

INSIDER

INDUSTRIAL AUTOMATION & PROCESS CONTROL

VOLUME 21
NUMBER 8
ISSN2334-0789
August 2017

Inside this issue:

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

HealthWatch

Nothing to Write Home About
Page 14



Your key to the latest industrial automation and process control information

Industrial Control System Cyber Security in the Age of the Industrial Internet of Things

AN INSIDER SPECIAL REPORT

Industrial Control System Cyber Security in the Age of the Internet of Things

By Walt Boyes

Where we are

A little over 13 years ago, Joe Weiss and I sat down and tried to figure out how many people in the entire world were competent industrial control system cyber security professionals.

That is, people who understood industrial control systems of all types and Operations Technology (OT), and who also had a significant



Joe Weiss

background in IT cyber security. We were looking for people who could meld the concepts of IT cyber security and the requirements of OT into a new thing—ICS Cyber Security.

We concluded that there were maybe 100 people, worldwide, who were competent ICS cyber security professionals. We also knew that there were at least that many (even all those years ago) people on the dark side of the Internet who were studying industrial control systems for vulnerabilities and ways to manipulate them without permission.

There are more now, but they don't seem to be having the effect we hoped for all those years ago. Now there are certifications, courses, and standards. But still, fewer than 30% of all industrial control systems are protected against most major types of attacks.

Since then, the vulnerability of industrial control systems has increased, and so have the attacks. Joe says that his database now has hundreds of confirmed cyber attacks on industrial control infrastructure, with, he says, "over a thousand deaths." Since 2007, Weiss has been talking about the "Aurora Vulnerability" which allows hackers to gain control of breakers and destroy transformers and generators by changing the phase of the generators randomly. *Wired* magazine recently ran an article showing that a team of Russian hackers apparently working for the Russian government, had, indeed, managed to take control of switches in many parts of the US power grid. They didn't do anything—it was clearly just a proof of concept raid. But they could have destroyed much of the power grid in the United States and kept the power off for months.

Weiss is frustrated, as are many cyber security experts, by the seeming lack of concrete response to these and other issues. ICS security expert, former head of ICS-CERT, and new Executive Director of the Automation Federation, Marty Edwards, agrees. "It isn't a technology issue," Edwards says, "it's a culture change issue."

ICS Cyber Security in the Age of the IIoT 1

INSIDER Roundup: 5

- What Is Going On With ISA?
- InstMC Gets New Leader
- Connected Industries
- Time Sensitive Networking Is Not Another Fieldbus
- Fluke Expands Condition Monitoring
- ABB Opens New Collaborative Operations Center for Pulp and Paper in the US
- Yokogawa Acquires TechInvent2
- Nick Grant Joins ABB
- Opto22 Announces IIoT Certification for Partners
- Schneider Gets Significant Process Win

The Way I See It— Editorial by Walt Boyes: The ICS Cyber Workforce: Where to Find It? 16

Rajabhadur V. Arcot: India's tryst with industrialization and its promising future 17

Want to know the **Mind of the Customer™**? Do you know why your customers buy and why they buy specific products or services, and don't buy others? If you don't know, call us to find out how we can help you! Call **Walt Boyes** at +1-630-639-7090.

Industrial Control System Security in the Age of the Industrial Internet of Things (continued)



Marty Edwards, new Executive Director of the Automation Federation

The culture, however, is seriously resisting changing. And it is something that we have to figure out how to deal with. Edwards notes, “Automation is everywhere. Lots of times, they don’t even know what they have.”

Weiss agrees. He’s been pointing out for years the fact that there are often unknown and unprotected entry points into industrial control systems.

“A contractor will leave a way in so they can remotely troubleshoot the system. Ancient dial-up modems can still be connected to the control system and nobody even knows they are there,” Weiss says.

Weiss is one of the few cyber security experts who will say it publically, “What is going to happen is that we will have a significant cyber event, which will cause damage and deaths, and probably the destruction of a major petrochemical plant, or a major power generating facility, or a transmission and distribution system will go up in smoke, before we do more than throw platitudes at the situation.”

Marty Edwards, over this time as a cyber security expert, from his days at Idaho National Laboratory to his just-completed tour of duty with the Department of Homeland Security’s ICS-CERT (Industrial Control System Critical Event Response Team), has gotten increasingly shrill, just like Joe Weiss has. “We can’t wait,” he says, “for a big event. We have to do more.”

In their new book, *Warnings: Finding Cassandras to Stop Catastrophes*, authors Richard Clarke and R. P. Eddy have a significant chapter on ICS cyber security, in which Joe Weiss is profiled. They note that many of his colleagues have claimed him to be “obsessed” as if that was not a good thing. They note that most of the “Cassandras” they profile in the book share a *difficult* perhaps abrasive personality, and Weiss cer-

tainly does. But his personality doesn’t make him wrong.

Edwards is more personable, but certainly no less concerned. For a couple of years now, he’s been sounding an alarm. Because of the complexity of attack vectors, he says, “anything you don’t want to be compromised, don’t connect it to the Internet. Period.” He said this in a keynote speech at the ARC Orlando Forum in February 2017, and the silence in the room was deafening.

Nobody wants to consider that connecting everything to everything else could possibly be not a good thing.

Edwards says, “Joe Weiss is right about one thing for sure. He insists that there is a serious threat vector coming from the sensors that we connect to industrial control systems. He’s right.”

Industrie 4.0 and The Industrial Internet of Things

Here’s the problem. All of the large industrial control system vendors, and many smaller ones, are betting on the come for the Industrial Internet of Things to usher in a new era which they’ve dubbed Industrie 4.0, meaning the Fourth Industrial Revolution—the data revolution.

They all believe, and have built their strategic plans around, the concept that Big Data and Big Data Analytics will show their customers the way to higher productivity and higher profits, and just coincidentally, increased profits for the industrial control system vendors themselves. In order to produce all that data, though, we are going to have to do something different: we will have to install a whole new set of sensors.

Right now, and for the past century, the sensors in an industrial control system are for *control*. We only install sensors where we need to monitor a variable, like temperature, or pressure, or level, or flow, etc., and use that variable to control the process or the assembly line.

Now we are seeing that we should use many more sensors, and not just for controlling the process. The more sensors we can have looking at the process or the assembly line, the higher the resolution of the data we can mine. This is the basis of the concept of the Internet of Things. Sensors and



Clarke and Eddy’s new book...

Industrial Control System Security in the Age of the Industrial Internet of Things (continued)

transmitters *are* the “things.”

The more sensors you connect to a network, the bigger the threat surface becomes, as each sensor is another potential threat vector. This is something nobody seems to have considered. In the electric grid areas, for example, power companies are giving away NEST smart sensors so they can have visibility into a customer’s use of electricity—and so they can take control eventually of a customer’s usage in the event of high demand. All of these sensors are the edge of the ICS’s new network.

All these sensors are presumed to be producing accurate information—that the data they are reporting is real. What happens if the data is compromised?

The Legacy of IT

The problem is part of the legacy of IT. Remember Joe and I figured that there were about 100 people who understood ICS Cyber Security over a decade ago. The shortfall in cyber professionals is being made up by people who enter the ICS space from IT. The edge of their network is a device or switch that is part of the network, and not a sensor connected to it.

Network visibility software, such as Statseeker, can give you great visibility into the network, but stops short of the sensor. Most sensors do not use Ethernet TCP/IP to communicate. They use semi-proprietary semi-open network protocols such as Modbus, HART, Profibus, Profinet, and Foundation fieldbus to communicate. Standard networks do not even see these devices, only their gateways.

Every single one of those industrial sensor protocols has known vulnerabilities that have been described at Black Hat and other dark side conferences.

“But nobody is paying attention to the sensors!” Weiss says. “Joe is right,” Marty Edwards says.

VCs and Cyber Security

Recently, we have seen the entry of venture capital into the cyber security “industry.” Most of it is going to companies that deal with cyber defense against nation-state threats to IT systems. But increasingly, some of it is going to companies like PAS Global, and others who are working in ICS Cyber Security. The question is whether these newly bankrolled

companies will actually produce safer infrastructure, or will they be part of what Clarke and Eddy called “satisficing.” That is, they’ll help companies to do enough that they will be able to say that they are better prepared, but not really.

What the VCs are not doing is investing in training and culture change.

Bob Adamski’s Nightmare

Many years ago, the late, very well-known safety and security expert, Robert Adamski suggested that the then-nascent remote operations business was fraught with problems.

