GE Energy Connections

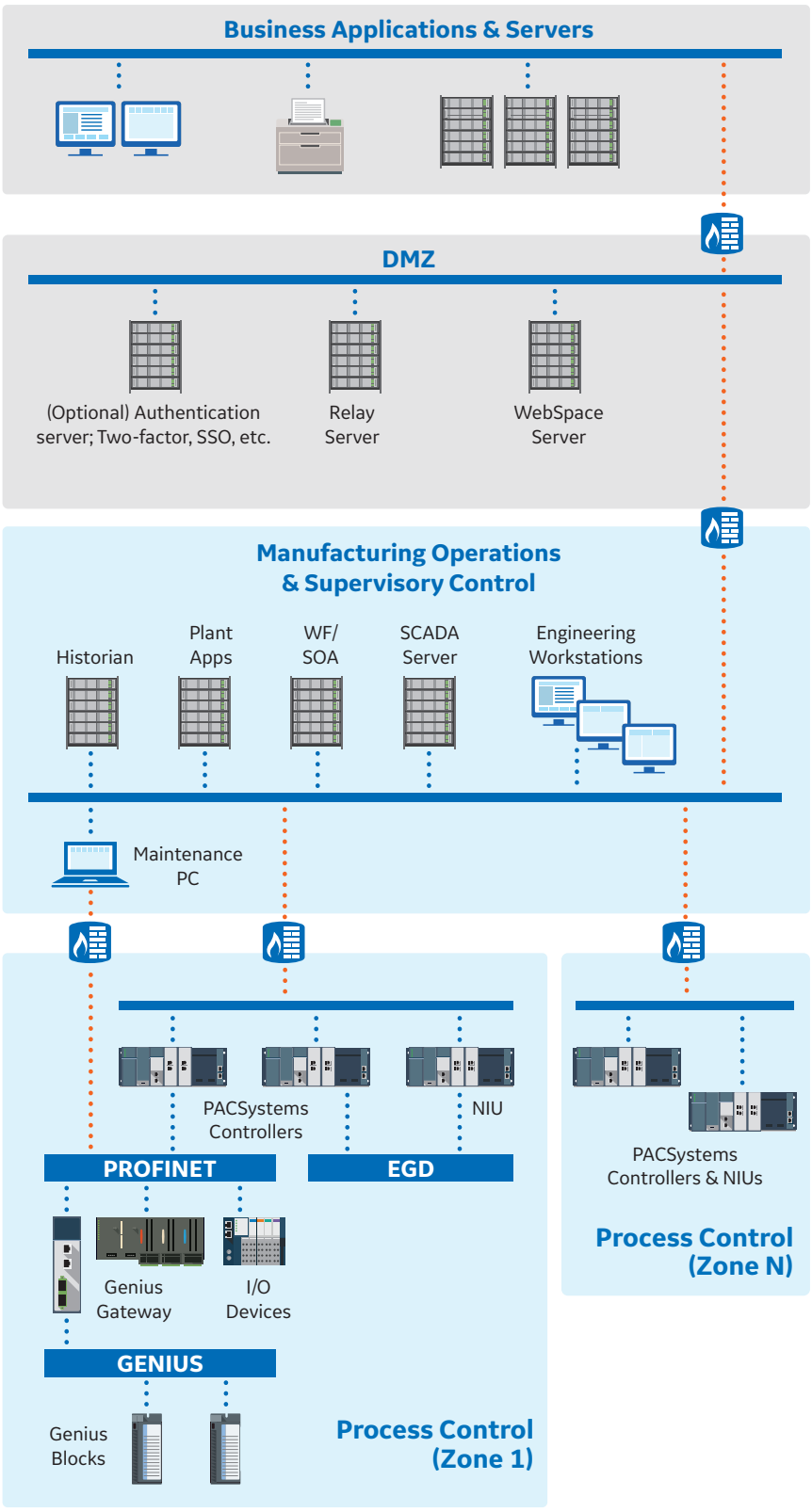
Cyber Security by Design – GE's Automation & Controls

Cyber Security by Design – GE's Automation & Controls

GE introduced the Industrial Internet Control System (IICS) where systems can exchange information across the globe. With the introduction of the IICS, cyber security has been an active topic of conversations. Malicious attacks occur daily across the globe so some have been reluctant to be early adopters of the IICS platforms. The consideration of cyber security isn't new at GE.

GE has taken an aggressive approach in circumventing attackers through a Defense-In-Depth approach, going beyond just leading edge technologies to implement an array of solutions to protect our critical infrastructures. Defense-In-Depth means that cyber security can be and should be applied at every level of product implementation.

