April 2016

The Bedrock™ Revolution

Chapter Three: Intrinsic Cyber Security Fundamentals

Introduction

All aspects of industrial control system (ICS) design have been rethought and rebuilt in the Bedrock™ system. The result is a new platform we call **O**pen **S**ecure **A**utomation. OSA™ delivers significant improvements in performance, reliability and security at lower lifecycle cost. Our first chapters covered the Bedrock™ backplane and Bedrock™ power designs. This chapter describes the *Fundamentals of Intrinsic Cyber Security*.

Automation systems are cyber vulnerable. When compromised by an attack, varying degrees of risk and consequences to people, the environment and infrastructure result. Current best practice for cyber defense of new and legacy systems is to build a *bubble* of complex enterprise defenses around an ICS target, while also attempting total system isolation. This is a less than optimal approach. The way forward is to design systems with deeply embedded intrinsic cyber defense.

Bedrock Automation OSA™ White Paper Series (Release title and sequence may vary.)

Chapter One:	Backplane - Our Journey Begins	RELEASED
Chapter Two:	Empowering Power	RELEASED
Chapter Three:	Intrinsic Cyber Security Fundamentals	RELEASED
Chapter Four:	Advanced OSA™ Security – Nation State Defense	FUTURE RELEASE
Chapter Five:	Virtual I/O and OSA™	FUTURE RELEASE

In the beginning…

Many ICS types including DCS, PLC, Safety and others, were developed using technologies and tools from the 1980s and 1990s. These "modern" systems are now up against rogue actors armed with cyber tools that are orders of magnitude more capable than the technologies used to engineer and build the systems in the first place. Exposed pins, ports, circuit boards and back doors into system networks create a host of vulnerabilities and a large attack surface.

Figure 1: Examples of ICS systems with cyber vulnerabilities

Intrinsic Security – The way forward

Intrinsic security implies security by design and requires a suite of technologies to be deployed in every aspect of a system's electronic components and modules. This approach is abstracted in Figure 2 below and represents the fundamentals of an integral root of trust with strong authentication of hardware, firmware, software and users. Let's review the component pieces.

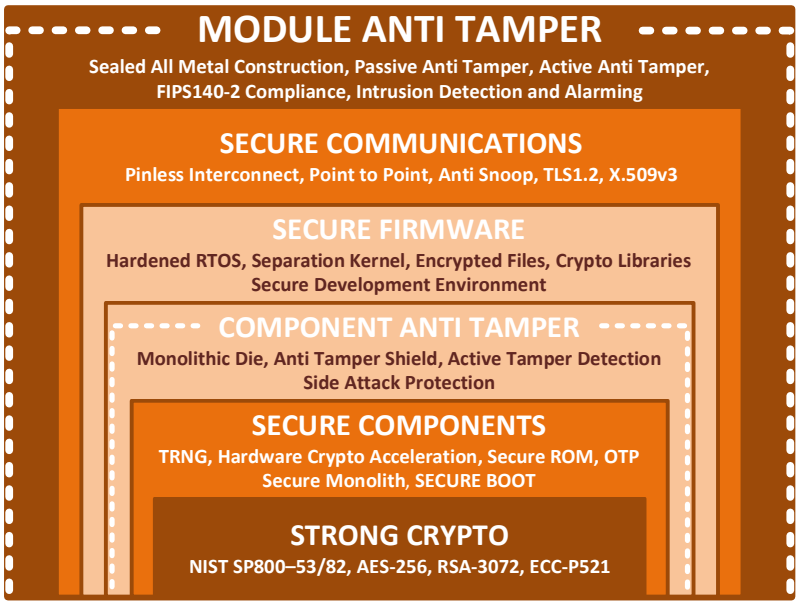

Figure 2: Building Blocks for Intrinsic Security

Metal – the way forward

The fact that carbonated water comes in all-metal enclosures while advanced ICS electronics are wrapped in plastic, will remain a mystery of our time. Table 1 lists the obvious advantages of all-metal ICS module construction, two of which – *EMI/EMP Hardening and Passive/Active Anti Tamper* – are critically important to cyber defense. The rest of this paper could be used to describe these advantages in detail, but in summary, there is no *secure* future in plastic.

