, Yokogawa, and Emerson Exchange (continued)

Yokogawa is quite enamoured of the synergies they've created with KBC:



Although CEO Takashi Nishijima did not attend, he sent along a video that was played at the opening session. The highest ranking Yokogawa Electric executive physically present was Tsuyoshi "Ted" Abe who recently came to Yokogawa from a long career at Intel. Abe strikes one as highly capable, and his biggest strength is also his greatest weakness as VP of Marketing: he doesn't know the industry. This can help him because he doesn't have the typical Yokogawa blinders, and it can hurt him because he may not know what he's seeing.

Nishijima-san

Emerson Exchange Comes Home to Austin

A considerably larger group with considerably more enthusiasm gathered in Austin for the first ever Emerson Exchange as Emerson Automation Solutions, the new melding of Emerson Process Management and Emerson Industrial Automation. It has always seemed a little strange that Emerson Electric had two automation divisions, neither of which spoke to the other.

To give former CEO. Steve Sonnenberg, a good sendoff, he and new CEO ("Executive President") Mike Train tag-teamed at the opening ceremony, along with retired Emerson CEO John Berra, who was there because he lives in Austin.

Sonnenberg says that as Chairman, he can focus on whatever he wants to do, which is acquisitions and talking to customers.

Executive President Mike Train

Mike Train is an interesting character. He is mild-mannered and seems a little laid back, until he snaps out an order and is instantly obeyed. He plays blues guitar, loves muscle cars and speaks Japanese. His background is primarily sales management, and has experience in Asia, as well as running Emerson's perennially anemic analytical instrumentation unit, which he finally got running on all cylinders.

He has a very interesting challenge ahead of him, since what used to be Emerson Industrial Automation lacks some significant products with which to take on Siemens, Rockwell, et al. The obvious is to attempt to acquire Rockwell, but I don't see that happening. Look for something else entirely, as Emerson goes shopping.

Despite the fact that both sides of the company had different cultures, the internal merger is apparently going very well, as Emerson adds even more new and different acquisitions, such as the valves division of Pentair, Permasense (a corrosion control sensor company from the UK) and more.

Expanding on last year's discussion on Top Quartile Performance, Emerson executives talked about the new solutions they've put in place to help their customers achieve it. Peter Zornio, Chief Strategic Officer offered a revised and resuscitated "PlantWeb" which made retired executive John Berra positively glow, since he'd come up with the concept twenty years before. PlantWeb is now going to be the Industrial Internet of Things platform for Emerson and will be as vendor agnostic as they can allow it to be. Emerson, of course, offered a set of services very much like everyone else. The current economic climate, as Rob McGreevy from Wonderware had noted two weeks previously, is designed to make end users think about ways they can not spend capital money. Emerson executive Mike Boudreaux (watch this guy, he's good) is in charge of the company's services offerings. Connected Services, as it is called, is powered by Microsoft Azure Cloud Services, and is primarily aimed at asset management and management of uptime.

CSO Peter Zornio

Mike Boudreaux

The Automation Whisperers: How SAIMC Reinvented Itself

Vinesh Maharaj and Oratile Sematle discuss the SAIMC: how it reinvented itself to emerge as automation's voice in South Africa and how automation can help to shape the future.

By Steven Meyer, editor, SA Instrumentation and Control.

The ample boardroom at Yokogawa South Africa's new head office in Randburg can easily accommodate twenty people around the working centre table. The four of us seem lost in the roominess, but that initial awkwardness soon fades and at the end of our allotted hour, there is barely enough space to contain the passion of two of the SAIMC's most enlightened presidents.

Yokogawa's Vinesh Maharaj and Oratile Sematle from SASOL

SA Instrumentation and Control product manager Jane van der Spuy and I are here to join Vinesh Maharaj (Yokogawa South Africa sales & marketing director, and immediate past president of the SAIMC) and Oratile Sematle (E&I Group manager at Sasol, and current SAIMC president).

We have all put aside our professional responsibilities for an hour and are meeting as volunteers serving an organisation that we are passionate about – the SAIMC.

Our aim is to review the progress the Society has made since it became the recognised 'Voice of Automation' in South Africa under Vinesh's capable leadership; and to talk about where it is headed, as Oratile carries the fire during his tenure for the next two years.

> To become more competitive as a nation we need to reindustrialise. The government has already started this, but they are getting the wrong advice on how to implement it. Automation is a key component, but instead of importing automation skills from abroad, we should be developing our own.

Vinesh's contribution to the SAIMC can be summed up in one word – transformation. "When I took over the presidency in 2013, Johan Maartens, my predecessor, had paved the way for change," he says. "But we needed more; it was time to take a calculated risk."

The plan was ambitious. "We needed to reinvent ourselves," explains Vinesh, "both in terms of our strategic objectives as an organisation, and in terms of our value proposition to members and to industry. We had to sweep away the cobwebs."

What followed completely redefined the SAIMC. A two-day strategy session with industry leaders sees the formulation of a medium term business plan, which includes championing the cause for Automation as the tenth distinct engineering discipline recognised by ECSA (Engineering Council of South Africa). A modern new logo emerges and the Society unveils its fresh persona in a glittering function at the end of 2013. Automation's voice speaks its first words. Something more subtle happens as well. A groundswell of urgency develops as the new culture takes hold. It draws industry leaders wishing to volunteer their time to serve at the top echelons of the organisation. People who want to get things done; people like Oratile Sematle.

"I've taken over a completely revitalised SAIMC thanks to the work of council under Vinesh's leadership," says Oratile, who has been listening intently up until this point.

"During my term, the challenge is different. My goal is to build on what we have already achieved, but we must take it further.

We have to make people at the highest levels in our country understand that automation is not a threat, but rather, a key driver for industrialisation in our region."