“Just suppose,” he said, “that a hostile person, let’s call him Ali AlQaida, is hired by one of the large automation companies to work in their Engineering Center in, say, Kazakhstan. Ali is doing remote optimization of a refinery in Houston, and he’s on the overnight shift because of time zones. Ali records good, stable plant readings using the simulator at the plant, and then one night substitutes the recorded values for the actual current values, including the Safety Instrumented System which he then screws up so that the plant blows up at 8:30 AM during shift change.

“That’s my nightmare.” Adamski didn’t live to see his nightmare become horribly possible, but it has.

And still there is a strange reluctance to act to protect plants and the electric grid from danger.

Standards, Training and the Automation Federation

Dutch professor Andrew S. Tanenbaum famously said, “The nice thing about standards is that there are so many to choose from.”

With industrial control security issues being disparate from industry to industry, this has caused a multiplicity of standards, from the NERC CIPs (which do not even cover the distribution system in the grid) to the ISA99/IEC62443 standards, to the new UL Industrial Control System standards that have just been launched.

“And if you don’t like any of them,” Tanenbaum went

Industrial Control System Security in the Age of the Industrial Internet of Things (continued)

on, “you can just wait for next year’s model.”

Training is lagging far behind even the standards-making process, and certainly lagging behind the hackers’ ability to penetrate industrial control systems. None of the training and certification models currently have an emphasis on the sensor end of the network, and most are pretty rudimentary as far as OT is concerned.

I pointed out to Marty Edwards that the Automation Federation is just such a place where we could have a standards clearing house, compliance and training organization for global industrial control system cyber security. He agreed, and said that the Automation Federation, under his direction, might well move in that direction.

A Safe Plant Must Also Be a Secure Plant

As early as 2004, myself and several other cyber experts, such as Kevin Staggs of Honeywell, Eric Byres, then the inventor of Tofino, and John Cusimano, then of Siemens and now of AE Solutions, started to point out that in order for a plant to be judged safe according to the standards for safety instrumented systems, it needed to be cyber secure as well. This is still true, and there is an effort to bring together safety and security in standards, but most plant managements still don’t realize the critical importance of this concept.

Compelling Performance, Not Just Compliance

In last month’s issue, Joy Ward suggested a mechanism for why people continue to whistle past the cyber security graveyard. She drew on her background as a well-respected qualitative market researcher to talk about the motivators and barriers that combine to produce action or inaction on a specific issue.



Spitzer and Boyes’ Joy Ward

She noted that nobody has done any qualitative research on this subject, and she reminds cyber security professionals who complain to the INSIDER that they just don’t understand why people aren’t more concerned about their plant’s vulnerability, and the huge losses that could result from a successful attack, that if they don’t know what the barriers

are, they can’t design motivators to overcome them.

“I’d love to design a study that would answer those questions,” she says, “because I live near critical infrastructure too.”

Many industries have taken the road they took for environmental regulations: legal compliance. The NERC CIPs, as Joe Weiss points out, have been carefully crafted for easy and inexpensive compliance, not for increased security and safety. This again is Richard Clarke’s “satisficing” at work.

Weiss, Edwards, myself, and over two dozen cyber security professionals I’ve talked to over the past year, all believe that a major destructive event will have to happen before plants act substantively in their own defense.

What can we do? Well, first we can do the research Joy Ward wants, to figure out what the motivators need to be. We need to start educating cyber security professionals about industrial sensors and what their data means. We need to start educating insurance auditors about the importance of security audits in addition to the safety audits they are already doing.

We’ve just had an example, at Arkema in Crosby, TX, of what can happen when a natural disaster turns off the sensors and control system. We’ve just had an example, at Merck, of how much can be lost by a cyber attack on a manufacturing system. We’ve seen that nationstate hackers are actively attempting to control critical infrastructure.

So are we just going to wait for a big bang?

Or are we going to do the qualitative research necessary to produce motivators that will drive companies to spend the time, talent and money necessary to secure their systems, and produce the training and standards needed to help them do that?

The INSIDER recommends that we do the research and avoid the big bang entirely, if we can.

The *INSIDER*'s August 2017 Roundup

What's Going On With ISA???

ISA has announced the firing of Pat Gouhin. I suppose that if you weren't in the know, this will come as a huge surprise. I heard about it a few days before it happened, and was sworn to secrecy. Now the announcement has been made:

International Society of Automation Plans for New Leadership of Professional Staff

Research Triangle Park, NC (21 August 2017) – The International Society of Automation (ISA) announced today that Executive Director and CEO, Patrick Gouhin, will be stepping down. ISA's President, Steve Pflantz, announced that a Search Committee will be formed in the immediate future to identify Mr. Gouhin's successor. The selection and announcement of a new Executive Director are expected to occur in the months ahead. Peggie W. Koon, Ph.D., CEO & Founder of Leading Change, LLC, will serve as Interim Executive Director.



Fired ED/CEO Pat Gouhin



ISA President Steve Pflantz

"Pat has been our Executive Director since 2006 and has been a dedicated employee of ISA," Pflantz said. "Under Pat's leadership, ISA has progressed on many fronts. We will continue to ensure ISA's long-term vitality as we continue our commitment to advance the profession of Automation. The Board is committed to the strategy work that has been done thus far and is grateful for Pat's leadership in bringing us to this point."

"This is an exciting time in the history of ISA, and I am proud of what we have achieved and the work we are doing," Gouhin said. "A strong foundation has been laid based on the effort of many passionate volunteer leaders and a wonderfully dedicated staff team that will allow the next Executive Director to hit the ground running."

During his 11+-year tenure at ISA, Gouhin has overseen many significant milestones in the Society's history, including the expansion of ISA's brand family to include the founding of The Automation Federation and the Automation Standards Compliance Institute, and the acquisition of digital media powerhouse Automation.com. The world's only consensus standard for industrial cybersecurity, IEC 62443, was also developed and expanded under his tenure.

Before joining ISA, Gouhin served as the Chief Operating Officer of the American Institute of Aeronautics and Astronautics (AIAA). He also served as the first Vice President of Operations and Technology Transfer for the National Institute of Aerospace (NIA) at Langley Research

Center, a start-up resulting from \$69 million government contract award to build a world-class research and education institute.

Interim Executive Director Dr. Koon's experience and expertise lies in strategy development and execution, leadership coaching, and change management. Dr. Koon is the former Vice President of Audience for the Augusta Chronicle/TAC Media, Morris Communications, LLC. She has over 25 years of experience in IT, process control, and process automation for both discrete and continuous process industries. She was a General Motors Scholar, earning a B.A. degree in Mathematics from Smith College. She also completed 2 years of graduate studies in Industrial and Systems Engineering as a General Motors Graduate Fellow at the Georgia Institute of Technology, and she has a Ph.D. in Management Information Systems from Kennedy Western University.

In addition to her experience managing strategic change, Dr. Koon has also been a member and leader at ISA for more than 20 years. She has held a variety of



Interim Executive Director Dr. Peggie Koon

The INSIDER's August 2017 Roundup (continued)

prominent roles in the Society, including Society President (2014), Chair of the Automation Federation (2015), member of the ISA Executive Board (2016), and Chair of Workforce Development for the Automation Federation (2016).

Lots of familiar faces are no longer there, not just Gouhin. Highly respected events manager Rodney Jones was apparently fired without notice before Gouhin left. Deb Eby, who secretly ran ISA for more years than I care to admit, retired in July, as did Susan Colwell, the Publisher of ISA Books, who announced suddenly she was moving on.

I have also heard rumors that there is significant resistance to Peggy Koon's appointment as interim Executive Director. Most of the resistance appears to center on her color rather than her accomplishments, which are many and mighty. The resistance appears to be coming from the same group who didn't like it when she was ISA president.

What the heck is going on here?

From the outside, it looked like ISA had finally stabilized after thirty years of volunteer vs volunteer and volunteer vs staff infighting. Now it is just as big a mess as when I was on the Executive Board more years ago than I want to count. Did Gouhin lose his mind? The stories about his last few months in office are very strange and don't reflect the Pat Gouhin I've come to know.

And there's the rumbling animosity over the hiring of Marty Edwards, formerly head of ICS-CERT at the Department of Homeland Security, and a major ICS cyber security expert to be Executive Director of the Automation Federation. Some members of the staff appear to be jealous of the salary supposedly paid to Edwards, but frankly I doubt he got much more than he was making at DHS.

Edwards is a fantastic hire. He will do a terrific job of focusing and directing the Automation Federation into some of the most critical areas in automation: workforce development, cyber security standards, and especially workforce training for cyber security. This is a huge opportunity for ISA and the Automation Federation, and may actually make the Automation Federation self sufficient.

