ARC VIEW

January 19, 2017

Bedrock Automation's Intrinsic Cyber Defense Makes Cybersecurity Easier for End Users

By Mark Sen Gupta

Keywords

Cybersecurity, Bedrock Automation, PLC, DCS, Control, Power, EMP, IIoT

Summary

ARC Advisory Group recently met with Bedrock Automation for an update on the company's progress to date and overall strategy. Bedrock has been busy expanding its portfolio to include secure power supplies, connectivity to third-party devices, and extending cybersecurity to networks and applications. Although the company has quite a few products in development, one theme is consistent: *intrinsic cybersecurity*.

Bedrock Automation has been busy expanding its portfolio to include secure power supplies, connectivity to third-party devices, and extending cybersecurity to networks and applications.

Everything Bedrock creates is designed to provide a strong holistic defense against networked and non-networked attacks. The hardware is designed to withstand physical and electronic attacks. Authentication is embedded at the chip level to protect against rogue control system parts being inserted into the system. That same authentication is being rolled out to support communications with edge devices and PC-based applications as well.

Key ideas Bedrock Automation highlighted during the briefing:

- Cybersecurity strategies must address more than network attacks
- Intrinsic cybersecurity makes it easier for users
- Any component not protected is a potential liability

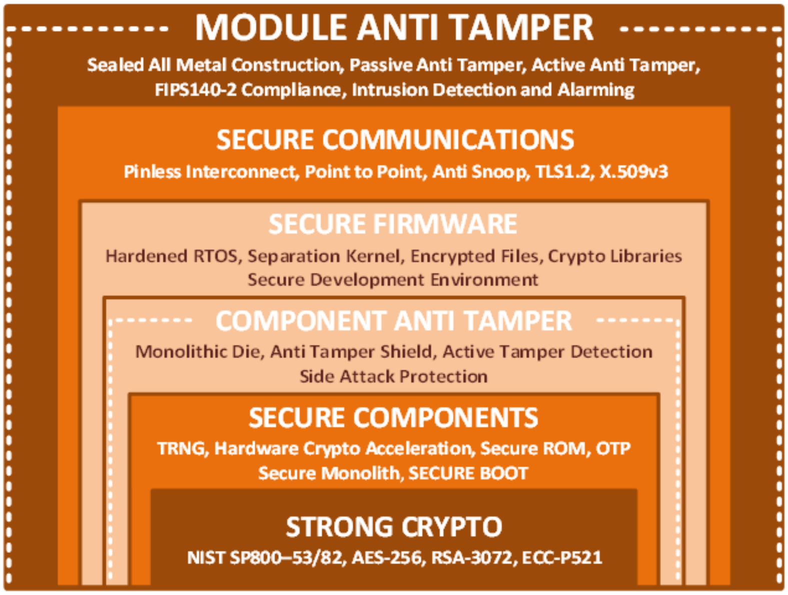
Current Cyber Threats

The majority of control systems in use today are vulnerable to cyber-attacks. These systems were designed before current hacking technology existed. The industry has witnessed determined and coordinated efforts by hackers to breach control systems. Weaknesses in IP-connected devices have been exploited. Physical breaches have compromised systems, and damaged hardware. Failure in standard operating procedures led to compromised systems (i.e., Stuxnet). Counterfeit control system parts containing malware are also circulating in the market. However, the people working around these systems remain the weakest link for cybersecurity. Inappropriate use of cell phones, USB drives, email, poor passwords, lost or stolen credentials and the like are attack vectors that hackers are learning to exploit.

These potential attack vectors increasingly affect capital and operational costs for companies around the world, but it appears that Bedrock Automation is on the right path to simplify the time and effort required for owner-operators to implement cyber-secure systems.

Expanding Product Line

Bedrock has been busy filling out its portfolio of cyber-secure automation products. Last year, it introduced an intelligent, standalone power supply to its line of "simple, scalable and secure" control technologies. The new SPS.500 Secure Power Supply, a complement to Bedrock's Secure Lithium UPS, provides the company's deep-trust cybersecurity authentication and onboard intelligence for diagnostics and secure OPC UA over Ethernet communications. According to the company, the IP67/NEMA 4/5/6 sealed aluminum enclosure allows users of any PLC, SCADA RTU, PAC, or DCS to retrofit the new SPS.500 and UPS.500 inside or outside enclosures, anywhere in a plant and in harsh environments. These secure field devices with secure OPC UA form the basis of Bedrock's platform approach to IIoT.