"This is crucial," agrees Vinesh, "but it is only one of the missing pieces in the puzzle."

"We need to get much closer to the industry fraternity and to the educators as well," explains Oratile, as the vibe in the room starts to build.

"And to ECSA," adds Vinesh, "but I know this has high priority on your agenda."

What they are intimating is that the work has only just begun. While there is much that can be accomplished along the way to add to the value proposition for SAIMC members and patrons, both Vinesh and Oratile believe that the big payoff will come when ECSA inaugurates Automation as the tenth official engineering discipline.

The Automation Whisperers: How SAIMC Reinvented Itself (continued)

"With the situation as it currently is people often just fall into an automation career by accident," explains Oratile. "Not just at engineer level, this applies to technicians and artisans as well. Most of them qualify in an electrical or electronic field and then it is up to their employers to equip them with the skills they need to undertake instrumentation or automation related work."

"To become more competitive as a nation we need to reindustrialise," adds Vinesh in a tone that conveys quietly controlled passion. "The government has already r this, but they are getting the wrong advice on how to implement it.

Automation is a key component, but instead of importing automation skills from abroad, we should be developing our own. We have everything we need; all that is lacking is a cohesive approach between the various stakeholders."

The two believe that this is where the SAIMC can and must make a meaningful difference.

"One of the ways we can stimulate our economy is to cut our reliance on imports," rationalises Oratile. "But in order to do this we must be able to offer a better quality of product at a price that compares with the cheaper imported equivalents, from China for arguments sake."

"Automated production and quality control can help us achieve this," adds Vinesh. "Look at the textile industry. It has been completely destroyed by cheap imports and thousands of workers have lost their jobs."

What they are hinting at is the belief that with proper implementation and the right focus, automation can create new jobs by either revitalising an industry that has become uncompetitive, or by opening up opportunities in areas that are currently underexploited – minerals beneficiation for instance.

Vinesh contextualises it perfectly: "Automation is not a silver bullet that can fix everything that is wrong in South Africa. We are where we are for many reasons, some of which are the legacy of previous governments, and others which are not. What is important is that we don't just accept that we are destined to stay where we are, and this is where automation has a role to play."

"To be competitive globally, I believe that automation and labour have to be successfully combined," says Oratile, warming to the theme. "You can no longer just rely on labour. The beauty of automation is that it cuts across all sectors, and with proper management, workers displaced by automation in one sector can be reskilled and deployed in another, which has become more competitive, because of automation."

"The question of skills shortage is a complex one," says Oratile

All very well, but how do we develop the capability?

"The question of skills shortage is a complex one," outlines Oratile. "Traditionally we have been strong in instrumentation, but the problem we are faced with is that those skills, mostly learned through experience, are not successfully being transferred to the younger generation."

"Exactly," Vinesh joins in animatedly. "A skilled person is not just somebody with a qualification. A skilled person is someone with the right qualification for their profession, enhanced by good on the job experience. Automation has become much more complex than just instrumentation, these days it takes 3-4 years for someone from another discipline, electrical for instance, to become fully productive as an automation engineer after they qualify."

"Automation is not a silver bullet that can fix everything that is wrong in South Africa. We are where we are for many reasons, some of which are the legacy of previous governments, and others which are not. What is important is that we don't just accept that we are destined to stay where we are, and this is where automation has a role to play."

"We could shorten that to 1-2 years if we had an appropriate automation qualification supported by relevant practical training," adds Oratile. "What happens currently is that after the 3-4 years Vinesh mentioned, these people become highly sought after and are often lost by the employer who initially invested in them. Sometimes they are even lost by the country, and then the cycle starts all over again."

The SAIMC identified this need early during Vinesh's term when the business plan was drawn up and something it hopes to address through the work it is currently doing with the Universities of Technology and with ECSA.

The Automation Whisperers: How SAIMC Reinvented Itself (continued)

"If the country is serious about a strategy to make local manufacturing more competitive, then automation is a key component of that and it is crucial that its role be adequately defined," says

"The status quo could continue indefinitely unless we get buy-in from industry," says Vinesh Maharaj

Vinesh heatedly.

"What we are trying to explain to the authorities is that the automation courses we need already exist," adds Oratile thoughtfully. "They just need to be repackaged into a qualification that can serve industry better. In the view of the SAIMC, it will not be necessary to introduce any new academic courses."

What has been raised at ECSA is that people currently being registered as process engineers were never specifically trained in this discipline.

"This status quo could continue indefinitely unless we get buy-in from industry who are the 'consumers' of such process engineers," explains Vinesh. "If we don't do something to change the situation, properly trained and experienced process engineers will remain a scarce commodity, and they will have to be imported from abroad."

"Surely it is better to develop our own people and then let them create jobs for others through the growth of our manufacturing sector as it becomes more competitive?" asks Oratile somewhat rhetorically.

"Our responsibility as the voice of automation is to raise the profile of our profession. We can make a real contribution if we can show young people that automation is cool, and a career path worth following."

"But we can't do this without offering them a properly recognised qualification," says Vinesh, in no mood to take prisoners. "We already know that there are universities eager to provide the courses we need. Now we need to take automation mainstream."

The next step is a presentation to ECSA and other stakeholders on 19 October to showcase what the SAIMC has accomplished to date. "This is a vital meeting for us," says Oratile earnestly. "ECSA will only recognise this tenth discipline if it has support from the academic institutions."

"We are almost there," adds Vinesh. "The presentation will be based on the business case for automation. We need to prove that there is a critical mass, around four hundred industry people out there, ready to register in an automation engineering discipline. This is research that Johan Maartens – the newly appointed SAIMC COO – is busy doing for us. We also need to show a development path that allows people to progress from one level to the next – how to get from artisan to technician level, for instance."

"ECSA would like to get as many people as possible registered," concludes Oratile. "What we must do on the 19th is show them how the SAIMC can help to achieve this. With the academic institutions behind us, we have a very strong case to present."