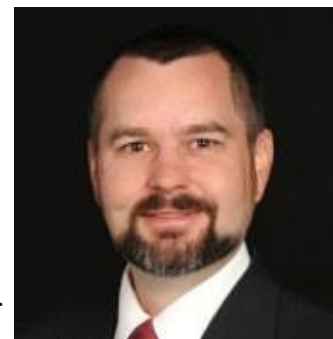
The Automation Federation could be a clearinghouse for international standards for industrial control system cyber security, and the training that goes with them, and the workforce development standards that could generate that training. There is no other agency in the world with the

ability to do this, and the positioning to do it, and the track record to do it.

But none of this is going to happen if the Executive Board and Senior Staff degenerate into name calling and game playing again. This happened before, twice. It took a series of good ISA presidents and Pat Gouhin ten years to straighten it out the last time. Looks like we're back where we were again.

ISA is in trouble, and we all need to rally round.

As for me, I'm used to being kicked. My blogs on this subject caused the "automation curtain" to fall. Almost no one on staff or on the Executive Board, including long time personal friends, will talk to me, about anything. This is a game ISA plays a lot: it's called shoot the messenger. It's okay, folks. I got shot the last time the Executive Director got fired. In fact, the then-Interim Executive Director, Bob Ives, threatened to sue me and my then soon-to-be employer, Putman Media, if I went to work for them. Nothing ever happened but I stayed away from ISA for years. So I feel bad about my friends, but I care more about the truth and ISA.



Marty Edwards, new Executive Director of the Automation Federation

Professor Graham Machin is Next InstMC President

In a much less angst-ridden change of leadership, the Institute of Measurement and Control (InstMC) in the UK has announced that The next President of The Institute of Measurement and Control will be Prof Graham Machin. Graham takes office in January 2018, succeeding Prof Sarah Spurgeon.

Graham is a Fellow of the Institute of Measurement and Control and a Chartered Engineer. He is a leading international expert in thermometry and is the science area leader of the NPL Temperature and Humidity Group. He currently holds visiting professorships at the University of Valladolid, University of South Wales and the University of Strathclyde. In October 2012, he was awarded the InstMC Callendar Medal award for improvements to the state of the art in temperature measurement. In 2017, Graham was awarded a Chinese Academy of Sciences Fellowship, in recognition of his world-leading position in and decadal contributions to the science of thermome-

The INSIDER's August 2017 Roundup (continued)

try.

Graham has a BSc and DSc from Birmingham University and a DPhil from Oxford University. He has published more than 200 technical papers and given numerous talks on temperature related topics.

As a Fellow of InstMC, I would like to offer my own congratulations to Professor Machin, and to the Institute for a very welcome choice.

—Walt Boyes



Professor Graham Machin, next InstMC President

South Africa lags in the great data race, but there's hope

By Steven Meyer, editor—SA Instrumentation & Control

“Organisations which fail to embrace the initiative of Industrie 4.0 risk obsolescence,” warned speakers at the recent Connected Industries Conference at The Dome in Randburg.

Keynote presenter Michael Ziesemer, chairperson of the German Electrical & Electronic Association (ZVEI), predicted that companies which did not adopt the ideas of the fourth industrial revolution would soon be overtaken by them. As a stark reminder of the



Michael Ziesemer

speed at which this can happen he asked delegates to consider how, in the hospitality sector, most hotel chains have dropped off the first page of Google search in favour of the numerous Internet-based booking services. In less than a decade, digitisation has robbed the hotel chains of their direct relationship with customers and placed it squarely in

the hands of a new owner – the ‘Where-should-I-stay-tonight’ app.

Fellow keynote and ZVEI board member, Dr Gunther Kegel, reinforced the urgency as he explained how survival in the modern era depends on smarter business and production processes, smarter supply chain collaboration and smarter products – Industrie 4.0 in a nutshell.



Dr. Gunther Kegel

While there is now little doubt that these ideas offer significant opportunities for manufacturing efficiency in the fully developed economies of Western Europe, the key question raised by the Connected Industries Conference is: “How effectively can they be applied in the emerging economies of Africa?”

SAIMC president Oratile Sematle put the conundrum nicely into context.



The paradox is that most

Oratile Sematle— SAIMC President

African societies have yet to experience the benefits of the second industrial revolution, but they are unlikely to remain sustainable unless they now find a way to embrace the fourth one.

The good news is that Industrie 4.0 can provide ways to leapfrog ahead.

But it will not happen without collaboration. What hit home in every conference session which I attended, is that the success of any digital leapfrogging endeavour in South Africa is heavily dependent on the future levels of cooperation between industry, labour, government and education.

So how should the stakeholders interact?

The DTI's Nigel Gwynne-Evans explained during a panel discussion that while government is supportive, it is only just beginning to get to grips with the implications of Industrie 4.0. What was encouraging to hear is that a

The INSIDER's August 2017 Roundup (continued)

new unit has been formed to investigate how incentives might be used to speed things along, much as they did so successfully in the automotive sector some years ago.



Nigel Gwynne-Evans

This is a step in the right direction. What South Africa's economy desperately needs is growth in the SME sector. Big business will adapt to whatever regulatory or economic environment it is faced with – big business is very, very good at doing this. What big business cannot do alone though, nor should it be expected to, is provide a solution to an unemployment problem the size of the one currently faced by South Africa. However, with the right incentives in place and the technologies of Industrie 4.0 to connect a suitably approved SME network into the big business supply chain, plus a little judicious foreign direct investment, who knows what might be possible.

Gwynne-Evans touched on the subject again at the conference's highly successful gala dinner. He stressed the importance of public/private sector partnerships as a key driver for local industrial growth, using the technologies of Industrie 4.0. Acting German ambassador Klaus Streicher explained to delegates and VIP dinner guests how Germany will present a recommendation for 'shaping a new digital world' at an upcoming G20 meeting. His message was clear: there should be unprecedented collaboration on digitisation in order that its benefits are as widely shared as possible.

The Connected Industries Conference did exactly what it was designed to do – it started a dialogue. It showed that while South Africa currently lags behind the developed manufacturing world in the sophistication of its digitisation efforts, it has the necessary infrastructure and skills to catch up. What works in Germany though is not necessarily guaranteed to work in South Africa due to the vastly different population demographics and more commodity-based economy. South Africa has a unique set of problems for which it must find a unique set of solutions. But, if we are prepared to work together and listen, then we just might "Get by with a little help from our friends."

Time-sensitive networking is not another fieldbus

Martin Rostan explains time-sensitive networking and discusses the advantages and disadvantages in an industrial automation context.

By Steven Meyer, editor, SA Instrumentation and Control.



Martin Rostan

Martin Rostan, executive director of the EtherCAT Technology Group, was recently in country to give a presentation at the Connected Industries Conference. He took a timeout to chat to SA Instrumentation and Control about an Ethernet layer 2 concept that is beginning to capture interest in the automation community – time-sensitive networking

(TSN).

Origins in the audio/video industry

TSN has its roots in a model pursued by the audio/video industry known as audio video bridging (AVB). Essentially, AVB is comprised of extensions to the IEEE802.1 specifications to enable networks such as Ethernet to stream time synchronised A/V data. The name TSN was adopted when the industrial automation industry, the telecommunication industry and the automotive industry got on board and the AVB task group widened its focus.

Within an Ethernet network, the TSN extensions help differentiate real-time data streams from the non real-time traffic – like sending a file to a printer – that can also flow through the network. All based on an industry standard approach, it allows for plug-and-play communication between systems from multiple vendors. AVB/TSN was developed to enable synchronized playback of audio and video data on different devices – in the automotive case these could be backseat monitors, amplifiers and speakers – using standardized IEEE 802 Ethernet.

"TSN is the extension of these concepts under the charter of the TSN Task Group, which aims to guarantee deterministic communication via Ethernet through low packet latency, low delay variation and low packet loss," explains Rostan. "But what one must keep in mind is that TSN cannot be considered another fieldbus because

The INSIDER's August 2017 Roundup (continued)

it does not provide an application layer.”

TSN is a toolbox of functionality

TSN is not a single technology for deterministic communication over Ethernet; rather, it is a set of IEEE 802.1 standards that extend the functionality of Ethernet networks to enable the coexistence of real-time (deterministic) and non-real-time data communication on the same network, while supporting fault-tolerance and bandwidth preservation.

“TSN is not a technology per se,” explains Rostan. “Rather it is a toolbox of standards that the TSN Task Group is in the process of developing. Some of these are almost complete and others are still in the early phases of definition.”

