Data Protection for Industrial Control Systems

Protection of Sensitive Data on Industrial Control Systems

DATA PROTECTION FOR INDUSTRIAL CONTROL SYSTEMS:

Protection of Sensitive Data on Industrial Control Systems

Industrial Control Systems (ICS) collect, process, and store sensitive apps, logs, and configuration files. ICS essential role in site operations makes them regular targets for espionage and sabotage. Lacking sufficient protection, these devices are susceptible to malicious attacks from insiders and external actors who seek to steal or manipulate data or compromise operations. Threats include both direct physical and remote device access.

Challenges to ensuring ICS data at rest (DAR) security include:

Protection and Availability

Ensuring data at rest remains secure while ensuring systems are constantly operational is a complex challenge, yet fundamental to the protection of these assets. Current protections are often inadequate in fully addressing all risks. Areas that may not be fully addressed include:

- *Ineffective Encryption*: Encryption is the foundational protection for DAR, but improper implementation, weak encryption algorithms, lack of sufficient authentication, and poor key management may compromise encryption effectiveness. Furthermore, utilizing software-only encryption presents risks as there are various techniques to circumvent software-only encryption.
- *Physical Device Access*: Adversaries who gain physical access to storage can clone, wipe, or employ a variety of advanced data recovery techniques, including chip off and post-quantum computing attacks that can overcome or bypass certain protections.
- *Operational Reboot*: Situations arise requiring a reboot of ICS devices in either a “warm” or “cold” reboot scenario. Data protections that compromise or inhibit an expeditious, autonomous reboot process will not be viable. Any protection approach will need to provide for such reboot requirements.

Ensuring Safe Updates

ICS devices require regular maintenance including software updates. These updates can be used to infect devices and/or extract data.Threat actors may seek to weaponize maintenance PCs or external media used for updates. Any ICS protection solution needs to address these devices, the systems being updated, and the update process.

Meeting Compliance
Government systems storing classified, CUI, and other sensitive data are required to meet multiple encryption and authentication compliance requirements such as FIPS, NIAP, CSfC, and other standards. Proposed solutions should, whenever possible, comply with or be certified to meet or exceed the relevant standards and certifications.

Preventing / Detecting Insider Threat
Insufficient protection may result in malicious insiders exfiltrating data or compromising ICS operations. Data Access Controls and proper authentication are fundamental to mitigating insider risks. Inadequate access controls allow unauthorized users to access sensitive information through oversight or exploitation of system vulnerabilities or credential theft. Even with proper access controls, detecting insiders and determining what data they accessed is a critical need. ICS storage lacks secure data access logging capabilities that could be utilized for detection and forensics.

Ensuring Full Device Sanitization
When a device requires sanitization, NSA Policy Manual 9-12 guidelines mandate device destruction requiring physical disintegration or incineration of storage. Meeting standards may be difficult to achieve due to mission parameters. Software-only tools and techniques are often ineffective in ensuring all data is destroyed. Furthermore, operators may utilize insufficient sanitization methods leaving vulnerable data at rest. Proposed solutions must include complete erasure verification that can be used during operations.

Device Monitoring
An enterprise-wide management system is essential to ensure that all devices across all facilities maintain their security configurations, are updated in accordance with changing policies, remain compliant with evolving requirements, and are consistently up to date in addressing regular CVE releases. Any proposed system, however, cannot introduce a threat vector. System access furthermore cannot be a requirement for system operation or reboot.

In conclusion, due to the critical role these devices play in operations and the sensitive data they collect, process, and store, ensuring their effective protection is essential. Security measures must provide granular access control with protections in place to ensure apps, logs, and configuration files are protected throughout their lifecycle.

To be effective, **protection must support the operational requirements** including providing secure maintenance, updates, and reboots.