Benefits of All Metal Module Housing	Benefits of Plastic Module Housing
Environmental Hardening	Cheap
EMI and EMP Hardening	
Structural Integrity	
Thermal Integrity	
Cyber Integrity - Anti Tamper	
+50 Year Life	

Table 1: Metal versus Plastic Module Housing Comparison

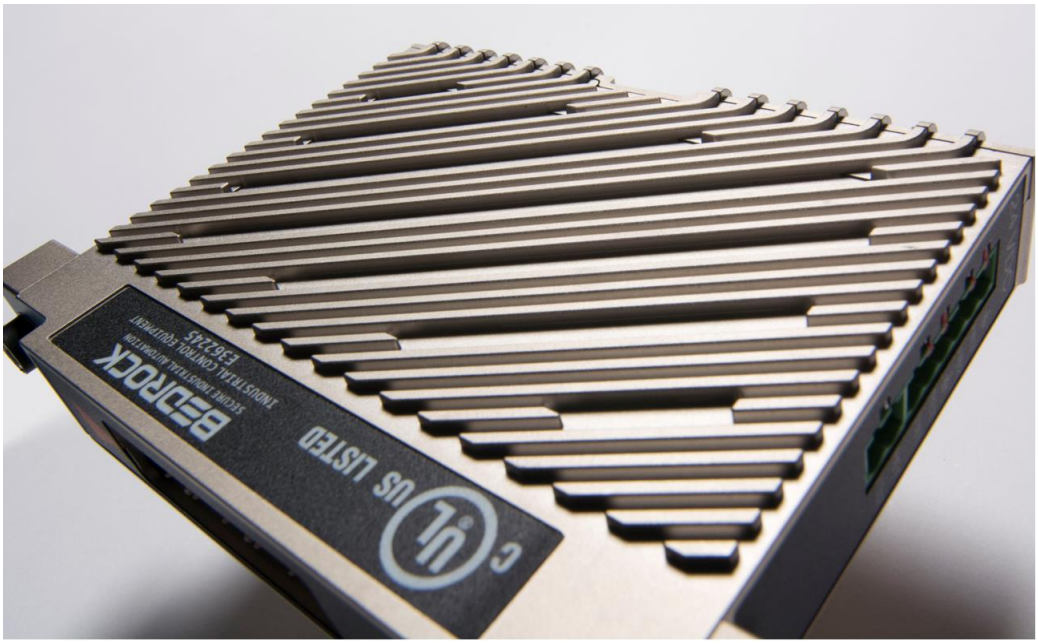

Figure 3: Example of a sealed all-metal cyber hardened OSA™ module

Ports

Typical system modules are designed with multiple communication ports for debugging, diagnostics and network connections. All traditional ports can be hacked and compromised to access and manipulate system resources. An intrinsically secure design eliminates all unnecessary access ports and then encrypts and authenticates devices and networks that communicate on the remaining ports.

Pins and Electromagnetic Interference - (EMI)

Backplane and module pins create a large cyber-attack surface to snoop or insert communication traffic. All electronic pins route, receive or radiate energy in the DC to RF spectrum, and virtually all 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

operated in close proximity can alter or interrupt communication and computation. From plant floor noise to emerging EMP weapons, electromagnetic radiation is an ICS cyber vulnerability. A pinless I/O backplane and sealed all-metal construction of all system modules extensively reduces electromagnetic susceptibility while providing integral EMP hardening without secondary containment. This is an important step to reducing the overall cyber-attack surface. (See also Bedrock White Paper Chapter 1: The Backplane.)

