ARC VIEW

FEBRUARY 1, 2018

Bedrock Automation's Open Secure Automation a "Win" with End Users

By Mark Sen Gupta

Keywords

Cybershield, Open Secure Automation (OSA), IIoT, Bedrock Automation, PLC, DCS

Summary

ARC Advisory Group recently had the opportunity to receive an update by executives from Bedrock Automation. It has been three years since Bedrock announced its vision of a cyber-secure industrial automation platform. The company continues to bring together technologies and talents in both the automation and semiconductor industries to create a clearly differentiated automation solution for industrial control. This effort is based on its three prime directives: simplicity, scalability, and security.

Bedrock continues to bring together technologies and talents in both the automation and semiconductor industries to create a clearly differentiated automation solution for industrial control. This effort is based on its three prime directives: simplicity, scalability, and security.

According to the company, the result is a system with a revolutionary electromagnetic backplane architecture and deeply embedded cybersecurity designed to deliver system performance, advanced cybersecurity, and reliability at a lower cost of ownership.

Key findings include:

- Bedrock's Open Secure Automation, (OSA) makes it easy for automation engineers to install secure control systems that also deliver the benefits of open technology.
- Bedrock and its partners have worked together to validate and secure HMI/SCADA applications with the Bedrock controller based on the latest security extensions of OPC UA and a Bedrock open SaaS Certificate Authority.

- Bedrock has more than twenty systems on-process, with another twenty systems slated to go online soon.

Accomplishments for 2017

As the "new kid on the block" in a market largely dominated by large and well-established suppliers, Bedrock Automation has a lot to prove. 2017 marked the third year since Bedrock came out of the shadows, seeking recognition for its intrinsically cyber-secure automation platform. To date, the system has garnered awards from Chemical Processing, Control Engineering, Design News, Processing Magazine, and Plant Engineering to name a few. However, the real accomplishments come in the form of deliverables. At last year's ARC Industry Forum in Orlando, Bedrock Automation put forth its goals for 2017.

Validation

Two of the more important goals company executives mentioned in February 2017 were *technology validation* and *market validation*. In May, Bedrock announced that the controller had achieved Achilles Level 2 Certification, joining the top automation vendors in using Achilles test products to verify and validate performance under real-world conditions, such as denial of service (DoS) attacks. In June, Bedrock released Cybershield 2.0, which enables authentication and encryption of I/O networks and field devices and protects compliant networks and user applications such as controller configuration, engineering, and SCADA. In November, the company announced it had successfully completed a clean, third-party audit of ISO 9001 requirements for "applying a quality system for the development, engineering, manufacture, and sales of cyber-secure process control equipment."

There are over twenty systems on-process and another twenty systems slated to go online soon. These installations are in industries that include oil & gas, water & wastewater, and electric power.

With regard to market validation, Bedrock has more than twenty systems on-process and another twenty systems slated to go online soon. These installations are in industries that include oil & gas, water & wastewater, and electric power. Furthermore, more than forty system integration companies in the Americas, Australia, the Middle East, and Europe have partnered with Bedrock to distribute its products and provide services to end users interested in deploying the technology.

Secure SCADA and Engineering Integration

It's one thing to have a secure controller. However, the more "exposed" pieces of a control system are the engineering workstations and SCADA operator stations. OPC UA and Bedrock's OSA Platform provide complementary technologies for HMI/SCADA application platforms. Together, they provide open automation solutions across all industrial automation and control market segments. The cyber threats to industrial control systems continue to grow in both scale and magnitude. As such, Bedrock has focused on providing an ultra-secure cyber solution using the best available technologies and has partnered with several HMI/SCADA companies to deliver a more coherent solution to the market.

Bedrock accomplishes this cybersecurity extension by working with partner organizations to incorporate third-party applications into its certification umbrella; its cloud-based SaaS Certification Authorization (CA) system. This CA allows users to implement secure OPC UA with encryption and authentication utilizing Bedrock's partner technologies like Inductive Automation, ICONICS, ETAP, and Tatsoft without having to rewrite the code.