In other words, TSN is a suite of different extensions to the IEEE802.1 standard with some elements completely defined and ready for use, while others are still in the early stages of development.

So which features should I choose?

Rostan believes that the answer to this does not lie with any individual control system or network designer, but that these decisions will be taken by technology groups and associations – he cites Profibus & Profinet International as an example – which will choose the set of TSN features that they believe will best support the next generation of their Ethernet-based fieldbus offerings, in this case Profinet.

“What one must always remember,” emphasises Rostan, “is that while TSN adds determinism to standard Ethernet, it does not make the cycle times any faster. To improve the speed, you still need to migrate to a faster Ethernet backbone, 1 GB for instance, and then enable the TSN functionality that you require.”

Advantages and disadvantages

“The TSN standards aim to define a method for the transmission of time-synchronised data over a standard Ethernet network,” says Rostan. “Once this is in place then it can be built into the next generation of Ethernet chips, which will eliminate the need for most of the proprietary solutions currently required to solve the latency and clock synchronisation problems.”

In practical terms this means that a drive could now be controlled using standard (TSN-enabled) Ethernet switches, which was not possible before due to the unpredictable latency and other timing related issues. According to Rostan, sub 500-microsecond cycle times are achievable using these techniques on a 1 GB Ethernet backbone. This is

more than adequate for most of today's factory automation and motion control applications, and TSN will make it achievable using commodity Ethernet chipsets.

Rostan believes that one of the biggest disadvantages at the moment is the lack of maturity of the technology. Even though there is enough of the functionality complete now to demonstrate Ethernet devices with basic TSN functionality, he believes it will be at least another three years before all the current development within the TSN Task Group is complete and five years before the results are widespread and available in the market. “This is potentially going to hold up the decision making processes within those fieldbus organisation that are looking to incorporate TSN functionality into their Ethernet-based standards,” he adds.

TSN in manufacturing

TSN is seen by many as the basis of the network infrastructure that will support the IIoT revolution. “To a certain extent this is true,” says Rostan. “But before that becomes a reality there is still a lot of work to be done.

“Firstly, the projects being undertaken by the TSN Task Group are all at different stages of maturity. This means that while there is already enough in place to demonstrate, and maybe even implement, the deterministic capability of the architecture, we are a long way from being in a position to finalise the design of a standardised TSN chipset, let alone the configuration tools that will be required to setup the networks.

“Secondly, we must remember that TSN is an extension of the capabilities of a standard Ethernet network. In a manufacturing context this means that real-time deterministic process control data will be mixed-in with the more traditional data found in manufacturing applications. Even though the technology will be capable of doing this very effectively once the chipsets become commercially affordable, it is unlikely to become a reality until the IT/OT convergence has matured significantly from where it is today.”

Rostan stresses again that since TSN is not in itself a fieldbus, it is never going to take the place of one. He sees the role of TSN as either an extension of the capability of an existing Ethernet-based field bus, Profinet for instance, or as a deterministic Ethernet technology for architectures working one layer above a traditional deterministic fieldbus.

He cites an EtherCAT example (he is after all the head

The *INSIDER*'s August 2017 Roundup (continued)

of the EtherCAT Technology Group). The scenario is a server in the control room i.e. a clean temperature controlled environment. This computer is running a soft PLC, which is remotely controlling a group of robots on the factory floor through a TSN backbone linking all the EtherCAT segments that form the control layers of the individual robots.

The value added by TSN here is the ability to setup real-time (deterministic) control via the plant network for a group of robots working together on a task – a synchronous network of robots in other words.

The TSN-enabled network does not challenge EtherCAT's microsecond on-the-fly processing capability. It is the level above that where Rostan sees TSN adding value in the future, which is why the EtherCAT Technology Group is an active participant in the TSN Working Groups today.

What became obvious during the discussion with Rostan is that TSN has the potential to add substantial value to the Ethernet-based networks that will dominate the IIoT era. But, as with the IIoT itself, the TSN functionality will only add value in those projects that have been intelligently conceived, analysed and understood. In the future it may extend the capability of an existing fieldbus network, but it will not replace it – TSN is not another fieldbus.

Fluke expands the Condition Monitoring system to include Thermal Monitoring

Maintenance managers can now visually inspect critical equipment remotely to build a real-time picture of an asset's condition

Fluke Corp. has expanded the capabilities of its Condition Monitoring system to include thermal monitoring with the addition of the new Fluke® 3550 FC Thermal Imaging Sensor. Maintenance managers can now collect a more comprehensive variety of key-indicator data — thermal imaging, voltage, current, temperature, and power — on critical equipment to build a real-time picture of an asset's condition. With the right mix of data all in one place, managers can implement planned maintenance and decrease the frequency of preventive rounds.

Fluke Condition Monitoring is a cloud-

based software platform in combination with rugged electrical, temperature, and power quality monitoring sensors to support condition-based maintenance programs. The software aggregates data pooling measurements from Fluke wireless tools with real-time condition monitoring data and historical records for a complete picture of asset health.

Fluke Condition Monitoring gives maintenance teams a practical, scalable system that allows them to visualize live readings. This accelerates issue detection, analysis, and resolution to optimize the lifespan of critical equipment without invasive retrofits or specialized training. Alarms can be set to notify technicians via their mobile phones when specific measurement thresholds have been hit, allowing teams to take immediate action to resolve issues.

Visually inspect thermal patterns on multiple assets

The new Fluke 3550 FC Thermal Imaging Sensor is the first thermal imaging condition monitoring sensor to visualize thermal patterns on multiple assets. Alarms can be set to notify the user when the center-point temperature exceeds preset parameters. The sensor communicates directly with the Fluke Connect® Cloud for continuous streaming of thermal images, enabling maintenance managers to detect problems by visually inspecting sequential thermal images remotely.

The compact sensor can be placed in areas that are dangerous or difficult to reach, reducing the risk to technicians. Images and measurements can be viewed on handheld devices or computers allowing anytime access to key data to conduct smarter evaluations.

The sensor can operate in high-performance mode to capture the most accurate images over a 11-14 hour period or in energy-saving mode to capture sequential images for up to three days. The ac power adapter can also be used for longer-term continuous monitoring. Equipment data can be viewed in multiple graphs, including center point temperature data, for more comprehensive evaluations of asset health.



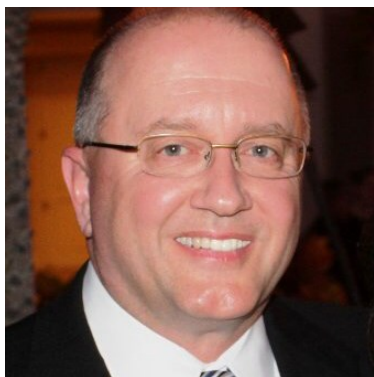
Fluke 3550 with an image capture of two motors

The INSIDER's August 2017 Roundup (continued)

ABB opens new Collaborative Operations Center for Pulp & Paper in Westerville, OH

In a move that seems odd, since the pulp and paper industry in the US is hardly booming, ABB has decided to open a new Collaborative Operations Center for Pulp and Paper in the US. The new center will function as the central focal point for resources and for systems that are equipped with ABB technology. It will leverage ABB's extensive pulp & paper expertise to provide true data-driven solutions for its customers by providing remote connectivity, secure access to process performance information, and technical support. ABB must be expecting maintenance and support to be more of a sure sale than new equipment has been.

Countless sensors and operation-critical systems transmit data on the health and performance of paper machines to the centers, where sophisticated software performs advanced data analytics on a 24/7 basis. The insights gained will allow engineers to quickly diagnose potential issues, advise on preventive maintenance or suggest measures to improve performance. ABB experts and customers work in close collaboration, taking data-driven decisions in real time that increase operational performance and business profitability.



ABB's Jim Fisher

"The new center demonstrates our leadership in delivering the real benefits of big data to our customers, changing insights into actions to improve their processes," says Jim Fisher, Global Product Group Manager for Pulp and Paper. "ABB remotely monitors and provides real-time support to close to 150 mills worldwide today, and we are expecting that number to rise with this new offering."

Later this year, ABB will open two additional centers with focus on the pulp and paper industry in Helsinki (Finland) and Singapore, leveraging the "follow the sun" principle to support customers anywhere in the world.

ABB Collaborative Operations is a true Internet-of-Things application and is part of the company's portfolio of ABB Ability with industry-leading digital solutions. Collaborative Operations provides performance management, remote monitoring and preventive analysis technologies to ensure security, and improve efficiency and productivity in various industries. ABB Collaborative Operations Centers connects people in enterprise-wide production facilities and headquarters to ABB's technology and expertise.

