INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

VOLUME 19
NUMBER 11
ISSN2334-0789
November 2015

Inside this issue:

INSIDER HealthWatch
Who Are We Trying to Fool?!? Page 17

Rockwell Automation Week Sets Attendance Records	1
Petrobras' Pain, and the Ghost of the Chem Show	4
PAS, Bedrock and Statseeker: IT/OT Convergence Rolls On	8
Nick Denbow's Roundup: OE Monopoly Assurance 360 in NZ Profinet Interface/RED Alfa Laval Leader Retires New Partnerships -GE acquires Advantec -HPS partners UOP -GE Healthcare +Emerson ISA Food /Pharma in Eire ABB and CGM TDLAS analyzers from China China Wind Power in UK Changing shape of magazines Big Bender HON/Elster acquisition Yokogawa's Big Order E+H starts Open Integration partnership	10
The ARC Forum is Coming in February	18
The Way I See It: Editorial by Walt Boyes: The Internet of Things May Be the Internet of No Jobs	19
Rajabahadur V. Arcot: The Automation Industry's Growth, Opportunities and Challenges	20

Your key to the latest industrial automation and process control information

Cover Story: Rockwell Automation Week Sets Attendance Records

The largest gathering of automation professionals in North America took place in Chicago in November. Taking up an entire week, Rockwell Automation's Automation Fair is actually several events, co-located this year at McCormick Place.

PSUG

The first event was the Process Solutions User Group, with just under 800 attendees, most of them customers. This event kicked off what we should probably be calling Rockwell Automation Week with two days of meetings, roadmap sessions, and customer presentations of how they used Rockwell's PlantPAx DCS in their operations.

RA's John Genovese talks DCS

John Genovese keynoted PSUG by making a comparison between what he called the traditional DCS and the modern DCS (Plant PAx). Unfortunately, the comparison is flawed since the competition has also moved to platforms similar to Plant PAx over the last two decades.

Rockwell introduced the new Director of Process Automation, Jim Winter, recently acquired from Emerson Process Management— an unusual occurrence since RA tends to hire from within for senior management positions. Rockwell also introduced Version 4.0 of Plant PAx, and Plant PAx MPC, which provides modular procedural control in the controller as a key feature. Rockwell says the new offering is based on the emerging ISA106 standard.

On the second day, and competing with PSUG, Rockwell offered a half day media extravaganza called Automation Perspectives. This annual event is the media ver-

Genovese's comparison of DCS types

Rockwell CEO Keith Nosbusch

Bedrock, PAS and Statseeker: IT/OT Convergence Rolls On

Everywhere you look in manufacturing, whether it is in the process industries or in discrete factory applications, the OT network that connects factory and process automation devices is looking more and more like the IT network that connects the enterprise above the plant floor.

We have taken to calling this the IT/OT Convergence, and it is real. Plant engineers, operators, and maintenance people have had to start learning the things that IT admins have known for a decade or more. Looking at the plant network with this in mind, here are three vendors who have something unique to offer in the cause of IT/OT integration.

SIO4.E module

Bedrock Automation has released a new 5 channel Ethernet I/O module. The new **SIO4.E** Ethernet I/O module plugs into the revolutionary Bedrock™ pinless electromagnetic backplane to receive Bedrock's patented Black Fabric™ cyber security protection. Each of the module's five I/O channels is independently software configurable. The initial library of Ethernet protocols includes Ethernet IP, Modbus TCP, and OPC UA on TCP IP. All channels also deliver Power over Ethernet (PoE) while Bedrock's unrivaled computing horsepower and advanced electronics enable easier integration into real-time communications and control strategies.

Tightly coupling Ethernet into the process control and I/O network enables deployment of a wide range of edge device and enterprise data into real-time control logic, much in the same way an engineer incorporates more typical process sensor and actuator data. This results in real-time communication channels for the exchange of data between OT production and IT enterprise systems.

Bedrock's Rooyakkers

"Unlike an Ethernet switch traditionally sitting at Purdue levels 3 to 5 with the operations and business networks, the SIO4.E module delivers Ethernet as **secure I/O** at levels 0 and 1 with the sensor, actuator and process control logic. This collapses the legacy hierarchical ICS model into a simplified and inherently more secure automation architecture. Equally empowering is the deployment of OPC UA on any of the SIO4.E Ethernet I/O channels, opening up a world of opportunity and innovation while reducing all aspects of software lifecycle cost. This is the way of the future," says Bedrock CTO and Engineering VP, Albert Rooyakkers.

Ethernet is becoming widely adopted for open ICS applications because it builds on proven, high speed stacks that have been enhanced for use on industrial devices such as robots, PLCs, sensors, CNCs and other industrial machines. Bedrock secures Ethernet I/O in many ways, including by connecting the FIPS compliant anti tamper SIO4.E I/O module on a pinless electromagnetic backplane, embedding authentication logic, true random number generation (TRNG) and cryptographic keys into the semiconductor hardware and by isolating information flow within each channel by way of separation kernel functionality in a secure real-time operating system (RTOS).