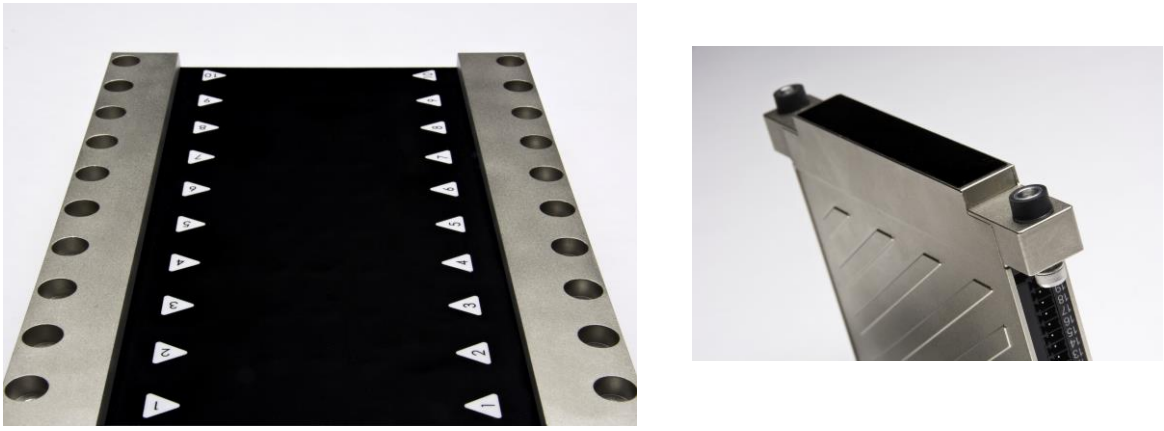

Figure 4: A Pinless Cyber Hardened I/O Backplane and I/O Module

Electromagnetic Pulse and Cyber Defense - (EMP)

EMP is a burst of electromagnetic energy that can occur naturally, like lightening; be man-made from the use of electronic and electrical devices; or be man-made as a weapon to *disrupt* electronic and electrical devices. Therefore, EMP is a kinetic form of cyber-attack that is impervious to even extreme digital defenses. While industrial equipment standards like IEC 60068 define compliance for systems to low energy EMP such as electrostatic discharge (ESD) and electrical fast transients (EFT), that level of system hardening will not defend against high energy EMP. MIL-STD-461, (respectively IEC 61000-4-25) defines tests for immunity of electronic equipment to a high altitude electromagnetic pulse (HEMP), equivalent to the energy of a nuclear EMP weapon. This is an extreme measure of electromagnetic hardening for systems and equipment without shielded secondary containment. MIL-STD-461E test RS105 requires repeated transient electromagnetic pulses of up to 50 kilovolts per meter with nanosecond rise times.

To some this may sound more like a movie or end-of-times, but more practically, non-nuclear EMP (NEMP) drone and missile weapons are part of the arsenal of many nation states and are too easily constructed by rogue actors. World-class intrinsic cyber hardening of automation for critical infrastructure will require MIL-STD-461 (IEC 61000-4-25) compliance to provide users decades of EMP cyber defense. This is the best way forward.

Counterfeiting

ICS module counterfeiting is widespread and so advanced that it is difficult to tell the difference between fake and authentic vendor products. While counterfeiting is used primarily for financial gain, rogue actors use this method as an attack vector by incorporating malware into the counterfeit product firmware. Intrinsic hardware and firmware authentication with strong encryption can identify and reject sophisticated fakes instantly, disabling this powerful cyber-attack vector.

Cryptography (*computerized encoding and decoding of information*) and OSA™

Encryption can be used in two basic ways in an ICS. The first is to hide the content of messages and system data. The second use of encryption is authentication, i.e., did this firmware update come from the correct source? Has it been tampered with? Is this ICS module genuine hardware? Did new user logic for the controller come from an authorized source? Is this set point change from an authorized source? Use of cryptography will provide not only unambiguous answers to these and other questions but more importantly, it can ensure that messages, code changes, and operator actions that flunk authentication are rejected. Encryption makes an ICS cyber-attack significantly more difficult.

There are two basic methods of encryption, *symmetric,* also known as secret key encryption, and *asymmetric*, or public key encryption. Symmetric encryption requires both parties to share a secret key, while asymmetric encryption uses a public key and a private (secret) key pair. The public key can be shared and accessed without compromising the private key and message. Without the secret and public key, an attacker sees only random gibberish. This would not only make it hard to extract information from the control system, it also makes it hard to manipulate because only properly encrypted commands would be accepted. The private key provides the means to create *digital signatures*, which can only be verified with the associated public key. Digital signatures then provide the means by which other entities can verify the *integrity and authenticity* of data sent with a particular private key.