ABB Measurement & Analytics welcomes Nick Grant as new head of Americas Hub

Nick Grant joins ABB as Group Vice President and head of Business Unit Measurement & Analytics' Americas Hub responsible for North & South America, bringing with him over 20 years of senior management experience in the instrumentation and analyzer business. He will be responsible for building ABB's Measurement & Analytics business in North and South America.



ABB's Nick Grant

"I am extremely pleased to welcome Nick to ABB and the Measurement & Analytics management team. The Americas Hub for our Business Unit is an extremely important part of our global growth strategy and Nick brings valuable experience and an exceptional track record to this role," says Ian Rennie, Managing Director, ABB Measurement & Analytics

Nick joins ABB from Ametek where he served as Corporate Vice President and General Manager of their Materials Analysis Division. He brings over 20 years of experience in P&L management, strategy creation, sales, marketing, operations and business development. Prior to Ametek, he worked for Emerson for 16 years holding a number of senior roles across the corporation, including leading Rosemount's global temperature business and being the head of Process Management's strategic planning and business development group. Nick has a Bachelor of Science in physics from Northern Kentucky University and an executive MBA from Xavier University.

In this role, Nick will be responsible for developing and executing ABB's Measurement & Analytics Next Level growth strategy for their business in the Americas Hub that comprises of North and South America. Local Business Unit Managers for Measurement & Analytics in all North & South America countries will report directly to Nick. He will report to Ian Rennie, Managing Director, BU Measurement & Analytics, and be based in Warminster, Pennsylvania.

The INSIDER's August 2017 Roundup (continued)

Yokogawa acquires FluidCom chemical injection valve technology

by Nick Denbow (originally published on @ProcessingTalk blog)

Yokogawa has announced the acquisition of TechInvent2 AS, a Norwegian enterprise that holds the rights to FluidCom, a chemical injection metering valve (CIMV). The FluidCom CIMV prevents blockages and corrosion in oil wells, pipelines, and other facilities and employs a patented technology for thermal control. It incorporates the functions of a mass flowmeter, control valve, and valve controller and has very few moving parts. FluidCom systems have already been delivered to several international oil and gas majors.

With TechInvent2 joining the Yokogawa Group, Yokogawa will now target delivery of this solution to the oil and gas upstream and midstream sectors, thereby helping to improve operational efficiency, reduce operational costs, and enhance health, safety and the environment (HSE).

Background Information

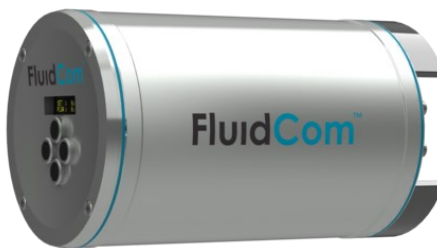
Based on its Transformation 2017 mid-term business plan, Yokogawa will continue to focus on the oil and gas industries, and will strive to strengthen its solutions targeting the upstream and midstream sectors, in addition to its forte downstream sector businesses.

Following its April 2016 acquisition of KBC Advanced Technologies, a provider of consulting services that are based on its own advanced oil and gas simulation technologies, the company has been striving to work with its customers to create value through the provision of solutions that address every aspect of their business activities. At oil wells and pipelines, efforts to ensure a secure oil flow path (flow assurance) play an important role in maintaining production efficiency. The adherence of various chemical substances to the inside walls of a pipe can reduce its internal diameter and causes corrosion. To prevent the accumulation of substances and corrosion, certain chemicals must be injected in the pipes. Improving the efficiency of this process is a major challenge in the upstream and midstream sectors.

The FluidCom CIMV

Chemical injection valves have traditionally been manually operated in the upstream sector, although there are cases where chemical injection has been automated using an actuated solution. In the former case, the valves must be frequently opened, closed, and adjusted by plant personnel. This is costly as it necessitates the hiring of additional staff, and it is work that must be done under very harsh environmental conditions in the field.

It is also a well-known problem that inaccurate and unstable dosing of chemicals leads to additional operational costs and challenges with specific processes. To address and resolve such problems, there is an increasing demand for integrated automatic injection solutions that perform stably and offer a high level of precision in the dosing. The FluidCom CIMV has a unique design which is based on a patented technology, providing integrated flow control and metering using a unique combination of material and thermal effects.



FluidCom CIMV

FluidCom is a fully automated and reliable device with a simple design that performs autonomous valve control and continuous flow metering. The device is able to stably inject chemicals in the required small

amounts. It has few moving parts and has proven to be an accurate, reliable solution for the control of chemical injection applications. No regular maintenance is required and remote control features are provided.

The device features a self-cleaning mechanism that reduces maintenance workload, and the automatic injection of chemicals in the correct amounts eliminates the need for manual interventions by plant operators and maintenance workers, thereby enabling personnel to lessen their exposure to harsh environmental conditions in the field.

Chemical injection valves have traditionally been operated as manual systems in the upstream sector under harsh conditions. The FluidCom can automate chemical injection operation and reduce times that plant operators and maintenance workers go to field and operate in harsh environments. So using FluidCom improves healthy and safety.

FluidCom is also a valuable solution for downstream operations, where corrosion prevention is always a pressing concern. An ISA100 Wireless version is planned. The ISA100 Wireless technology is based on the ISA100.11a standard. It includes ISA100.11a-2011 communications, an application layer with process control industry standard objects, device descriptions and capabilities, a gateway interface, infrared provisioning, and a backbone router.

Commenting on the acquisition of this company, Shigeyoshi Uehara, head of the Yokogawa IA Products and Service Business Headquarters, said: "FluidCom will improve flow assurance, which is a key concern of our customers in the oil and gas industry, and it will make a major contribution to their operations by helping them not only improve production efficiency and reduce operational costs, but also enhance

The INSIDER's August 2017 Roundup (continued)

HSE. The combination of FluidCom, KBC simulation technology, and Yokogawa field devices will allow us to expand the range of our upstream and midstream solutions and enable the delivery of value in new ways to our customers.”

About TechInvent2

TechInvent2 has been a fully owned subsidiary of TechInvent AS, a Stavanger, Norway-based company founded in 2008. TechInvent is owned by the founder and CEO Alf Egil Stensen, the venture capital firm Statoil Technology Invest AS, Aarbakke Innovation AS, and Ipark AS. The company has been supplying its FluidCom chemical injection technology to major oil companies since 2016. Alf Egil Stensen will continue as CEO of the company now that it is part of Yokogawa.

Opto 22 IoT Certified System Integrators Bridge the OT/IT Gap

Opto 22's IoT Certified System Integrators combine domain expertise in both Operational Technology and Information Technology, to help organizations more easily deploy industrial Internet of Things applications.

Opto 22 announced their IoT Certification program for authorized System Integrators, called *OptoPartners*. This program addresses a specific need as Internet of Things (IoT), Industrial Internet of Things (IIoT), or Industry 4.0 applications and projects proliferate.

The potential benefits of IIoT applications are enormous, from predicting system failures to making processes more efficient to reducing costs. However, to realize these benefits, information technology (IT) and operations technology (OT) teams must work together to leverage and apply each other's technology and skillsets.

“At ACS, we recognized that having the skills to get data where it needs to go was going to be necessary for our growth as a business,” says Dave Pilliod, President of IoT Certified OptoPartner Advanced Control Solutions. “With their mindset of multi-platform communications, Opto 22 has provided the tools to enable us to have Operations and Information Technologies come together. It would be a disservice to our customers not to be as learned as possible on the technologies of today, even if they lie outside the traditional realm of automation.”

IT/OT convergence continues to be a challenge on both the technical and cultural fronts. In today's enterprise, a significant communication gap exists between OT and IT technologies. Each uses its own methods of connectivity, from the physical connectors and buses that data rides on, to the language each uses to convert bits and bytes into human readable and actionable information.

Opto 22 OptoPartners who carry the IoT Certification possess

the unique combination of skillsets in both the OT and IT domains. They have demonstrated proficiency in OT technologies such as sensors, instrumentation, controls, and automation as well as with IT technologies such as networking, databases, computing, data analytics, and cloud or edge IoT platforms.

With this holistic expertise, these IoT Certified OptoPartners are positioned to help customers achieve their IIoT goals using Opto 22's IoT-enabled automation platform—SNAP PAC System™ and *groov*®—plus connectivity tools such as Node-RED® and commercially available IT and IoT solutions.