> "But we can't do this without offering them a properly recognised qualification," says Vinesh in no mood to take prisoners.

In conclusion

Some of what has been discussed is idealistic, and most certainly there will be obstacles along the way. To sit in comfortable surroundings discussing the pros and cons of automation as a driver for economic growth in Africa is one thing, but overcoming the harsh political and demographic realities is quite another.

What is undeniable though is that the new SAIMC has leaders of vision and purpose. If automation can make a meaningful contribution to South Africa's growth and prosperity, then there is a passionate organisation run by committed people ready willing and able to make it happen.

Anyone wanting more information can reach Oratile or Vinesh through SAIMC secretary Ina Maartens, +27 (0)86 107 2462, admin@saimc.co.za, www.saimc.co.za

The *INSIDER's* October 2016 Roundup

Advantech's Great Wzzard Adventure

Advantech, Taiwan's answer to National Instruments, has taken a flier on an American company, which is, we believe, a first for the highly diversified automation company. They acquired, last December for a little over $99 million, the Ottawa, IL, based B+B Electronics. B+B started out as a catalog reseller of automation and networking products, including Advantech's ADAM line of field devices. Over the years, B+B morphed into a manufacturer, rather than a reseller, and that is what Advantech was looking for. Now called B+B SmartWorx, the Advantech division has released what they call, "an intelligent sensing platform," called Wzzard. This is hardly unusual for B+B, since they have been involved at the cutting edge of industrial wireless since it's beginning. The very first industrial wireless sensor application I reported on was an installation in 2004 by B+B of a Sensicast wireless temperature transmitter used to detect breakthrough in a water cooled continuous casting application.

Advantech's new Wzzard

The most interesting part of this is that B+B SmartWorx and Advantech have partnered with Inductive Automation's Ignition product line to provide what B+B calls, "a complete wireless sensor connectivity platform for the rapid deployment of scalable, intelligent, and reliable Industrial IoT networks…"

So, B+B is not just another sensor maker, or just another radio seller. They have complete products and solutions. Their first two application bundles are a condition-based monitoring bundle, costing less than $2200.00, and an energy monitoring bundle for approximately $2400.00. These bundles include sensors, nodes, a cellular gateway, cables and accessories.

Pepperl+Fuchs joins forces with mobile explosion protection pioneer ecom instruments

Pepperl+Fuchs announced the acquisition of ecom instruments GmbH, the world market leader for mobile industrial devices for hazardous areas. Ecom, of Assamstadt, Germany, has developed explosion proof cell phones, 4G smartphones and tablets. With this Pepperl+Fuchs complements its portfolio in explosion protection with mobile solutions. The INSIDER covered ecom instruments' latest product releases in the September 2016 issue.

"In ecom instruments we found an industry pioneer with 15 percent growth rate lately who, for decades, proved and strengthened his technology leadership in mobile explosion protection and now complements our offering with a competitive portfolio reaching far into the future" said Dr. Gunther Kegel, CEO of the Pepperl+Fuchs group.

"Besides the expanded product portfolio we can see new opportunities arising along the entire value added chain. With this we can not only strengthen our offering in the field of explosion protection, but we can achieve a much better market position – with a partner from our region – and consequently generate new solutions around the complex of Industry 4.0", added Kegel.

"The expertise in explosion protection and the wide-spread international sales force of Pepperl+Fuchs made them our favorite partner from the very beginning. Our innovative devices do not only fill a gap in their portfolio, but allow ecom instruments and Pepperl+Fuchs to develop future business models and solutions at the Center of Competence at Assamstadt to gain access to the enormous growth potential of the ongoing digitalization of industry", Rolf Nied stated, founder and managing partner of ecom instruments GmbH.

GE Oil and Gas Merges with Baker-Hughes

As a former employee of, first Baker International and then Baker-Hughes, I find it interesting to watch the company, even though they are mostly out of the automation industry now.

GE and Baker Hughes have merged GE Oil and Gas with Baker Hughes, to produce what the companies call "the New Baker Hughes, a GE Company." GE will own 62.5% of the new company, and Baker Hughes existing shareholders will get a one time payment of $17.50 per share, and 37.5% of the new company. The combined companies will have over $32 billion in revenues.

Siemens names new management in UK and Ireland

Siemens has announced two new senior managerial appointments for the UK & Ireland with effect from October 2016.

Andrew Reeks moves to take up the position of General Manager - Partner Management, with responsibility for the Digital Factory and Process Industries and Drives divisions.

Reporting to Brian Holliday, Managing Director - Digital Factory, Andrew will oversee the Partner Management team and drive the growth strategy for Siemens' partners. His responsibilities will include assessing the current partner strategy and processes to further enhance organisational efficiencies and strengthen existing partner relationships.

After a period as General Manager for Partner Management, **Stephen Hughes** is taking up a senior role with responsibility for Strategic Sales Projects and as executive sponsor for

The *INSIDER's* October 2016 Roundup (continued)

food and beverage sector sales. Reporting to Jim Harris, Siemens UK & Ireland Sales Director, Stephen will oversee a number of strategic sales initiatives, including the introduction of Siemens' General Motion Control (GMC) solutions into the heating, ventilation and air conditioning (HVAC) market alongside Siemens Building Technologies, as well as developing growth into the maintenance, repair and operations (MRO) market.

Andrew Reeks, Siemens

Andrew Reeks comments: "I am delighted to be taking over responsibility for our important partner management relationships. I intend to build upon and further develop the excellent work Stephen Hughes has carried out to establish the strong, vibrant and mutually beneficial partner management program we have today."

Stephen Hughes, Siemens

Stephen Hughes says: "Having enjoyed the responsibility of building relationships with Siemens partners, I am excited to be moving to my new role. It is designed to focus on strategic sales projects and target where Siemens' market-leading solutions can help improve efficiencies, drive productivity gains and aid company growth across industry."