Strong Encryption – Suite B

Automation systems have an expected useful life of decades. As a result of Moore's Law and emerging capabilities in quantum computing, the strength of encryption methods degrades over time. Suite B is an interoperable cryptographic framework published by the National Security Agency. (See also Table 2 below.) Different key strengths are recommended for TOP SECRET protection based on security tasks such as encryption, digital signatures, key agreement and others. It could be argued that every transaction in automation is mission critical and should be ranked TOP SECRET. Therefore, an OSA™ requires use of the strongest Suite B encryption, and as well should deploy a means for adaptive encryption in anticipation of quantum attacks in the future.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS PUB 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Use Curve P-384 to protect up to TOP SECRET
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 to protect up to TOP SECRET
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	FIPS SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET

Table 2: Use Of Public Standards For The Secure Sharing Of Information Among National Security Systems
(Committee on National Security Systems, Advisory Memorandum 02-15-15v)

Secure Boot

A secure module must be able to start up and to decay in a secure state. This is an absolute prerequisite for a secure module to perform a secure initialization from a cold start or a hot reset. No unauthorized party can tamper with the software while the module processor is starting up. A secure boot starts with an initial phase loaded from on-chip masked ROM monolithically part of the microprocessor silicon. Keys that authenticate, decrypt, load and start additional levels of encrypted software are stored in this secure memory. Intentional or unintentional power cycling must not degrade the protection of the secret keys. The microprocessors must also have on-chip hardware math acceleration to perform the required encryption and decryption calculations in real-time so that security does not degrade the ability of an ICS to perform real-time process control.

True Random Numbers

High quality random numbers are critical to strong cryptography. Random numbers are used in real-time to derive symmetric keys or as an initialization vector for an authentication protocol. An example is a *nonce*, an arbitrary single-use number used in authentication to prevent the reuse of older communications, (a vulnerability known as a replay attack). There are two types of random number generators: pseudo random and true random. Pseudo random numbers (PRNG) are mathematically generated in software while true random numbers (TRNG) are generated in semiconductor hardware with an entropy engine and are far less vulnerable to discovery. *The strength of system cyber security can be directly correlated to the TRUE randomness of the random numbers.* All ICS microprocessors must be equipped with integrated high quality true random number generators.

Security Hardened Operating Systems - (OS)

Operating system vulnerabilities are many and can wreak havoc on system security because they directly affect all aspects of firmware and software execution. While only a few general OS's dominate the market, i.e., Windows™ and Linux, there are more than 50 commercially available real-time operating systems (RTOS) and choosing the right one will have a significant impact on the cyber strength of control, I/O and network computing. The RTOS must have an inherent architecture to support integrated and validated middleware, secure communication stacks, network security protocols, and embedded encryption libraries for safety and security applications. There are very few RTOS products that meet these requirements.

Evaluation Assurance Level - (EAL)

Testing and validation of an OS is important to measure design robustness. An OS security robustness metric is Evaluation Assurance Level (EAL1 through EAL7). EAL is a numerical grade assigned following the completion of a Common Criteria security evaluation. Common Criteria is an international standard of security testing in effect since 1999. A higher assurance level denotes increased requirements to achieve Common Criteria certification and provides higher confidence that the operating system security features are reliably implemented.

Anti-Tamper for Cyber Defense – FIPS 140-2

Intrinsic security requires layered anti-tamper protection to keep secret keys secret. Anti-tamper is almost entirely not used in automation systems, but widely experienced in everyday life. From pills to peanut butter, we mostly know if someone has been there before us, and how to keep valuable products inside their containers or away from children. Standards and practices for electronic systems in military and communications security exist, including Federal Information Processing Standards, FIPS Pub 140-2, *Security Requirements For Cryptographic Modules*. FIPS 140-2 describes crypto strength, crypto boundaries and *levels of tamper protection*. Tamper protection is logical at two levels: the secure semiconductor component boundary, and that of the system module boundary. Advanced secure component design and sealed all metal module construction combined can provide FIPS 140-2 Level 2 to Level 4 anti-tamper compliance. FIPS 140-2 is the right standard to design and measure anti-tamper cyber defense of ICS modules.