GE distributes Secure Deployment Guides for product families that address cyber security. These guides address implementation considerations that customers can use to restrict access by malicious hackers. Common elements of a secure deployment could include firewalls to block unsolicited incoming traffic, and isolating networks to restrict data transfer to only the needed devices. Industrial routers can be implemented to manage data transactions between those isolated networks.



The Secure Deployment Guides provide examples of checklists to help guide the process.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node.
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram.
5. Configure firewalls and other network security devices.
6. Enable and/or configure the appropriate security features on each GE product.
7. On each GE product, change every supported password to something other than its default value.
8. Harden the configuration of each GE product, disabling unneeded features, protocols and ports.
9. Test/qualify the system.
10. Create an update/maintenance plan.

The Secure Deployment Guides do not include the scope and scale that GE has implemented within product designs. The security measures that GE implements are not common knowledge, and may contribute to the confusion or concerns about adopting IICS. We want users to fully understand the measures that have been taken to ensure the security of our controls platforms.

Communications

Some of the fundamental steps to combat cyber security start at the communications link to the devices. Only the essential ports and protocols are supported. All other ports and protocols are removed. Station Manager, USB and SD card ports are disabled by default. Access to the devices is restricted to only what is needed for the supported communications protocols: HTTP Proxy support for controlled access to the Internet, HTTPS protocols with certificates for secure Predix connection on the WAN. For Field Agent products, GE has implemented a private cellular network with carriers.

In addition, enhanced communications protocols are encouraged. OPC-UA is becoming a widely accepted manner of secure communications between systems. OPC-UA is platform independent and no longer requires security of COM/DCOM. OPC-UA security allows for managed certificate exchange between client and server. This certificate is an electronic ID held by the application that defines the identity of the holder. These certificates conform to the X509 specification.

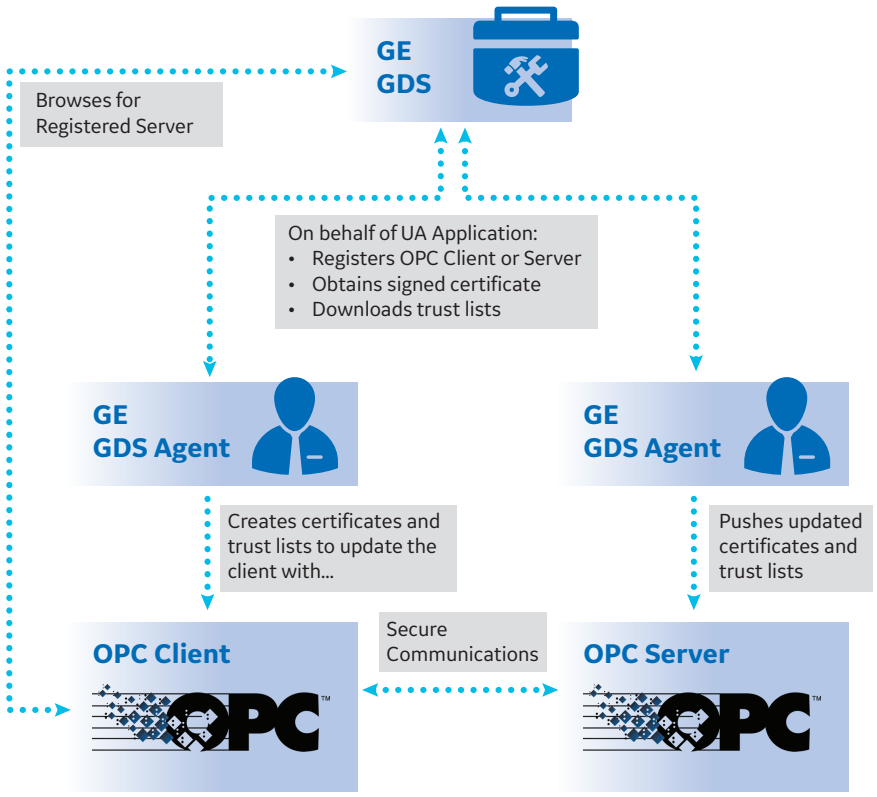
The data is encrypted between end points of the OPC-UA exchange to deny man-in-the-middle access. Even with its enhanced features, OPC-UA is IT network friendly and communicates through standard HTTP or UA TCP port. UPC-UA can connect securely over VPN and through firewalls.

Defense-In-Depth Review

As part of a product development cycle, the component is put through Defense-In-Depth review where the hardware and software are scrutinized with privileged knowledge of design and implementation. Testing and review is performed to mitigate possible attack vectors. Possible hidden passwords, software or hardware vulnerabilities, enabled through modified jumper settings, are evaluated. Possible open system boot vectors are evaluated.