“Today, knowledge in both Operations Technologies and Information Technologies is an absolute requirement for the networked and data-driven applications our customers demand,” says Todd Reynolds, President of IoT Certified OptoPartner Perceptive Controls. “As a result, we've staffed up and educated our team with the necessary skills from both camps. As a long-time Opto 22 systems integrator, we're pleased to see the updated OptoPartner program recognize our unique skill set with the new IoT Certification badge.”

Additionally, Opto 22 is part of the IoT ecosystems of three major IT companies: Dell® (IoT Solutions Partner), IBM® (Registered Business Partner- Ready for IBM Watson IoT) and AT&T®/ M2X (IoT Partner).

These relationships and the new network of IoT Certified system integrators will help customers more easily design, install, and commission their industrial IoT projects and quickly realize a return on their investment through increased business intelligence.

Schneider Electric Gets Significant Process Win

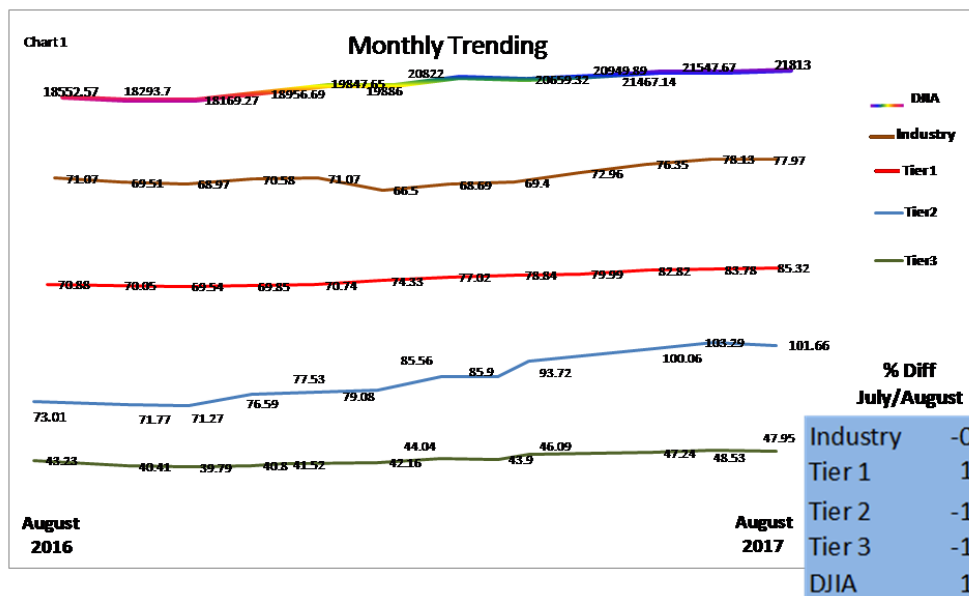
As another sign of the rebound of both the oil industry and Schneider Electric's flagship DCS, Schneider Electric has signed a contract to provide comprehensive process automation systems, solutions and services to Dangote Oil Refinery Ltd., a subsidiary of African business conglomerate Dangote Group.

Under the terms of the agreement, Schneider Electric will supply its EcoStruxure system architecture and platform, comprising its EcoStruxure Foxboro distributed control system, Triconex process safety solutions, PI-ONIR analytical fuels blending systems and a suite of SimSci and Wonderware software solutions, including its unified supply chain management and operations management software, to drive supply chain and operational efficiency, reliability and profitability improvements at Dangote's greenfield refinery in Lagos, Nigeria.

Nothing to Write Home About!

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Health Watch



The Leaders

This month, IDEC and Vishay Precision far outstripped other companies with double-digit growth.

IDEC – \$11.07 to \$17.12 EPS — that’s a 54.6% Increase since April and has been the Industry leader in June with 18% increase, and once again this month with 28% percent increase between July and August.

IDEC must be feeling the effect of their acquisition in April of APEM, a major manufacturer of HMIs, panels, and systems.

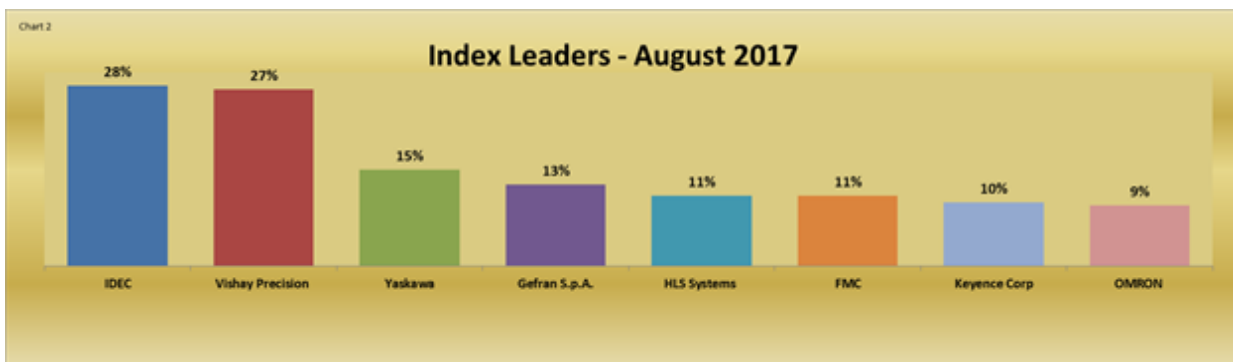
The industry overall held its own this month, but it performed slightly worse than the DJIA and the performance both is certainly nothing to write home about.

These numbers were pulled before the advent of monster hurricanes Harvey and Irma, and they don’t reflect any of the effects certain to be seen by the industrial process industries as a result of hurricane and flood damage.

One thing that’s certain, when a

hurricane hits an oil refinery or a chemical plant, the winner is the hurricane— and the automation suppliers who will have to jump through tight hoops to get new product to replace the damaged stuff, so that the plants can re-open and stop being a drain on the corporation.

“This acquisition is a major step for IDEC to establish solid foundations for global growth. It provides us with access to new customers, new markets, and greater range of products and services. Combining the two companies, we are a much bigger enterprise with a global reach. Together



Nothing to Write Home About! (continued)

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

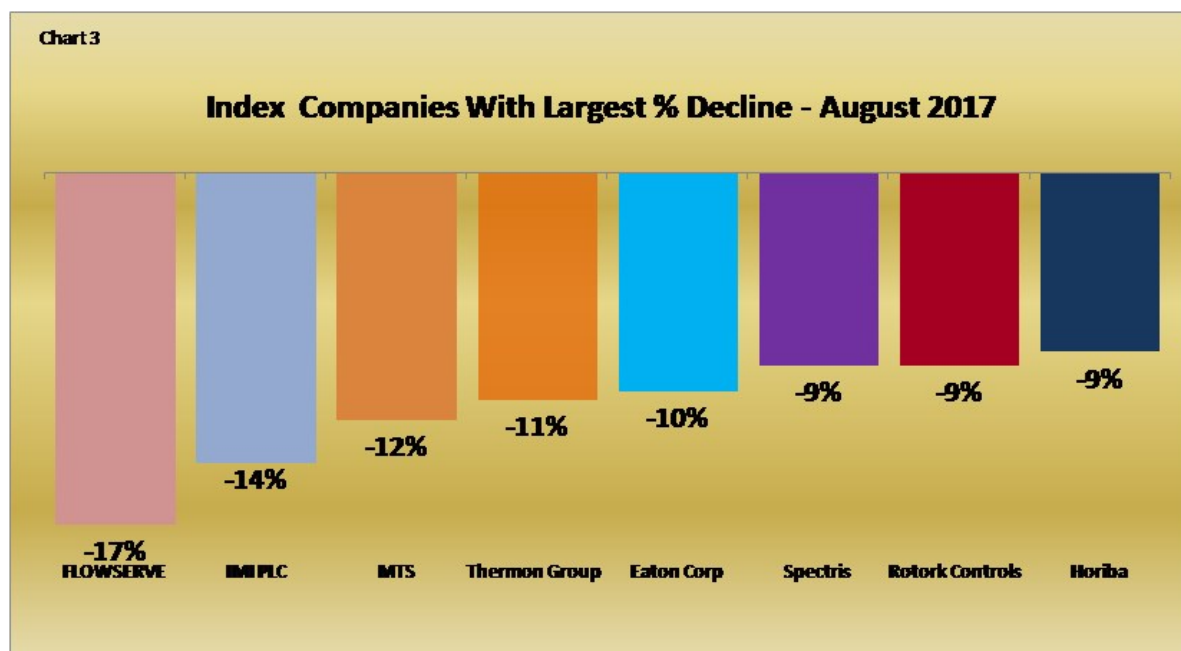
Health Watch

we have \$500 million sales, 3500 people worldwide, Sales subsidiaries in 15 countries and factories in 10 countries. Thanks to the complementary product offerings, business models and geographical presence of the two companies, we expect significant synergies as we combine the two companies together,” says Toshi K. Funaki, the President of IDEC.