Secure Supply Chain and Key Management System - (KMS)

Secure systems require a secure supply chain to eliminate an array of possible attack vectors. There are many factors to a comprehensive secure supply chain, including a KMS. The purpose of a KMS is to control the creation and distribution of certificates and keys, so the KMS must support meticulous attention to detail. An industrial KMS is built on a specialized set of high security computer appliances certified to FIPS-140 Level 3. It must be an integral part of a supplier's factory in order to equip and lock every module's secure silicon with a custom package of certificates and keys at the time of module *creation.* The correct certificates and keys must get to the correct places. Secret keys must be kept secret. A secure supply chain is required.

Public Key Infrastructure - (PKI) enables Open Secure Automation (OSA™)

Use of asymmetric cryptography for authentication and key exchange is the basis of secure e-commerce and makes widespread electronic commerce possible. In the internet context, there is a critical additional piece, a root of trust at the center of an exchange. This is called a Certificate Authority, or CA, such as Verisign™. Key pairs, certificates, a root of trust and interoperable algorithms together form a Public Key Infrastructure, or PKI, and PKI includes the infrastructure and policies to *manage and maintain the trust*. Some of the building blocks of PKI include the following:

Signatures

The signing operation involves generating a cryptographically secured message using a one-way computation function referred to as a hash. Hash functions take an arbitrary sized message and produce a relatively small fixed length message referred to as the hash value or digest. The digest is then encrypted using the private key and referred to as the signature. When an entity that holds the public key receives the signature, it decrypts the signature and performs an independent digest operation on the message contents. If the decrypted digest matches the newly computed digest, it is understood (with great confidence) that the message is the same as the one signed by the entity holding the matching private key.

Transport Layer Security – (TLS)

In order to overcome key distribution problems associated with symmetric encryption and the higher computational requirements of asymmetric encryption, a hybrid technique (called the handshake) using Asymmetric and Symmetric Encryption is used to generate a shared secret between the entities. Once the shared secret is exchanged, communication can be established using much faster symmetrical algorithms. The newly generated key is only used once per session and is commonly referred to as the session key or ephemeral key, as it is regenerated for each session.

The most commonly used protocol for performing this handshake and switch-over process is called Transport Layer Security (TLS). A requirement of Asymmetric Encryption is that each entity needs to exchange public keys. TLS accomplishes this by using X.509 certificates (which contain the public keys) from each entity as part of the handshake process.

X.509 Certificates

A digital certificate is a public piece of information (called the subject) that has been signed by a trusted source. X.509 certificates contain the public key of an Asymmetric key pair. The subject is then embedded within a container format including other meta-data. A digital signature from the issuer is attached to the end of the container. In order to ensure that the subject is not modified, the certificate used to sign the message needs to be verified that it is authentic. Authentication is accomplished by the certificate chain of trust.

Certificate Chain of Trust

When signing a certificate, the public key used to decrypt the signature is also stored in a separate certificate. This certificate is signed and authenticated with another certificate, forming a "chain" of certificates that are linked together and commonly referred to as the "chain of trust" or "hierarchy of trust." A certificate that is used to authenticate another certificate is called a Certificate Authority (CA). The chain forms a hierarchy that ends in a single certificate authority. The top-level certificate is called the root certificate authority because all certificates are based on it.

Root Certificate Authority

The Root Certificate Authority is self-signed and must be inherently trusted by all entities. It is the root of trust as all other certificates are ultimately based on it, and is referred to as the trust anchor of the system. The root CA must be distributed to all entities in the system and precautions must be taken to ensure that this certificate is not tampered with or replaced. The root CA is often referred to as the source of trust; it is actually the public key of the root key-pair that must be trusted.

Hardware Root of Trust - (HRT)

PKI is widely deployed e-commerce technology. However, the application of PKI to automation has not happened because of an absence of the innovation and motivation to deliver it, and too much core technology is missing in a conventional ICS. Internet connectivity with automation systems is simply not acceptable for safe process operations. However, by implementing the full suite of ideas and technologies outlined in this paper, a *Hardware Root of Trust, HRT is embedded in the control system!* Now deploy an industrial PKI for OSA™ and everything changes. The ability to encrypt and authenticate automation systems from the sensor to the user credential exists. OSA™ becomes the architecture for intrinsic security. Figure 5 abstracts such an architecture.