Secure Remote Password Protocol

When a user authentication is required between client application(s) and server, a Secure Remote Password Protocol (SPR6a) has been implemented. SPR6a allows for a client side application to submit an authentication sequence to a server, where the actual password is never revealed. What the server understands is a cryptographically secure one-way value that was derived based on the user's password. So if an eavesdropper, or man in the middle, attempts to get between the client and server, there is no way for the attacker to obtain the password. SRP6a is a new class of strong authentication protocols that resist all the well-known passive and active attacks over the network.



GE's OPC-UA Global Discovery Server

Securely manages the authentication and certificate exchange between OPC-UA client and server.

Trusted Platform Module

The Trusted Platform Module (TPM) is a separate hardware module with a dedicated microcontroller providing cryptographic keys. Since each TPM chip has a unique and secret RSA key burned in, it is capable of performing platform authentication. Software can use TPM to authenticate hardware devices.

TPM can be used for encryption and decryption operations. TPM is a great source for a random generator, used for entropy in encryption and system validation. The random generator makes it virtually impossible for any other system to duplicate. This unique number can be combined with the server public key to create an encrypted link between two ends. Since the TPM has generated this non-repeatable number, outside influences can't decipher the data being transmitted.

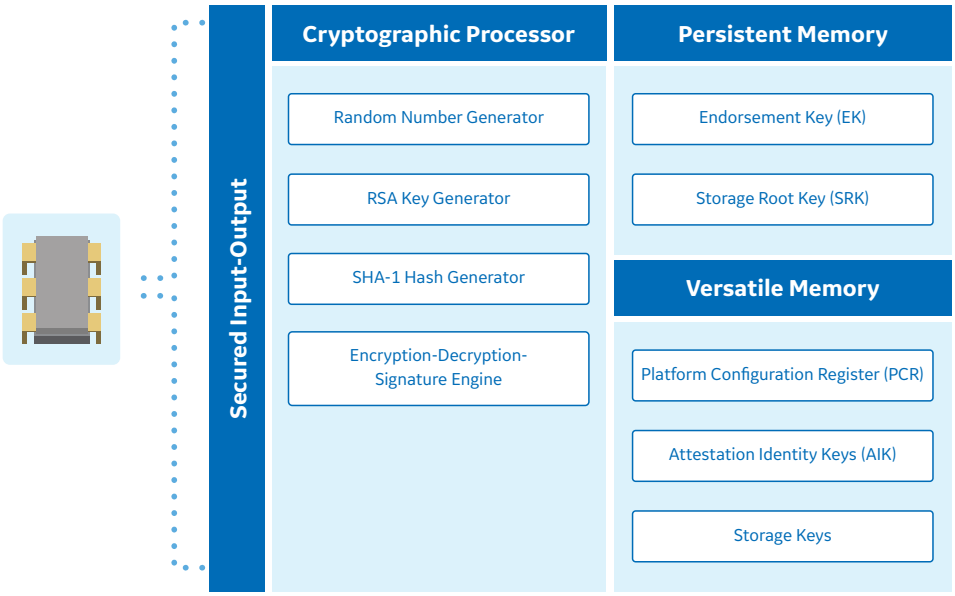
TPM can be implemented on any computer platform and is required by the United States Department of Defense (TPM version 1.2 or higher) for many of their devices, including phones and computers. TPM forms a "root-of-trust" in conjunction with BIOS.

Roots of Trust (RoT) is a set of functions in the trusted computing module that is always trusted by the computer's operating system (OS). The RoT serves as a separate compute engine, controlling the trusted computing platform cryptographic processor on the device it is embedded in.

TPM allows secure storage and reporting of security metrics that can be used to validate the system's configurations and therefore ensure changes haven't occurred.

Remote Attestation can be facilitated when the TPM creates a nearly unforgeable hash key that is a signature of the hardware and software configuration. This allows third party systems to verify that the software has not been changed.

Binding by encrypting data uses TPM bind key, a unique RSA key descended from a storage key. If the TPM binds data, then data is simply encrypted using asymmetric cryptography. The asymmetric keys used for binding can be migratable or non-migratable storage keys. If non-migratable storage keys are used, the encrypted data is bound to a specific platform. Otherwise, we have no platform binding and the cipher text can be decrypted on different platforms using the appropriate private key.



Sealing by encrypting data in a similar manner to binding, but in addition specifies a state in which TPM must be in order for the data to be decrypted (unsealed). Contrary to binding, only non-migratable storage keys can be used to seal data. Consequently, the encrypted data is always bound to a specific platform.

Secure Boot

Secure Boot is a technology where the system firmware checks that the system boot loader is signed with a cryptographic key authorized by a database contained in the firmware. It is used by UEFI (Unified Extensible Firmware Interface) in conjunction with BIOS for controlled boot where it prevents the execution of unsigned programs.