Brian Holliday, MD Digital Factory for Siemens UK and Ireland

Brian Holliday, Managing Director - Digital Factory, Siemens UK & Ireland comments: "We welcome Andrew and Stephen to their respective new roles. They are key senior appointments in strategically important areas for the Siemens business and both will make significant contributions in supporting our business growth objectives and focus on helping drive productivity for our customers.

Bedrock Automation Extends Cyber Security to Industrial Serial Communications with the New Bedrock™ *SIOS.5* Serial I/O Module

Bedrock Automation has extended cyber security to serial communications with a new ***SIOS.5*** Serial I/O module for its Bedrock™ Open Secure Automation (OSA™) control system. The ***SIOS.5*** has five channels, each supported by an independent cyber secure 32-bit ARM processor. Each channel is software-defined for RS-232, RS-485 or RS-422 communications, extending the range of industrial edge devices that can be secured by users of the Bedrock OSA. Combined with other software-defined I/O modules, Bedrock OSA is the only system that delivers analog, discrete, digital, pulse, Ethernet and Serial data as intrinsically secure I/O.

Bedrock CTO Albert Rooyakkers

"We connect every signal type to the Bedrock controller as software-defined I/O, with intrinsic cyber security. The SIOS.5 I/O module provides users tight and effortless serial data integration. Extending Bedrock intrinsic cyber to serial communications delivers authentication of the firmware and drivers. The SIOS.5 will be valuable for users and necessary for building a secure IIoT," says Bedrock CTO and Engineering VP, Albert Rooyakkers.

Extending cyber security to serial communications results in improved reliability on a wide range of applications:

- RS-232 support enables secure communication with modems, gateways, printers, barcode readers, programmable devices and PC peripherals.
- RS-422 support with a single bus master for process automation (chemicals, brewing, paper mills), factory automation (autos, metal fabrication), HVAC, security, motor control, and motion control.
- RS-485 support for multi master bus/drivers.
- Mainstream protocols such as Modbus and ProfibusDP.

Each of the ***SIOS.5*** channels is independently configurable to support independent concurrent drivers. Five independent 32 bit ARM™ processors enable real-time performance of communications and control.

Schneider acquires AIT

Schneider Electric has acquired Applied Instrument Technologies, Inc., a leading provider of online process analyzers for

The *INSIDER's* October 2016 Roundup (continued)

the hydrocarbon, petrochemical, chemical, pharmaceutical and steel-making industries. The acquisition adds to Schneider Electric's process automation portfolio that already includes Foxboro plant instrumentation, Foxboro and PlantStruxure PES process automation systems, Modicon PAC systems and Triconex safety systems.

Based in Upland, Calif., AIT has an installed base of more than 1,000 systems and a breadth of spectroscopy and chromatography solutions, including a comprehensive portfolio of process analyzers and associated implementation services. Its technology improves process optimization, asset protection and compliance with environmental regulations, allowing customers to better manage and improve their operational profitability.

"AIT enhances our portfolio and strengthens our position as one of the world's leading providers of process automation systems, solutions and services," said Gary Freburger, president, Schneider Electric's Process Automation business. "Growing our capabilities is a critical part of our strategy to help our customers transform their businesses, improve their operational profitability and realize the future of automation. We are excited to add AIT and its accomplished team, and we will work closely and diligently with them to effect a seamless transition for our customers and other stakeholders." The acquisition builds on a partnership the two companies established in 2015.

Gary Freburger

Chris Lyden

"As a trusted partner, AIT enabled us to offer one integrated solution for enhanced process analysis, control and asset protection, improving efficiencies and adding significant value for our customers," said Chris Lyden, senior vice president, Process Automation, Schneider Electric. "Formally adding them to our business not only increases the value we are able to provide to existing strategic accounts, it fortifies us in new markets. In short, we'll be able to bring far more business value to customers we already share while enhancing our cross-selling abilities and opportunities."

The INSIDER believes that the acquisition also provides Schneider Electric the ability to extend its process measurement, automation and safety solutions to a broader customer base, especially in fuels blending, petrochemicals and gas processing.

"AIT has been building a highly successful organization for almost 20 years, one that has helped revolutionize process analysis in several important industries," said Joe LaConte, president, AIT. "Our employees and industry thought leaders have the proven ability and expertise to develop and deliver groundbreaking tools and technology that help our customers improve their operational profitability. We look forward to capitalizing on and strengthening the synergies we have cultivated with Schneider Electric over the years."

AIT's Joe LaConte

AIT and its offerings will be fully integrated into Schneider Electric's process automation business by late 2017 and will continue to be managed by its existing executive team.

Emerson and FLEXIM combine flow portfolio

Emerson and FLEXIM are collaborating to help process customers optimize their flow process design, flow meter selection and flow meter installation on capital projects to reduce execution risk and costs. Emerson's project teams, using FLEXIM's clamp-on, ultrasonic flow metering portfolio in combination with Emerson's own flow metering offering, can consult early and throughout the project cycle to reduce engineering, piping and installation costs as well as schedule risk.

This cooperation will support Emerson's Project Certainty – what Emerson calls a transformational approach to enabling top-quartile performance in capital projects.

The non-intrusive nature of FLEXIM's ultrasonic flow meters makes this product a powerful contributor to reduced engineering, piping and installation costs as well as schedule risk, given that it can be installed after piping is fabricated. Emerson and FLEXIM will collaborate to ensure less time is spent on engineering and installation through the selection of the optimal flow solution.

Bret Shanahan

"In today's market, we are seeing that our customers are looking for us to advise them early in their project cycle on technology to ensure streamlined and cost-effective project execution," said Bret Shanahan,

The *INSIDER's* October 2016 Roundup (continued)

vice president of flow solutions, Emerson Automation Solutions.