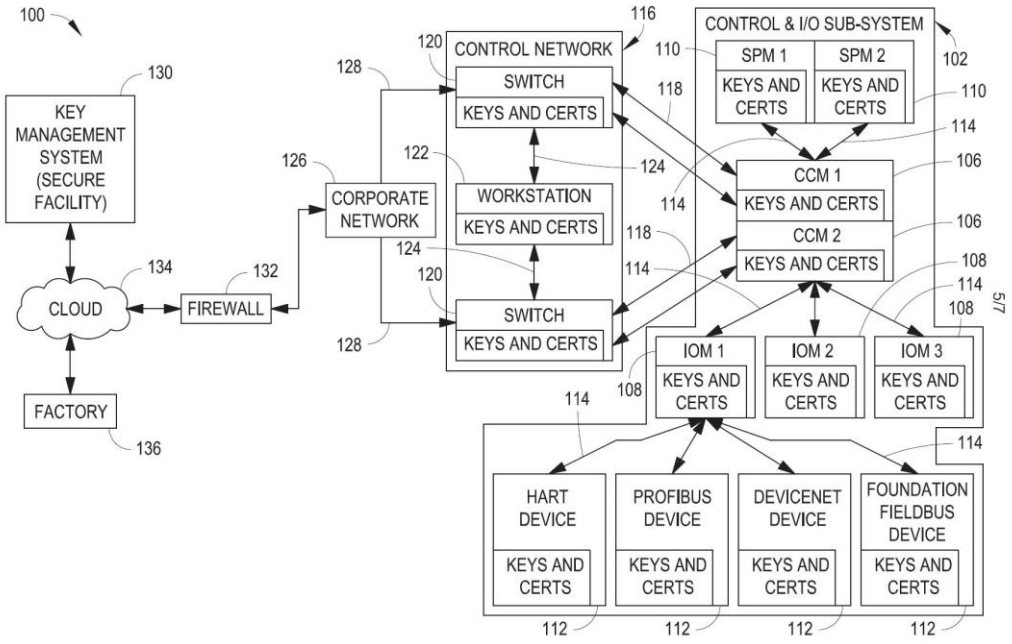

Figure 5: An OSA™ Cyber Architecture with an Intrinsic Hardware Root of Trust
(Reference also to US patent 9,191,203 B2)

Cyber Standards and Certification

Many government standards are referenced that can guide the design of OSA™. IEC and UL standards also continue to evolve, that in combination, define a coherent ICS cyber defense design strategy. The ISA Secure certification program, *Embedded Device Security Assurance (EDSA),* for example, focuses on the security of embedded devices and addresses device characteristics and supplier development practices for those devices. http://www.isasecure.org/en-US/Certification/IEC-62443-4-2-EDSA-Certification. There can be no excuses...combining modern technologies and robust standards will ensure a world-class defense to a world-scale issue. Building secure automation to help build a more secure world is completely possible. That future is now.

Summary

This paper outlines the *Fundamentals of Intrinsic Cyber Security* at the heart of Open Secure Automation. Without such a layered and deeply embedded approach, there is little chance of lasting success. It is a complex technical challenge but one that Bedrock Automation has taken on and is commercializing now. The standards to define and measure such an effort are in the public domain. One final note: As with all good technologies, market adoption depends largely on the user experience. Intrinsic OSA™ done right is intuitive and transparent to the user. To ensure broad adoption and success in a hostile cyber future, security must *"just happen"* or it may never happen.