Vishay Precision is doing it the old fashioned way, by producing good financial results. On a per-share basis, the Malvern, Pennsylvania-based company said it had profit of 27 cents. Earnings, adjusted for restructuring costs, came to 29 cents per share on second quarter profit of \$3.6 million on sales of \$62.3 million.

Those Not So Fortunate

Flowserve, at a decline of 17% is the winner of this month’s dubious achievement award. All of the decliners were victims of large declines for the month. Most of these companies will be grateful for the emergency business that the hurricane challenged industry will be forking over next month.



We will see what the long term effects of the hurricanes will be on the petrochemical sector, and the automation companies that serve it.

The short term should involve significant increases of business for companies manufacturing valves, transmitters, cable, conduit, pumps, motors, and anything else that will not fare well for being under water for several days to several weeks.

We expect that the hurricane-caused disasters will put a hold on the Industrial Internet of Things projects. We expect that the plants will feel that simply getting back on their feet and making product will be much more important than Industrie 4.0 for the medium term. We should expect a spike in good old fashioned instruments and controls sales and profit.



THE WAY I SEE IT

Editorial

The ICS Cyber Workforce— Where to Find It?

Around ten years ago, Joe Weiss and I tried to figure out how many competent ICS security professionals there were. After long argument, we concluded that there were about 100 people in the entire world who could successfully operate as cyber security professionals with Industrial Control System experience.

A week or so ago, Joe and I revisited the issue. Yes, there have been improvements. There are now significant numbers of people who have certifications in Industrial Control System Security. But how good are they really?

Because it is a relatively new profession, many of the practitioners are young, and do not have much experience doing anything other than working with computers.

Joe pointed out, and I completely agree with him, that this is one of the reasons why ICS security, just like IT security, is computer and network-centric.

Network visibility tools give you visibility to the edge of the network— that is, to the

Comments? Talk to me!
waltboyes@spitzerandboyes.com

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

controller. None of them gives you visibility to the sensor and its input. This is not good, because the control system depends on the accuracy and veracity of the sensors to which it is connected. It has no way of determining if the sensors have been spoofed, or are being bypassed, and false information being injected into the controllers. So the

The Automation Federation could be developing workforce specifications, providing globally-recognized testing, and working to develop a significant cadre of senior ICS cyber security professionals with core competency in OT and plant operations underlying their security knowledge and experience.

only things ICS security professionals regularly look at are the networks and the devices connected to them.

In addition to this blind spot, new ICS professionals are most likely from an IT background, not an OT background. They don't understand what the data they are guarding means. This, of course, allows any smart hacker a route into the control system where the security professionals aren't looking.

We concluded that there are not many more fully-trained ICS cyber security professionals at a senior level than there were when we

first counted them.

What to do? What to do?

One of the things we can do is to realize that we have a hidden gem in the Automation Federation.

Newly taken over by Marty Edwards, former head of ICS-CERT for the United States, the

Automation Federation is precisely situated at the junction where education, workforce development, and training come together.

This would be a good time for ISA, which owns and sponsors the Automation Federation, to take a good look at what the Federation could do for ICS Cyber Security and Workforce Development. The Automation Federation

could be developing workforce specifications, providing globally-recognized testing, and working to develop a significant cadre of senior ICS cyber security professionals with core competency in OT and plant operations underlying their security knowledge and experience.

This could also allow the Automation Federation to stand on its own, without being a drain on ISA itself.

ISA Executive Board: think about it!

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.



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: India's tryst with industrialization and its promising future

The world is getting ready to usher Industry 4.0, the fourth era of Industrialization, a trigger for enhancing the productivity and growth of manufacturing industries.

While for some countries, such as England, Germany, and the US, the industrial age began in the late 18th century, India had to wait for almost another 200 years to start traversing that path. It had to wait to attain its independence for starting on the journey of industrialization.

Making up for the time lost has not been easy, but the country has made tremendous progress since then. It can look back with satisfaction about the economic and industrial accomplishments it has achieved since 1947, the year of its independence. India can draw inspiration from its accomplishments in a short span of few decades and look forward to sustain the growth of the industrial sector in the years to come.

The country's accomplishments achieved during the last seven decades are very significant. Encouraged by these achievements, India has made ambitious plans to increase, by the mid of next decade, the manufacturing industry's share in its GDP to 25 percent from the present 15 percent, emerge a global manufacturing hub, remain one among the world's fastest growing large-sized economies, and expand further its economy.

Reports such as the World Economic Forum's "The world's 10 biggest economies in 2017," which identifies India as having emerged as the seventh largest economy in the world and the United Nations Industrial Development Organization's yearbook that says that India has become the sixth largest manufacturing

country in the world in the year 2015 supports such expectations.

Independent India's industrial policy initiatives

Driven by India's first Prime Minister Jawaharlal Nehru's beliefs that "no country can be politically and economically independent unless it is highly industrialized and has developed its resources to the utmost" and that the development of electric power industry is crucial for the country's economic devel-

"...no country can be politically and economically independent unless it is highly industrialized and has developed its resources to the utmost"

—Jawaharlal Nehru

opment, some of the independent India's initial policy initiatives were related to spurring the growth of the country's industries including the power sector.

Therefore, Independent India's first-government, enacted the Electricity (Supply) Act 1948 (ESA 1948) that provided an elaborate institutional frame work and financing norms for the performance of the electricity industry in the country and the Industrial Policy Resolution of 1948 (IPR 1948) that provided the basic guidelines for the manufacturing sector's development. Even though they have undergone revisions in subsequent years, the imprint of ESA 1948 and IPR 1948 on the India's industrial landscape remains strong.

IPR 1948 gave preeminence to State ownership. This approach, which gave a far bigger role for the government and little or no role for the private sector, was largely influenced on one hand by the government's primary policy decision to pursue the command & control and centrally planned socialistic pattern of economy.

Lack of necessary financial capital and infrastructure, industrial entrepreneurship and capabilities, and basic technology skills in the country also forced the government to adopt this economic development path for building

Rajabahadur V. Arcot: India's tryst with industrialization and its promising future (continued...)

the industrial base and establish government funded enterprises often referred to as public sector companies / units (PSU) or state owned enterprises (SOE).

IPR 1948 entrusted the government the exclusive responsibility to develop energy, railways, coal, iron and steel, ship-building, manufacture of telegraph, telephone, wireless apparatus, minerals & oils, and such other essential industries. Industries such as automobiles, tractors, and others that catered to the aspirational wants were allowed to be in the private sector, subject to government regulation and supervision.

The following examples show how backward the country was in 1947, the year of India's independence. India, with a population of around 400 million people, at the time of its independence had a total installed electric power generating capacity of mere 1,362 MW and two automobile companies that together annually produced a few thousand cars of models such as Morris and Fiat 1100, under licensing arrangements. The, electric power was available only in a few urban centers; rural areas and villages did not have electricity. The entire country had less than 100,000 telephone subscribers at the time of its independence!

Planned sector by sector approach

Guided by the 1948 industrial policy framework, India sought the technical and financial help of developed countries such as the US, UK, Germany, the erstwhile Soviet Union, and others to help it establish production facilities to make power plant equipment such as boilers and turbines, steel, drugs & pharmaceuticals, and such others.

In order to spur the growth of electric power industry and domestic availability of necessary equipment, the government established production facilities at Bhopal, Hyderabad, Trichy, and Hardwar to manufacture steam turbines, generators, steam boilers and associated equipment in collaboration with the technical and financial support of UK, erstwhile Czechoslovakia, and Soviet Union. These plants now form part of Bharat Heavy Electricals Limited, which was established in 1953. Integrated steel plants were established; the first one came up at Rourkela and the second one at Bhilai. These were followed by a third at Durgapur and fourth at Bokaro. While the Rourkela Steel Plant was built with West German collabora-

tion and inaugurated in 1959, the Bhilai plant, commissioned in the same year came up with the collaboration of Soviet Union. Durgapur and Bokaro plants, commissioned in 1965, were set up with the collaboration of British and Soviet Union respectively.