"We are pleased to be working with FLEXIM to provide our clients with the most appropriate flow solution that can be applied and support greater capital efficiency," Shanahan said.

Flexim's Schwanekamp

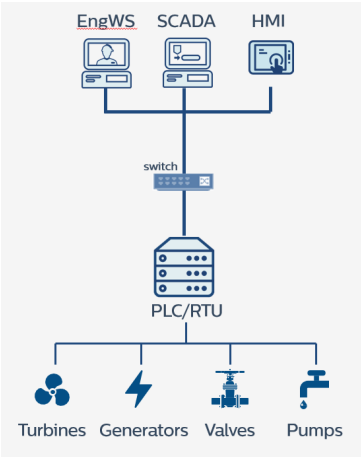
"FLEXIM is excited to partner with Emerson on capital projects; our flexible, world-class, non-invasive meters are a perfect fit with Emerson's experienced project teams," said Guido Schwanekamp, managing director sales and marketing of FLEXIM. "Together we will be able to offer fully customized solutions that are tailor made for a wide variety of capital projects aimed at reducing capital expenditures while increasing efficiency for our clients and reducing total cost of ownership at the same time."

Right now, it appears, Emerson and FLEXIM are only dating. It remains to be seen if Emerson will pop the question soon or not. Emerson has an empty place that FLEXIM will fit right into.

New SCADA Vulnerability Enables Remote Control of ICS Networks

Mille Gandelsman, CTO, Indegy and Avihay Kain, R&D, Indegy gave a paper at the recent 2016 Industrial Control Systems Cyber Security Conference (also known as WeissCon, after its founder Joe Weiss) and their blog about it is excerpted here by permission.

As part of our ongoing R&D efforts we occasionally discover vulnerabilities in industrial controllers (PLCs, RTUs, DCS etc.) and software tools. Recently, Indegy Labs team discovered a vulnerability in Unity Pro, Schneider Electric's flagship software application for managing and programing industrial controllers.. Before we get into the specifics, it's important to point out that unlike in IT networks, a vulnerability is not necessarily required to compromise controllers in an ICS network.



That's because industrial controllers lack authentication and industrial communication protocols lack encryption

Surprising as it might sound, anyone who has access to the control network, also has unfettered access to all of its industrial controllers. This means that anyone who can ping a controller, can probably send it a stop command or reprogram the device to cause operational disruptions. Nonetheless, some vulnerabilities can pose exceptional risk to ICS networks.

The vulnerability in Unity Pro allows any user to remotely execute code directly on any computer on which this product is installed, in debug privileges. The vulnerable software tool is present in every control network in the world that uses Schneider-Electric controllers. Regardless of the SCADA/DCS applications in use, if Schneider Electric controllers are deployed, this software will be used on the engineering workstations. This makes this attack relevant across virtually any process controlled by these PLCs. Since Schneider Electric is one of the largest industrial control equipment providers, this vulnerability is a major concern.

As a result of Indegy's responsible disclosure, Schneider Electric has developed a new release of its product which fixes this vulnerability: http://www.schneider-electric.com/ww/en/download/document/SEVD-2016-288-01.

Further Details

The Unity Pro software platform runs on Microsoft Windows machines. The vulnerability found affects all versions of this software, including the latest one. It resides in one of its components named 'Unity Pro PLC Simulator', that is used to test industrial controllers' code prior to executing it on the controllers themselves. The control code projects are compiled as x86 instructions and loaded onto the PLC Simulator using a proprietary format named 'apx'.

Since these x86 instructions are later executed 'as is' by the simulator, an attacker can direct their control flow to execute

The *INSIDER's* October 2016 Roundup (continued)

arbitrary malicious code. As bothersome as this might sound (being a somewhat 'classical' data/code mixture), the knock-out is that receiving .apx files from a remote location to execute them on the simulator is natively supported by the Unity Pro software platform!

ISA announces results of 2016 leader elections

Society President-elect Secretary:
Brian Curtis, Cobh, County Cork, Ireland

Society Treasurer:
Thomas W. Devine, Cazenovia, New York, USA

Executive Board Member: Geographic (2 seats)
Carlos Eduardo Rodrigues Mandolesi, Itatiba, SP, Brazil
James (Jim) Hunter Haw, Houston, Texas, USA

Brian Curtis of GE Healthcare becomes next ISA President-elect Secretary

Executive Board Member: Technical
Jeremey Steven (Steve) Mustard, Houston, Texas, USA

Automation & Technology Department Vice President-elect:
Grant T. Patterson, Tullahoma, Tennessee, USA

Publications Department Vice President-elect:
Michael B. Fedenyszen, Boston, Massachusetts, USA

Standards & Practices Department Vice President-elect:
Christian (Chris) Monchinski, Neptune, New Jersey, USA

Strategic Planning Department Vice President-elect:
Yesid Alberto Yermanos Aldana, Bogota, Colombia

The response rate for the election was 4.82%. The ISA election is conducted by Survey and Ballot Systems (SBS), a company that has been conducting online elections for over 20 years. For comparison, according to data compiled by SBS, societies with membership counts between 15,000-33,999 conducting an online election typically have response rates less than 9%.

Control System Integrators Association emphasizes expanding international presence with announcement of new board member from Australia

The Control System Integrators Association (CSIA) announced that Adrian Fahey has accepted a position on its board of directors. Fahey is CEO of SAGE Automation, a CSIA Certified control system integrator in Melrose Park, Australia. SAGE is one of the largest control system integration companies in Australia and a leading provider of industrial automation and control services.