Author

Albert Rooyakkers, Founder, CTO, VP Engineering, Bedrock Automation:
https://www.linkedin.com/profile/view?id=32444535

Contributing Authors

Sam Galpin, Bedrock Automation Fellow

Craig Markovic, Director of Development, Cyber Security, Bedrock Automation

John Weismiller, Senior Software Engineer, Bedrock Automation

Visit Bedrock Automation: www.bedrockautomation.com
Follow Bedrock on LinkedIn: https://www.linkedin.com/company/bedrock-automation

Intrinsic Security Technology Checklist				
Item	**Security Technology**	**Description**	**OSA™**	**ICS**
1	Secure Digital Components	Secure Microprocessors.	✓	
2	True Random Number Generator	Silicon embedded entropy engine for highly random number generation used in authentication and key generation.	✓	
3	Secure ROM and OTP	On-chip storage for secure keys and firmware.	✓	
4	Secure RAM	On-chip code execution. Secures firmware, secure keys.	✓	
5	Hardware Accelerators	Faster crypto math execution, higher performance.	✓	
6	Secure Boot	On-chip initialization. Fundamental to secure firmware and secret key protection.	✓	
7	Component Anti Tamper	Monolithic die shield, side attack protection. Protection of secret keys.	✓	
8	Strong Crypto, NIST SP800-57, Suite B	TOP SECRET data and communications integrity. Longest life of crypto keys.	✓	
9	AES-256, HMAC-256	Symmetric block cipher for information protection.	✓	
10	RSA-3072	Asymmetric algorithm used for key establishment.	✓	
11	ECC-P521	Asymmetric algorithm used for digital signatures.	✓	
12	Hardened Real Time Operating System (RTOS)	Separation kernel, EAL rated, Crypto libraries. Critical to overall system security and attack robustness.	✓	
13	Secure Communications	A critical component of cyber defense. Available to all channels and sockets.	✓	
14	TLS 1.2 Open Standard Support	Transport Layer Security. A requirement of asymmetric encryption to exchange public keys.	✓	
15	X.509 Certificates Support	X.509 Certificates contain the public key of an asymmetric pair.	✓	
16	Pinless I/O Backplane	EMI and EMP hardening. Anti snoop.	✓	
17	Pinless I/O Module	EMI and EMP hardening. Anti snoop.	✓	
18	Point to Point Bus	Reduced communication attack surface.	✓	
19	Sealed All-Metal Construction	Cyber hardening, module anti tamper. FIPS 140-2 compliance.	✓	
20	Passive and Active Anti-Tamper	Physical security of system modules and secure components.	✓	
21	MIL-STD-461/IEC 61000-4-25 Compliance	A military and IEC standard for advanced electromagnetic compliance. HEMP resistant.	✓	
22	FIPS 140-2 Compliance	Federal Information Processing Standards – Security Requirements for Cryptographic Modules. Defines a suite of cyber defenses for communication systems, including anti tamper.	✓	
23	Intrusion Detection	Embedded detection of abnormal network activities and attacks.	✓	
24	Intrusion Alarming	Hardware cyber indication. Embedded logging.	✓	
25	Hardware Root of Trust	Embedded Certification Authority Equivalence. Enables integrated PKI and extended authentication.	✓	
26	Public Key Infrastructure	Method of extended authentication.	✓	
27	Secure Supply Chain	Cyber secure manufacturing infrastructure. Elimination of supply chain attack surfaces.	✓	
28	Key Management System (KMS)	Specialized high security appliances. Controls the creation and distribution of certificates and keys.	✓	
29	Authenticated Modules	Secure component signed and encrypted to circuit board.	✓	
30	Authenticated Firmware	Module firmware signed and encrypted with secret keys.	✓	
31	Authenticated Communication	Support TLS 1.2, PKI, Hardware Root of Trust, secure OPC UA.	2016	
32	Authenticated Applications – Engineering, SCADA	Support TLS 1.2, PKI, Hardware Root of Trust.	2016	
33	Wurldtech L2 CRT Compliance	Communication Robustness Testing.	2016	
34	Authenticated User	Support TLS 1.2, PKI, Hardware Root of Trust.	2016	
35	ISA Secure/IEC62443 Compliance	Embedded Device Security Assurance.	2016	