With regard to the drug and pharmaceutical industry, after the failure of its attempts to attract global pharmaceutical companies to establish production centers in the country, the government set up Hindustan Antibiotics in 1954 to produce antibiotic with the assistance of World Health Organization and UNICEF; and Indian Drugs and Pharmaceuticals Limited in 1961 with the support and assistance of the Soviet Union to produce antibiotics, synthetic drugs, and surgical instrument drugs.

In addition, the government also created a number of supportive research institutes under the guidance of the Indian Council of Medical Research and the Council of Scientific and Industrial Research. They played pivotal roles in the growth of the sector and relevant technological advancements in the country.

Even though at the time of the formulation of 1948 industrial policy framework, there was the realization about the need to ensure energy security, the government did not take proactive measures in developing the oil and gas industry. Private oil companies mainly carried out exploration of hydrocarbon resources of India; based on their assessment they concluded that major part of Indian sedimentary basin was unfit for development of oil and gas resources.

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



Rajabhadur V. Arcot: India's tryst with industrialization and its promising future (continued)

In 1955, the Government of India decided to take direct control to develop the oil and natural gas resources in the country.

With this objective, it set up the Oil and Natural Gas Directorate in 1955 with a nucleus of geoscientists from the geological survey of India and a year later the Directorate was expanded to become Oil and Natural Gas Commission with enhanced powers. Foreign experts from the US, West Germany, Romania and Soviet Union were invited to visit India and help the government with their expertise. Finally, the visiting Soviet experts drew up a detailed plan for carrying out geological and geophysical surveys and drilling operations.

The Oil and Natural Gas Commission was charged with the responsibility to plan, promote, organize and implement programs for development of Petroleum Resources and the production and sale of petroleum and petroleum products produced by it, and to perform such other functions as the Central Government may, from time to time, assign to it.

Since then, ONGC has played a major role in transforming the country's limited upstream sector into a large viable playing field. In early 70's, ONGC discovered the giant Bombay High oil field. This discovery, along with subsequent discoveries of huge oil and gas fields in Western offshore changed the oil scenario of the country.

Impressive achievements

Over the years, the country's industrial base overcame the inherent handicaps of a late starter and expanded. Recently, the installed capacity of electric power industry generation exceeded 330 GW; and India has emerged as the world's third largest producer and fourth largest consumer of electricity. Renewable power plants constitute almost 30 percent of total installed capacity. The electric power industry's growth prospects look highly promising. India has set an ambitious plan to add 175 GW of renewable energy generation capacity by 2022. The country aims to have 100 GW of solar power by 2022 along with 260 GW of thermal and nuclear generation and 62 GW of

Walt Boyes and the other INSIDER staff are available for speaking engagements, webinars, and workshops. Walt is a member of the Association of Professional Futurists, as well as an ISA Life Fellow and an IN-STMC Fellow in the UK. For information, contact Walt at +1 630-639-7090 or waltboyes@spitzerandboyes.com.

hydro generation capacity. Recently, India's Power Minister Piyush Goyal, speaking about the opportunities that India's power industry, highlighted that India would spend around US\$ 1 trillion by 2030 on ramping up its power infrastructure.

With India's last year steel production exceeding 100 MT India has emerged as the world's third-largest steel producer and the largest producer of sponge iron in the world in 2016. According to

Recently, India's Power Minister Piyush Goyal, speaking about the opportunities that India's power industry, highlighted that India would spend around US\$ 1 trillion by 2030 on ramping up its power infrastructure.

the recently released draft National Steel Policy 2017, crude steel production capacity will reach 300 MT by 2030-31 and per-capita consumption of steel rise to 158 kilograms of finished steel from the current level of 61 kilograms.

The Indian pharmaceuticals market is the third largest in terms of volume and fourteenth largest in terms of value and the demand is largely met through domestic production. India has emerged as the world's largest provider of generic drugs and ac-

counts for almost 20 per cent of global exports in terms of volume. According to available industry reports India's pharmaceutical exports stood at US\$ 16.4 billion in 2016 and are expected to reach US\$ 20 billion by 2020.

With the country not well endowed with oil and gas energy sources, India depends on imports to meet its energy needs. The country's energy import dependence continues to expand and according to reports India has surpassed Japan to become the third largest importer of crude. In order to balance its oil import bill, India exports petroleum products and for this purpose has built massive refining capacity in the country that is in excess of its needs; it has become a major refining hub and ranks fourth globally, with only the United States, China and Russia ahead, according to the International Energy Agency.

India's cement and automotive industries have also grown tremendously in recent years and what distinguishes them from other core industries, such as energy and power, is that their growth has been largely driven by non-state owned enterprises. India's cement industry, with nearly 400 MT of cement production capacity and accounting for 6.7 per cent of world's cement output, is the world's second largest cement producer and exports to around 30 countries across the globe. The cement production capacity, which in 1947 was only around 2 MT, is estimated to touch 550 MT by 2020.

The Indian automotive industry, presently contributing to almost 7 percent of the country's GDP, is vibrant and grown enormously in the last two decades. Recently the Society of Indian Automobile

Rajbahadur V. Arcot: India's tryst with industrialization and its promising future (continued...)

Manufacturers (SIAM) and the government unveiled the Automotive Mission Plan 2016-26 (AMP 2026). The plan aims to make the Indian automotive industry to expand from the present US\$ 74 billion to US\$ 260 billion to 300 billion, generate 65 million more jobs, and contribute over 12 percent to India's GDP.

Robust demand provides impetus for future growth

While many of the core industries, such as those described above, have also grown tremendously, India does not have strong a defense and semiconductor & electronics industry to meet its strategic needs. With domestic industrial infrastructure lacking design, engineering, technology and production capabilities, India largely depends on imports to meet its needs in both these sectors. As regards the defense industry, driven by neighboring adversaries' threats, India's spending on defense equipment is significant. According to reports based on World Bank statistics, India spends over 2 percent of the country's GDP. Similar is the case with regard to electronics industry. In the last 15 years, the import bill of electronics goods recorded a CAGR of 18.3 percent. If this trend is not reversed, industry reports estimate the electronics import bill will exceed US\$ 400 billion by 2022. This will completely distort the country's trade balance which is already negative and impede the country's economic growth plans and hence this option is unacceptable. This massive demand pull for both defense equipment and semiconductor & electronics will spur the growth of these industries and sheer market opportunities will attract the entry global players.

The industrial age began in India only a few decades ago and exciting days are ahead. It is young, energetic, and holds promise of a bright future. The country's economy is growing and its favorable demographic profile supports India's long term growth prospects. Presently, India is a supply-side constrained and domestic consumption-led economy.

As Indian economy grows and the country becomes more prosperous, the domestic consumption will expand. Any increase in consumption will result in boosting demand for almost everything and that will have a cascading effect on overall growth including the industrial sector.

The dawn of the fourth industrial era provides the country abundant opportunities to sail with the wind. While in certain industrial sectors, the country has made spectacular progress, the best is yet to come. Despite the growth of many industries, the per capita consumption of almost all consumables still remains very low compared to world average.

For example, per capita steel consumption in India is around 61 kg in 2014 against global average of 216.6 kg. In the case of cement, per capita is only 200 kg compared to world average, which stands at about 500 kg.

The country has just 15 cars per 1,000 people. China in comparison boasts of 60 per 1,000; in Brazil it is 200 and in the United States, 800. Compared to some of the developed countries of the world, India's per capita consumption of electricity which is little over 1010 kilowatt-hour

Spitzer and Boyes LLC offers unique services to high tech companies such as—

Mind of the Customer™ research, which can tell you what your customers really think, and what they really want, both in products and services.

Content Generation for high tech and automation companies. We have the research and experience to write in your words, for you, on the subjects you care most about, and are most valuable.

Strategic Research on Smart Manufacturing, Industry 4.0 and the Internet of Things, Cyber Security and other hot topics, to help you position your company properly for the years ahead.

Contact Walt Boyes for more information. +1 630 639 7090
waltboyes@spitzerandboyes.com

is a third of the world average and is just 7.5 percent that of USA and 6.6 percent of Canada.

India's per capita energy consumption is a third of the global average, according to the International Energy Agency's India Energy Outlook Report 2015.

Apart from building global sized industries in some sectors, it has made tremendous progress in improving manufacturing competitiveness.

Deloitte's Global Manufacturing Competitiveness Index 2016 states that India's competitiveness ranking "to improve from 11th in 2016 to the number five spot by 2020."

It further says that India along with Malaysia, Thailand, Indonesia, and Vietnam could possibly represent a "New China" in terms of low cost labor, agile manufacturing capabilities, favorable demographic profiles, market and economic growth, with their competitiveness ranking rising in the next five years.

India's industrial journey is all set to gather steam.