Fahey says he feels honored to be able to give back to the organization that has given him and his company so much. SAGE has been a member of CSIA since 2001. Fahey sees the biggest benefit to being a CSIA member as the opportunity to engage and benchmark against leading integration companies, indicating that "The Australian market is a lot smaller than in the United States. Therefore, we tend to be much more guarded about sharing information." He continued, "The openness we have observed and been able to participate in as members of CSIA has been outstanding, and has enabled us to develop close working relationships with a number of individual companies."

About Certification, Fahey said, "I think the opportunity to challenge your business through the Certification process is of enormous benefit. We pride ourselves on our systems and processes, but CSIA Certification was a whole new ballgame. The auditing process dove deep into practices and processes and benchmarked them against our specific industry rather than a generic whole of industry."

SAGE Automation's Adrian Fahey

CSIA board chairman Mike Miller (ESCO Automation) said, "SAGE Automation truly understands the value they receive from actively participating as CSIA members. Every year, SAGE sends a large contingent, from Australia, to the CSIA Executive Conference. And, their membership is marked by consistent and enthusiastic networking, applying best practices and maintaining Certification. Fahey's leadership at SAGE, his passion for CSIA and his overall presence on the global stage will make a great addition to an already incredible board."

With Fahey joining the CSIA board, the association's growing international presence is underscored. CSIA has members in 27 different countries, and Certified members are headquartered on every continent except Antarctica.

Presenting the 21st Annual ARC Industry Forum
Industry in Transition: Realizing the Digital Enterprise

February 6-9, 2017 - Orlando, Florida

Industrial companies are starting to employ 'digitalized' business processes and exploit the increasing convergence between operational technology (OT), information technology (IT), and engineering technology (ET) on the plant floor. How will disruptive technologies change existing products and plants? How will open source solutions impact traditional software and automation domains? Is cybersecurity a threat to digitalization? How 'smart' are smart machines? How do Big Data and predictive and prescriptive analytics enable operational change? Join us to learn how the digital enterprise benefits from smarter products, new service and operating models, new production techniques, and new approaches to design and sourcing.

Industrial Cybersecurity and Safety
Analytics and Machine Learning

Asset Performance Management

IT/OT/ET Convergence

Service Performance Management
Automation Innovations

Industrial Internet Platforms

Connected Smart Machines

For more information, please visit our Website at arcweb.com or contact us.

ARC Advisory Group

Founded in 1986, ARC Advisory Group is the leading research and advisory firm for industry and infrastructure. For the complex business issues facing organizations today, our analysts have the industry knowledge and first-hand experience to help our clients find the best answers.

Keynote Speakers:

Marty Edwards
Assistant Deputy Director, National Cybersecurity and Communications Integration Center
Director, Industrial Control Systems Cyber Emergency Response Team
U.S. Department of Homeland Security

Don Bartusiak
Chief Engineer, Process Control
ExxonMobil Research & Engineering

Who Should Attend

ARC's Industry Forum is a must-attend event for:

- CEOs, COOs, and Presidents
- CFOs, VPs, and Directors of Finance
- CIOs and CTOs
- VPs and Directors of IT
- VPs, Directors, and Managers of Operations
- VPs, Directors, and Managers of Engineering
- VPs, Directors, and Managers of New Projects
- VPs, Directors, and Managers of Procurement
- VPs, Directors, and Managers of Supply Chain and Logistics
- Directors, Managers and Architects of Automation and Enterprise Integration
- Plant Managers and Supervisors

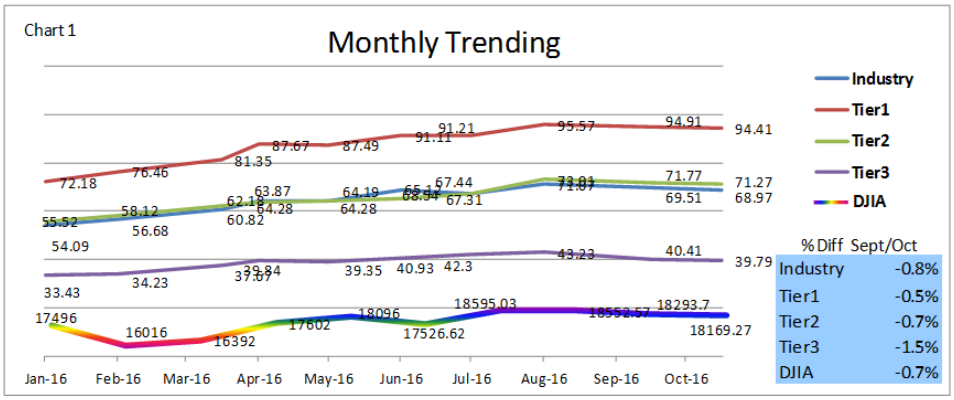
Production Managers and Supervisors

In past Forums, over 50% of the attendees have titles like Chairman, CXO, President, Vice President, Director, or Partner.

Waiting for the election, or somebody like that...

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Health Watch



Aside from the acquisition noise, which is increasing, really nothing much is going on in the automation industry. It would appear that, like the stock markets, everyone is waiting for some semblance of sanity to return to the United States—hopefully by November 9th.

Index leaders for the month of September included Alps Electric, FMC, Fuji Electric, Gefran S.p.A, Yokogawa, Mitsubishi, and Cameron.

Index laggards for September included Meggitt SA, IMI plc, Flowserve, Pentair, FLIR Systems, Honeywell Automation and Controls, Toshiba, HLS Systems International (Hollysys) and Ametek EIG.

Some of the laggards may have been affected by recent merger and acquisition movements.

- ABB announced Q3 results as "Continued margin growth in tough markets." Some highlights reported were
  Operational EBITA margin1 increased to 12.6%
  White Collar Productivity on track towards $1.3 bn savings; expected total costs reduced by $100 mn
  Net Income $568 million; basic earnings per share up 2%
  Base orders -6%2; total orders -13%; reflect Q3 uncertainty
  Revenues steady
  Cash flow from operating activities $1,081 million, more consistent quarterly cash generation
  Timo Ihamuotila to succeed Eric Elzvik as Chief Financial Officer effective April 1, 2017
  ABB launched Stage 3 of its Next Level Strategy – committed to unlocking value.