Table 3: Intrinsic Security Technology Checklist

Item	Patent/Publication Reference	Country	Title
1	US 2015/0048684 A1	USA	Secure Power Supply For An Industrial Control System
2	US 9,191,203 B2	USA	Secure Industrial Control System
3	US 2016/0078213 A1	USA	Secure Industrial Control System
4	App. No. 14/918,558	USA	Tamper Resistant Module For An Industrial Control System
5	US 2015/0046710 A1	USA	ICS Redundant Communications/Control Module Authentication
6	US 2015/0046697 A1	USA	Operator Action Authentication In An Industrial Control System
7	US 2015/0296619 A1	USA	Industrial Control System Cable
8	US 2015/0154136 A1	USA	Input/Output Module With Multi Channel Switching Capability
9	US 8,971,072 B2	USA	Electromagnetic Connector For An Industrial Control System
10	US 2015/0123490 A1	USA	Electromagnetic Connector
11	App. No. 14/381,140	USA	Smart Power System
12	US 8,862,802 B2	USA	Serial and Parallel Communications Switch Fabric
13	US 8,868,813 B2	USA	Serial and Parallel Communications Switch Fabric
14	App. No. 29/462,572	USA	Backplane For An Industrial Control System
15	US 2015/0236981 A1	USA	Communication Network Hopping Architecture
16	CN 104025387 A	China	Electromagnetic Connector & Comms/Control System/Switch
17	CN 104134512 A	China	Electromagnetic Connectors
18	CN 104347256 A	China	Electromagnetic Connector
19	ZL 201430023921.0	China	Backplane For An Industrial Control System
20	ZL 201430023931.4	China	Power Module For An Industrial Control System
21	CN 104850091 A	China	Secure Power Supply For An Industrial Control System
22	CN 105278327 A	China	Industrial Control System Redundant Controller Authentication
23	CN 105278398 A	China	Operator Action Authentication In An Industrial Control System
24	CN 104852839 A	China	Communication Network Hopping Architecture
25	CN 105281061 A	China	Industrial Control System Cable
26	EP 2798707	Europe	Electromagnetic Connector & Comms/Control System/Switch
27	EP 2811496	Europe	Electromagnetic Connectors
28	1402820-0001 to 1005	Europe	Backplane For An Industrial Control System
29	EP 2908193	Europe	Secure Power Supply For An Industrial Control System
30	EP 2966806	Europe	Industrial Control System Redundant Controller Authentication
31	EP 2966520	Europe	Operator Action Authentication In An Industrial Control System
32	EP 2908488	Europe	Communication Network Hopping Architecture
33	EP 2966950	Europe	Industrial Control System Cable
34	Pub. No. 2015-505440	Japan	Electromagnetic Connector & Comms/Control System/Switch
35	Reg. No. 1504043	Japan	Power Module For An Industrial Control System (ICS)
36	Pub. No. 2014-220494	Japan	Electromagnetic Connectors
37	Pub. No. 2015-032836	Japan	Electromagnetic Connector
38	Reg. No. 1509447	Japan	Backplane For An Industrial Control System
39	Pub. No. 2015-156786	Japan	Secure Power Supply For An Industrial Control System
40	Pub. No. 2016-019280	Japan	Industrial Control System Redundant Controller Authentication
41	Pub. No. 2016-019281	Japan	Operator Action Authentication In An Industrial Control System
42	App. No. 2015-136186	Japan	Industrial Control System Cable
43	Reg. No. 30-784311	Korea	Backplane For An Industrial Control System
44	Reg. No. 30-778929	Korea	Input/Output Controller For Industrial Automation System
45	Reg. No. 30-778929-1	Korea	Communication Controller For Industrial Automation System
46	Reg. No. 30-778929-2	Korea	Power Supply For Controller For Industrial Automation System
47	App No. 103300681	Taiwan	Backplane For An Industrial Control System
48	Reg. No. D164951	Taiwan	A Portion Of Power Module For An Industrial Control System (ICS)
49	Reg. No. 154938	Canada	Backplane For An Industrial Control System
50	Reg. No. 154939	Canada	Power Module For An Industrial Control System (ICS)
51	App. No. 2,875,517	Canada	Secure Power Supply For An Industrial Control System (ICS)
52	App. No. 2,875,518	Canada	ICS Redundant Communications/Control Module Authentication
53	App. No. 2,875,515	Canada	Operator Action Authentication In An Industrial Control System

Table 4: Bedrock Automation OSA™ Security Related Patents

End of white paper.