Bedrock has implemented several technologies to extend the intrinsic security to these third-party technologies. According to the company, it developed a new software component to allow third-party HMI/SCADA OPC UA client applications to securely connect and communicate with Bedrock's OSA Platform. The OSA Platform has cybersecurity embedded within the silicon, firmware, and software using state-of-the-art semiconductor technologies coupled with new hardware and communications architectures. The company states the platform uses a combination of standards-based Suite B encryption, X.509 certificates, and lightweight embedded certificates to create a simple, robust, and secure environment. The software extends this security out to the periphery.

Challenging the Headwinds

Cyber threats are real and growing. US-CERT issued a technical alert advisory on October 21, 2017 (Alert TA17-293A) warning of advanced persistent threat activity targeting energy and other critical infrastructure sectors across the US. Information provided from both the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) indicate, energy, nuclear, water, aviation and critical manufacturing sectors are at ongoing risk from cyber-attack.

The Stuxnet computer virus, discovered in 2010, was used to attack Iran's nuclear program. A second virus, known as "Crash Override" or "Industroyer," was discovered in 2016 by researchers who said it was likely used in an attack that cut power in Ukraine. In December 2017, "Triton" emerged as the third computer virus discovered to date that can disrupt industrial processes. In this recent case, the virus was used to attack safety systems in an undisclosed Saudi Arabian facility.

Cyber-attacks are exceedingly sophisticated. Most industrial users do not have the staff or technology in place to mount much of a defense against these targeted "nation-state" level of attacks.

These attacks are increasingly sophisticated. Most industrial users do not have the staff or technology in place to mount much of a defense against these targeted "nation-state" level of attacks. Most manufacturers already understand that air gapping is not a valid cybersecurity strategy. The costs associated with bolting on cyber protections are increasing, and the technologies are changing fast.

Moving Forward

Bedrock engineers continue to focus on cybersecurity using a holistic perspective. According to the company, its controller is the first OPC UA server with intrinsic security built on a cyber-secure public key infrastructure (PKI) certificate chain of trust. This holistic, ground-up approach means the controller has cybersecurity designed within the chipset, the components, the network, and the ecosystem.

In December 2017, the company announced that its Q2 2018 OSA firmware will include intrinsic Anomaly Detection (AD). AD will be available as standard integrated functionality at no additional cost. It will monitor the controller's network and system time continuously to detect intrusions and anomalous behavior. AD will extend to network port scanning, system time monitoring, dynamic port connection monitoring, cryptographic controller engineering key lock functionality, and intrusion event logging. By adding AD to the firmware, the Bedrock solution falls in the highest level of cybersecurity as defined by ARC's Maturity Model for ICS Cybersecurity.

ARC's Take

The increases in malware and related industry breaches underscores the fact that it's past time for manufacturers and other industrial organizations

to get serious about cybersecurity. Many users have cybersecurity policies in place, but the policies/procedures tend to adapt slowly, be disjointed, and rely on hard-to-find specialists. Moreover, today's increasingly connected environment drives the process industries to search for automation solutions that deliver the benefits of open communications with "baked in" cybersecurity.

By extending its secure automation technology to third-party software providers, Bedrock Automation addresses this key pain point of future automation requirements. ARC believes the intrinsic and no-cost approach of Bedrock's cybersecurity strategy is the quintessential quality missing in control systems today; it makes securing the system easy for automation engineers over the entire product lifecycle. Because the cybersecurity is built-in, the system is secure from the start. The Bedrock supply chain and lifecycle help ensure security from the day the controller is put together until it is retired. The addition of secure HMI/SCADA and engineering workstations further ensures the safety of the system. The system is secured with regards to power supply and third-party network standpoints as well, with products Bedrock released last year.

ARC believes the intrinsic nature of Bedrock's cybersecurity strategy is the quintessential quality missing in control systems today; it makes securing the system easy for automation engineers.

All Bedrock's customers cite this "easy intrinsic cybersecurity" as a reason for choosing the Bedrock platform for their control needs. End users with large installed bases of legacy control systems will need to decide if the risks of cyber hacks on those platforms are enough to justify migrating to a new, more secure platform.

The links below provide more information on installations of Bedrock Automation's products:

- City of Lynchburg Wastewater Treatment
- Pinnacle Midstream
- Clarksville Light and Water
- Russellville Water and Sewer

For further information or to provide feedback on this article, please contact your account manager or the author at msengupta@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.