ABB is, according to Ulrich Spieshoffer, Chairman and CEO, a "a hidden digital champion today. It is ideally positioned to win in the digital space with new and existing end-to-end digital solutions. The newly launched ABB Ability offering combines ABB's portfolio of digital solutions and services across all customer segments, cementing the group's leading position in the Fourth Industrial Revolution and supporting the competitiveness of ABB's four entrepreneurial divisions."

But nothing can hide the results: Process Automation orders down 22%, Power and electrification off significantly, as were discrete automation and motion.

ABB really needs that Digital Ability transformation they say they've started.

Next month the picture will be very different— the US Election will be over, and there will be, for better or worse, a coherent policy going forward. The INSIDER can hardly wait.

THE WAY I SEE IT
Editorial

Shutting Down the Internet of Things

Friday, October 21st, a DDOS attack on Dyn Inc., brought down several major sections of the Internet including large retailers, Amazon and Ebay, and PayPal. What was different about this attack was that it was conducted by a bot army made up of devices from the Internet of Things. About 500,000 wifi cameras, refrigerators, smart thermostats, and other devices were used, in three waves to throttle Dyn's servers and keep major websites from operating.

The US Government gave as its opinion, that it was not a state-sponsored actor (the Russians or Chinese) and that was given more weight after the attacks died down shortly following the release of a notice from WikiLeaks that the rumored death or kidnapping of Russian-sponsored hacker Julian Assange were incorrect and that he was safely in the Ecuadorian embassy, as before.

Aside from the tie between Assange's followers and Russian sponsored attempts to damage the campaign of Hillary Clinton and cast doubt on the validity of the US election process, the thing that is truly scary is that it is easily possible with open source code to do this again, using IoT devices as bots.

Comments? Talk to me!
waltboyes@spitzerandboyes.com

Read my Original Soundoff!! Blog:
http://waltboyes.livejournal.com

The question becomes, do we want our refrigerators spying on us for a foreign power, or maybe used to feed data illicitly obtained to our health insurer for the purpose of finding out what we eat, how much, and when...and that's so real it isn't funny anymore.

...the attacks died down shortly following the release of a notice from WikiLeaks that the rumored death or kidnapping of Russian-sponsored hacker Julian Assange were incorrect and that he was safely in the Ecuadorian embassy, as before.

Of course, the Industrial IoT is somewhat different, and is unlikely to be any great part of such an army of IoT device bots.

Why? Most of the field devices in manufacturing, so far, are not IP equipped, and are not directly connected to the Internet, as the botnet army was on the 21st. Cisco and Endress+Hauser, and their partner Rockwell Automation, have been preaching IP to the device, IP to the edge, for several years.

We might want to re-think that.

But more, we should re-think the way we protect our networks. Defense in depth has been shown to be essentially ineffective.

So, too, is the individual protection of each device. It isn't a great leap to imagine that a maintenance supervisor could go to Home Depot and buy an inexpensive IP wifi camera to use to look at a bad actor valve or motor. Suddenly, there's a window for IP based malware into the plant network and systems.

Would this happen? Nobody has been successful underestimating the actions of end-users. People continue to fall for phishing expeditions, and continue to click on malware in emails. We aren't going to be able to rely on education or even discipline to keep this sort of stuff from happening.

If we are behind the eight ball, what can we do?

What is needed, I believe, is a complete rethinking of the way industrial networks are architected, to include security built in at the chip set level. Secure data hand-off, from device to device, and perhaps along each cable, could be designed and should be designed.

The real issue is that end-users want better security but aren't willing to pay for it. I suppose it will take a huge incident, much bigger than the Dyn incident, to get people to accept that security costs money.

The Industrial Automation and Process Control INSIDER™ is published by Spitzer and Boyes LLC., Copyright 2014-2016, 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.

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: Ensuring that ICS are cyber secure is strewn with challenges

The Department of Homeland Security (DHS), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Institute of Standards and Technology (NIST) and similar others are constantly endeavoring to disseminate information and heighten necessary awareness about cyber security issues among the stakeholders and spur them to adopt counter measures that will ensure the security of critical infrastructure industries from cyberattacks.

However, the countermeasures, already in use in enterprise networks for mitigating the risks associated with IT solutions, often do not work in ICS environments.

However, the threat actors continue to enjoy first mover advantages. While industrial control systems related cyber incidents are on the increase, the measures to protect them continue to remain predominantly reactive.

The recently released ICS-CERT report "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense–in-Depth Strategies," prepared by it jointly in association with the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) confirms the view that the challenges in ensuring the cyber security of Industrial Control Systems are formidable and that there are no quick fixes.

While automation suppliers are using more and more commercial off the shelf (COTS) technologies, communication protocols, and open architectures in their industrial control systems (ICS), such as PLC and DCS, many critical infrastructure industry asset owners are integrating their IT Information Technology (IT) solutions with ICS.

This trend, driven by technological developments and business imperatives, has positive and negative implications for owner operators of critical infrastructure companies and security of countries.

Integration empowers asset owners to access more data and generate actionable information that helps them achieve higher levels of productivity and efficiency but they also introduce risks that did not previously exist with isolated ICS built using proprietary approaches.

Integration has resulted in increasing the risk exposure of ICS as they help cyber criminals to leverage known and already exploited cyber vulnerabilities.

However, the countermeasures, already in use in enterprise networks for mitigating the risks associated with IT solutions, often do not work in ICS environments.

While confidentiality, integrity, and availability drive security decisions associated with IT solutions in that order, ICS ranks safety and availability as the most important considerations followed by integrity and confidentiality in that order.