MODULE ANTI TAMPER
Sealed All Metal Construction, Passive Anti Tamper, Active Anti Tamper, FIPS140-2 Compliance, Intrusion Detection and Alarming
SECURE COMMUNICATIONS
Pinless Interconnect, Point to Point, Anti Snoop, TLS1.2, X.509v3
SECURE FIRMWARE
Hardened RTOS, Separation Kernel, Encrypted Files, Crypto Libraries Secure Development Environment
COMPONENT ANTI TAMPER
Monolithic Die, Anti Tamper Shield, Active Tamper Detection Side Attack Protection
SECURE COMPONENTS
TRNG, Hardware Crypto Acceleration, Secure ROM, OTP Secure Monolith, SECURE BOOT
STRONG CRYPTO
NIST SP800–53/82, AES-256, RSA-3072, ECC-P521

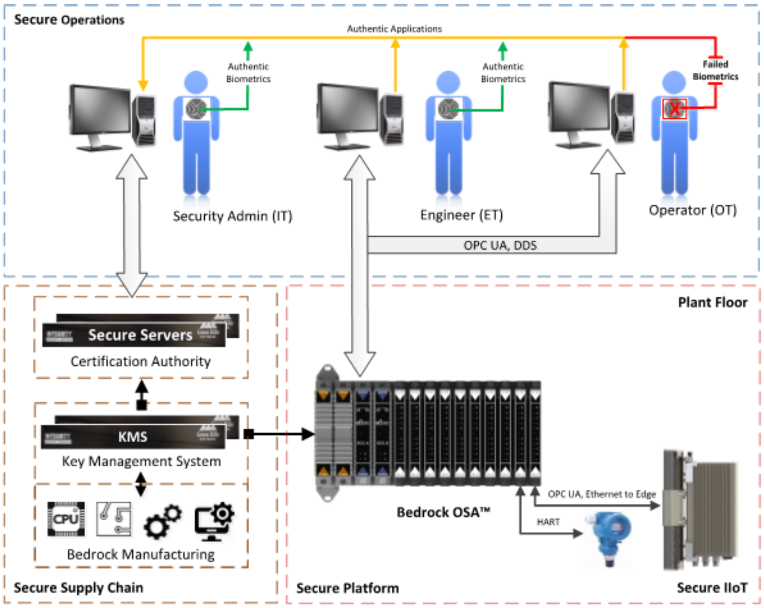
Intrinsic Security Layers

The company also introduced a secure, universal multichannel serial I/O module that plugs into its pinless electromagnetic backplane to help protect the control system from insecure communications with third-party devices (other PLCs, printers, bar code readers, etc.). The SIOS.5 has five channels, each supported by an independent, cyber-secure 32-bit ARM processor. Each channel is software-defined for RS-232, RS-485, or RS-422 communications. This extends the range of industrial edge devices that can be secured by Bedrock Open Secure Automation (OSA) users.

Late last year, Bedrock introduced a software-configurable Ethernet I/O module with embedded cybersecurity. The SIO4.E Ethernet I/O module plugs into the company's pinless electromagnetic backplane to benefit from its patented Black Fabric cybersecurity 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).

CyberShield: Bedrock's Approach to Total Integrity

During the briefing, Bedrock Automation executives walked ARC through the strict methodology it uses to develop the product line. The original idea (and current approach) is cybersecurity centric. The introduction of Bedrock's Open Secure Automation System ushered in the beginning of its CyberShield offering. At the time, Bedrock detailed the cyber-secure aspects of the controller platform.



Bedrock Automation's Secure Communications Paths

The diagram depicts the different secure communications "paths" implemented within the system and throughout the product lifecycle. It captures the overall scope of the cybersecurity conundrum as Bedrock views it, which encompasses much more than the control system itself. The company utilizes a public key infrastructure (PKI), which is similar to the methodology used to secure e-commerce transactions. The novel application of PKI, in which the *OSA system* is the root of trust, enables authentication across sensors, networks, and applications, as defined in the diagram. According to the company, this provides automation users with intrinsic and holistic cyber defense and a level of security not yet in widespread use in the automation industry.

Every detail of the hardware, software, and associated manufacturing processes is designed to secure the owner-operator's intellectual and physical property. This contrasts with the typical industry approach of protecting the system after installation.