Secure Boot will revoke known-bad certificates and application hashes. Secure Boot enables TPM but doesn't require TPM during BIOS boot process. Secure Boot's responsibilities are prior to operating system loading.

Trusted Boot

Trusted Boot takes over where Secure Boot leaves off. Trusted Boot verifies the digital signature of the OS. In turn, the OS verifies the components it will use in the start up process such as startup files and boot drivers. If a file has been modified the boot loader detects the change then refuses to load the corrupt component.

Trusted Boot will only use trusted software, often implemented by using signed and certified software from the manufacture.

Memory Management Unit

The Memory Management Unit (MMU) is a hardware component that controls all memory and caching operations associated with the processor. The MMU primary roll is to translate virtual memory addresses to physical memory addresses.

MMU functions can be defined in three categories:

1. Hardware memory management, which oversees and regulates the processor's use of RAM and cache memory.
2. Operating System memory management, which ensures the availability of adequate memory resources for the objects and data structures of each running program at all times.
3. Application memory management, which allocates each individual program's required memory, and then recycles freed-up memory space when the operation concludes.

In the case of the hypervisor environment the memory usage is restricted. The different operating systems use different memory regions and are not allowed to directly interact between environments.

Achilles Testing

The Wurldtech Achilles Certifications are communications tests performed on devices while monitoring specific performance indicators. Achilles testing is categorized into three main groups.

Achilles Grammars - Achilles Grammars test for protocol boundary conditions in the device communications. They systematically iterate over each field and combinations of fields to produce repeatable, quantifiable tests of the common types of implementation errors. Achilles Grammars send invalid, malformed or unexpected packets to the Device Under Test (DUT) to test for vulnerabilities in specific layers of the protocol stack.

Achilles Storms - Achilles Storms generate packets at a high rate in order to examine the DUT's ability to handle high traffic rates for different protocols. The Achilles Test Platform also includes the ability to search for the denial-of-service threshold for a given type of storm traffic – the storm rate at which the device is no longer able to respond to other normal requests.

Known Vulnerabilities - Known vulnerability test cases generate exploit traffic for vulnerabilities that have a high probability of existing in control devices. (CERT list)

WurldTech further describes the Achilles Grammars test as a Fuzz test where invalid, unexpected, or random data is provided to the inputs. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks.

While conducting Achilles testing the equipment is monitored using communications responses, discrete and analog signals. The device must maintain the responses and signals throughout the test to within acceptable specification.

Extensible Systems Design

As cyber threats evolve the existing systems must be capable of changing to meet that threat. GE designs the controllers and field devices with the capability to adapt to future needs, creating environments that can be securely maintained to stay abreast of our changing world.

For some devices such as our Field Agents, updates can be remotely monitored and managed. This helps ensure that the operating systems stay current with the manufacturer's latest patches and security updates. Other devices, such as our controllers, require a physical connection to the local hardware for firmware updates. This security measure provides a physical gap that an attacker can't bridge. Encrypted and digitally signed firmware updates have also be introduced for enhanced security.

Security Monitoring

GE is actively monitoring and adapting to cyber security threats. GE has centers open around the clock to monitor cyber activity and adapt if needed. GE offers a number of methods to help our customers stay informed. The following links provide information about cyber security resources at GE.

GE's Automation & Controls Security webpage: http://www.geautomation.com/security

GE Product Security Advisories support page: https://ge-ip.force.com/communities/en_US/Article/GE-Intelligent-Platforms-Security-Advisories

GE Product Security Advisories - Auto-Notification Service: http://support.ge-ip.com/support/index?page=autonot&id=ST14

Third-Party Patch Validation: https://ge-ip.force.com/communities/en_US/Article/Information-on-Product-Compatibility-with-Critical-Microsoft-Security-Patches

Evolution of Security Requirements: http://support.ge-ip.com/support/index?page=alerts&id=2330110e3570c-01112cba473a007ba9&catnm=&cat=-GLOBAL_ALERT

Product Vulnerability and Security Concern Reporting:

E-mail: security@ge.com

Conclusion

With GE's introduction of the Industrial Internet Control System, the next evolution in controls technology has begun. The power of 1% is possible. Interconnected systems can provide efficiencies never before possible. The scope of the benefits of adopting the IICS can't be ignored if organizations want to be competitive in today's world economy. GE is providing safe, secure products to enable customers to be a part of this new evolution.

Where others have stopped, GE has continued to deploy layers of security, closing access to would be attackers through both hardware and software, by design. With security experts on hand GE continues to adapt to any security threat.

GE Energy Connections
Automation & Controls
2500 Austin Dr
Charlottesville, VA 22911
1-800-433-2682 or 1-434-978-5100
www.geautomation.com

1.17