While IT solutions deal with transactions, ICS works with real-time and process-critical data and this necessitates different approaches.

Rajabahadur V. Arcot: Ensuring that ICS are cyber secure is strewn with challenges (continued...)

The ICS-CERT report vindicates my impression that while the threat from malicious actors of cyberattacks to critical infrastructure using computer-based industrial control systems is on the increase, the availability of ICS-specific security solutions has not kept pace with escalating cyber threats.

There is also a serious need to create greater awareness among the stakeholders about cyber threats to critical infrastructure industries and their strategic implications.

...an organization must first identify the systems and components they consider business or mission critical and then must determine the criticality of the assets based on its function and importance to operations, perform risk analysis to identify the current threats, vulnerabilities, and risks to the system or operations, and the impact should a threat be carried out.

The ICS-CERT report not only aims to fill that void, especially among asset owners of critical infrastructure industries, but also recommends Defense-in-Depth mitigation strategies to prevent the cyberattacks from succeeding or at least lessen their impact. The Defense-in-Depth strategies include system & network monitoring, intrusion detection systems, security and audit logging, incident & event logging apart from the usual perimeter security, firewalls, data diodes, and patch and vulnerability management for securing ICS from cyberattacks. Implementation challenges of Defense-in-Depth strategies go beyond technical issues. Initiation of ICS Defense-in-Depth strategy demands asset owners to develop "an understanding of the business risk associated with ICS cybersecurity and manage that risk according to the overall business risk appetite." It also demands a clear understanding of the threats to the business; the operational processes and technology used within the organization; and its unique functional and technical requirements. In addition, the ICS-CERT report highlights that the ultimate success depends on the willingness of the ICS operations staff to accept security as an imperative for all computer-oriented activities, to apply security controls to their operational technology from the standpoint of acceptable risk and more importantly on all individuals at all levels within an organization to understand ICS risks and actively engage themselves in the risk management process. Regarding the process, the report says that an organization must first identify the systems and components they consider business or mission critical and then must determine the criticality of the assets based on its function and importance to business operations and perform cybersecurity risk analysis of the system to identify the current threats, vulnerabilities, and risks to the system and/or operations, and the potential impact should a threat be carried out. Many of the end user companies may find it challenging on two counts; undertaking the process and accessing human resources, much less build in-house competencies, to undertake such tasks.

The report, which is an update of the earlier version released in 2009, provides recommendations and guidance for developing strategies to create necessary defenses to emerging threats to critical infrastructure industries from control systems-related cyber threats. Recognizing that a clear understanding of the current security challenges is needed to develop holistic and specific defensive countermeasures to mitigate cybersecurity threats and vulnerabilities, the document begins by highlighting that the convergence of information technology and operational technology has sharpened the potential risks to control systems and goes on to outline of the current state of ICS cybersecurity, recommends the defense in depth strategy, and explains what defense in depth strategy means in the control system context. The document also lists some of the intrusion methodologies that could enable an advanced persistent threat to remain undetected for long periods of time. These include things such as malware infiltrated through Internet connected ICS devices, remote access credentials stolen or hijacked from authorized ICS organization users, and such others.

While the ICS-CERT report is explicit in making recommendations to asset owners, it does not make similar specific recommendations to ICS vendors that would make it obligatory for them to incorporate in their offerings cyber security features.

In my opinion it is incumbent for vendors to be held accountable as safety is one among the major considerations that spurs owner operators to invest in ICS.

The ICS-CERT document goes on to say that "in the last several years vendors have become aware of the importance of cybersecurity in industrial control systems and in many cases have incorporated security into their product life cy-

Rajabahadur V. Arcot: Ensuring that ICS are cyber secure is strewn with challenges (continued…)

cle."

It however concedes that "not every vendor is taking this approach" and only suggests to asset owners, operators, integrators, and suppliers to use the procurement language during the buying process.

In my opinion it is incumbent for vendors to be held accountable as safety is one among the major considerations that spurs owner operators to invest in ICS.

A few interesting observations about the document are the following.

While the document is silent about ISA- 99 / IEC-62443, it refers to North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) standards, NIST ICS Framework, and specific sub-sector guides such as DOE developed Electricity Sub-sector Cybersecurity Risk Management Process, Transportation Safety Administration (TSA) developed the Pipeline Security Guidelines, and such others.

The document, in its opening paragraphs, quoting Tony Bradley, a Certified Information Systems Security Professional (CISSP) and Information Systems Security Architecture Professional (ISSAP), points out that "if anyone or anything accidentally discovers the vulnerability, no real protection exists to prevent exploitation."

In this context, it is necessary to recognize that threat actors to ICS are high-stake players endowed with deep pockets and technical resources and they are persistently endeavoring to identify sophisticated threat vectors and do not depend on accidental discovery.

Once again, the document says in the concluding paragraph that "Defense-in-Depth measures do not and cannot protect all vulnerabilities and weaknesses in an ICS environment.

"They are applied, primarily, to slow down an attacker enough to allow IT and OT personnel to detect and respond to ongoing threats, or to make the effort on the attacker's side so cumbersome that they decide to put their effort toward easier prey."

These are worrying disclaimers.

The path to secure the critical infrastructure industries, whose strengths are in generating electric power, pumping crude and refining them and such others, from cyber threats is strewn with challenges.

[Editor's Note] It goes without saying that vendors cannot be held liable for the entire cybersecurity situation. End users, frankly, are responsible for more than fifty percent of the situation, and more than that if you consider end user good practices that aren't followed even when written. This does not release vendors from their part of the liability. If an exploit is successful and an attack is made and assets or lives are damaged or lost, there is enough responsibility (blame) to go around. The fact is, the end users must hold the vendors to a higher standard than they have been.

—Walt Boyes

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**