Cyber Lifecycle Starts Before Installation

Bedrock's approach addresses weaknesses in the supply chain. It has partnered with Green Hills Software Integrity Security Services to effectively create a "birth certificate" of cryptographic keys and certificates that are written into specialized embedded chips and system components. This forms the basis of a hardware root of trust and helps guarantee that module hardware, firmware, and applications are from reliable sources and specifically for a particular industrial customer. Because Bedrock manufactures its own components, this certificate guarantees that the modules are from Bedrock. (In contrast, many other suppliers purchase components from other companies). According to the company, its approach prevents rogue agents from infiltrating the supply chain prior to delivery of the modules to the customer.

Counterfeited control system parts are getting so sophisticated, it can be difficult to tell the difference between fake and authentic vendor products. While counterfeiting is used primarily for financial gain, rogue actors could use this method to incorporate malware into the counterfeit products' firmware. Intrinsic hardware and firmware authentication with strong encryption can identify and reject sophisticated fakes quickly, thwarting this cyber-attack method.

The company believes that secure systems require a secure supply chain to eliminate an array of possible attack vectors. There are many elements to a comprehensive secure supply chain, including a key management system (KMS), which help control the creation and distribution of certificates and keys. As a result, the KMS must support meticulous attention to detail. An industrial KMS is built on a specialized set of certified, high-security computer appliances. It must be an integral part of a supplier's factory to equip and lock every module's secure silicon with a custom and secret package of certificates and keys at the time the module is created. Secret keys must be kept confidential. This requires a secure supply chain.

Cybersecurity Encompasses Physical Security

With its designs, the company strives to address all possible attack vectors. One of the most striking differences between Bedrock products and its competitors is the product construction. Bedrock utilizes sealed, all-metal housings, including the backplane. The company claims this increases environmental robustness, tamper resistance, and structural and thermal integrity; and provides protection against electromagnetic interference (EMI) and high-energy electromagnetic pulses (EMP).

Bedrock utilizes sealed, all-metal housings, including the backplane. The company claims this increases environmental robustness, tamper resistance, and structural and thermal integrity; and provides protection against electromagnetic interference (EMI) and high-energy electromagnetic pulses (EMP).

Bedrock also claims that backplane and module pins represent a real vulnerability that could allow hackers to snoop or insert communication traffic. All electronic pins route, receive, or radiate energy in the DC-to-RF spectrum, and most typical ICS modules are encased in vented plastic with little or no EMI protection. Pin-based systems can be so susceptible to EMI that even a power tool operating nearby could alter or interrupt communication and computation. From plant floor noise to emerging EMP weapons, electromagnetic radiation is an ICS cyber vulnerability. The company believes that its pinless I/O backplane and sealed, all-metal construction for all backplane I/O system modules reduce electromagnetic susceptibility while providing integral EMI and EMP hardening, without requiring secondary measures. This is an important step to reducing the overall cyber vulnerability.

Security Made Easy

Intrinsic security measures of this nature and to this degree clearly reduces the cybersecurity burden for end users. Although current measures taken with traditional automation systems are good practice, the added steps implemented by Bedrock require no extra effort on the part of the user. The embedded authentication techniques ensure that if rogue hardware, firmware, or applications were to be installed, it would fail to be accepted. The internal secure communications require no setup by the user, nor does the inherent module authentication. The intrinsic security measures employed appear to reflect the current ease-of-use requirements set forth by several large operating companies.

The result is a more secure system overall; with less effort required by the end user.

Conclusion

Hackers are increasingly sophisticated and the simplistic approaches of the past only protect against the amateurs. Nation-states have been stealing secrets for decades and have the resources to employ a variety of methods for a variety of goals. Security is no longer about your network defenses alone. Some of the threats identified by Bedrock Automation might make for good movie plots, but the reality is that these threats are real. (In just one example, a quick search on the web will instruct the interested in how to construct an EMP gun).

ARC is not aware of any other supplier implementing a cyber strategy as stringent and comprehensive. In examining the current portfolio, the Bedrock engineers and architects are tackling cybersecurity in a more intrinsic and holistic fashion than many end users have considered. The message? Air gaps and firewalls are not enough.

End users should carefully consider the various impacts of each type of attack to weigh the importance of the security measures. These impacts include, but are not limited to, extended downtime, loss of intellectual property, physical damage to equipment and personnel, environmental impact, and loss of product quality.

Bedrock Automation will be participating in and demonstrating many of its cyber-secure products at the upcoming ARC Industry Forum in Orlando, Florida, February 6-9, 2017.

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.