"Robust ICS cyber security is just part of the tremendous value that the new Bedrock module brings to process automation," says Bedrock Automation President Bob Honor. "The fact that each channel can be software configured adds new levels of flexibility and scalability. No other I/O module allows process engineers to program so much communications capability into one system component. We are especially excited about the positive impact for ICS users. That user experience is increasingly configurable."

What this leads up to is the network visibility issue. OT networks are comprised of sensors, which usually cannot be seen using IT network technologies like network information management software, and increasingly, IT network technologies which can.

The most important IT tool for OT network administrators is the network information manager. These software applications, such as Statseeker, provide real time visibility deeply into the network, down to the device and port level. OT sysadmins can use Statseeker to help architect the network, determine where bottlenecks, non-performing devices, heavy traffic and even problems with some sensors and edge devices. Statseeker's ability to store time-series data in real time granularity allows it to be used for the network in the same way that a data historian is used for the process data. Trends, potential maintenance issues, and other problems can be seen and dealt with before a network failure occurs. Unusual traffic patterns can be used to detect potential intrusion into the network.

Statseeker Version 4.0 combines the full features of previous versions with a range of additional features such as Advanced Report Generation with Customized OID Support – see more of your network by discovering and monitoring specific data from all of your supported devices; Multiple Dashboards – save time by configuring multiple dashboard displays and automatically rotate different dashboards for a greater range of metrics from a single screen; Increased VM Interface – reduce CAPEX/OPEX costs and add flexibility as Statseeker now supports up to 150,000 interfaces from a single virtual machine environment; 95th Percentile Usage Reporting – add greater visibility for ISPs and customers who use services with 95% billing – plot your 95% usage lines against your defined interface usage reports, or calculate the 95% value for suitable times of the day such as business operating hours; and a RESTful API Inter-

IT/OT Convergence Rolls On (continued)

face – add more comprehensive network information. Statseeker's outbound web based API query engine allows specific data extraction requirements to query Statseeker and easily retrieve information in a real-time basis.

Statseeker CEO Frank Williams

"Interdependencies between applications, servers, and your network facilitate your businesses operational efficiency, or will contribute to its failure," remarked Frank Williams, Statseeker CEO and long time automation professional. He continues by saying "this is quite a challenge and one that is becoming tougher to manage. Using the right network monitoring solution makes the above challenges much easier to manage."

Other tools OT admins can borrow from IT include intrusion detection and prevention systems that can react to threats coming from outside the network, or from another part of the network. The OT admin should be able to conduct deep packet inspection on any network trunk to see if malware is finding its way into the network. Intrusion detection (IDS) systems are passive monitoring systems that detect suspicious activity. Intrusion prevention (IPS) systems are active systems performing in-line monitoring and can prevent attacks from both known and unknown sources.

Like any IT network, OT networks need anti-malware systems. Anti-virus and anti-malware systems need to be updated and upgraded regularly, and you should be able to both monitor for intrusion by malware and also perform surveillance on users and others who may be introducing malware into the network. Anti-malware best practices include the use of whitelisting and blacklisting IP addresses and web URLs, as well as filtering and proxies.

The Industrial Internet of Things will force the OT network to cope with mobility, both of devices and of various HMIs like tablets and smartphones. Plant operators and managers will want to be able to connect from anywhere, so another IT tool that the OT network sysadmin can borrow is mobile device management (MDM) software, which will enable the OT admin to push patches where possible, remotely monitor usage, remotely control security configurations, manage policies and procedures for mobile device use. OT admins will also need network access control (NAC) systems that allow you to enforce your security policies by granting access to the network to only compliant devices, as well as controlling access by authorized persons by responsibility, role, and geographic location. This software can manage roles and responsibilities to only serve appropriate data to the device. Additional tools can be found in authentication and authorization rule sets, such as Active Directory, or by use of newer authentication software that manages digital certificates and public key authentication schemes. The most recent version of the SNMP protocol, SNMPv3, even provides authentication, authorization and encryption capabilities not found in the first two versions.

Finally, OT networks still need firewalls, both in-line and edge. Next generation firewalls provide stateful inspection, deep packet inspection, and application visibility functions. OT network admins still need to keep firewalls configured properly, and updated regularly. Firewalls can be used to segment off various portions of the network to direct traffic and establish authentication and authorization policies.

But what about the rest of the network?

PAS' David Zahn

PAS, which is well known for its Integrity software, has perhaps solved the problem with its new release of *Cyber* Integrity 5.0, a part of the PAS Integrity Software Suite, according to David Zahn, general manager of the cyber security business unit at PAS.

PAS Cyber Integrity is based upon the proven PAS Integrity platform, and it automates internal and regulatory compliance reporting while reducing associated efforts by up to 90 percent.

Cyber Integrity works across the heterogeneous control environment found in plants providing enterprise scalability and performance. Cyber Integrity enables industrial companies to gather and maintain an accurate inventory of IT and OT cyber assets, automate patch processes throughout the enterprise, monitor for unauthorized change to cyber asset configurations, and implement a program for system backup and recovery.

As the Purdue model melts down into one or two layers, it is becoming more and more important to have visibility into the plant's OT network. With tools like Statseeker, PAS Integrity Suite, and hardware like Bedrock's native cyber security, the IT /OT Convergence will be manageable, instead of the royal clusterfluff many people have been expecting it to be.