CIGENT

Cigent Overview

To address the outlined risks, while ensuring operational availability on ICS, a layered approach, inclusive of secure storage, enhanced firmware, and data access control software is required. Cigent data experts have worked extensively with Federal agencies to develop methodology and apply technologies to support ICS operations and ensure data integrity throughout its lifecycle.

Key benefits of the Cigent solution include:

Protection for data while device is in-use.	FIPS-validated file encryption, MFA for file access, and whitelisted apps ensure access integrity and prevent unauthorized data access even while operational.
Malware prevention	Applications and configuration files are stored in secured, read-only partitions with limited access. A file filter driver prevents malware from being saved to writeable partitions.
Protection against insider threats	All data access is captured in secured logs with restricted access. Logs can be mined to detect nefarious actions.
Verified storage sanitization	Complete data destruction using both crypto and comprehensive block erasure validated by patented firmware-based verification built-in to storage.
Malware recovery	Software updates are stored securely on read-only partitions providing the ability to rapidly recover from malware.
Maintenance operations	Device status, compliance, and health across all PLCs, consoles, media, and maintenance PCs via central command and control center system.

Cigent Operational Approach

ICS role in the collecting, processing, and storing of sensitive apps, logs, and configuration files require layered protection and methodology that does not disrupt operations while ensuring data integrity and system resiliency. The integrated solution ensuring data integrity throughout its lifecycle addressing a myriad of threat vectors including data extraction or tampering, malware insertion, and insider threats. The solution is agnostic to the software or operating system being utilized by control system component.

The operational execution of Cigent capabilities are outlined in detail below.

Data at Rest Protection

Fundamental to data integrity is protecting data while in use and not in use. Data at rest (DAR) protection is provided with multiple security layers, using a defense-in-depth strategy to protect data from all adversarial attack vectors during all operational scenarios.

1. *Hardware Full Drive Encryption.*
   Encryption is AES-256 and FIPS compliant in accordance with the TCG (Trusted Computing Group) Opal 2.0 or similar guidelines. Storage may also adhere to the FIPS 140-2 Level 2 requirements, including using epoxy on the drives.

2. *Locked Ranges.*
   Ranges are defined segments of data storage that are monitored and protected independently. To protect data from attempts to wipe, clone, or view data at the hex level storage ranges are locked at the firmware layer, rendering the ranges/data unreadable by cloning tools and hex readers.

3. *ADR Protection.*
   To protect data from advanced data recovery methodologies such as chip off or utilization of an electron microscope:
   - All storage utilizes hardware encryption. If an adversary removes the data from the drive with advanced techniques, the data remains in an encrypted state. Without the decryption key, adversaries will be unable to decrypt the data.
   - The key will not be stored in its entirety anywhere on the drive and the pieces of it that are stored on the drive will be encrypted. Between these two measures, the key will not be able to be accessed or recreated.

4. *Secured Firmware.*
   In addition to the encryption capabilities, the storage firmware has been modified to resist advanced threat vectors. SSD firmware has been modified to meet compliance with FIPS 140-2, NIAP Common Criteria FDE_EE standards, and CSfC DAR Capabilities Package 5.0 requirements. Including:
   - Standalone approved cryptographic algorithm certification, power-on self-tests of all cryptographic algorithms, a module entering error states when any cryptographic function fails, NIST approved methods for cryptographic key generation and using approved techniques for the generation of random bits, and minimum entropy of hardware random bit generator evaluated according to SP 800-90B, and tamper-evidence protection.

Multiple security layers ensure protection against all adversarial attack vectors during all operational scenarios.

Pre-boot Authentication

Pre-boot authentication (PBA) provides a secure user authentication platform on the device that is fully protected at rest. Properly configured PBA prevents adversaries from circumventing encryption by manipulating the boot process.

1. Prior to proper pre-boot authentication, the entire drive, minus a small Shadow MBR (Master Boot Record) partition, will be locked in a locked range.
2. Upon power-up, an O/S designated for the purpose of authentication will boot from the shadow partition and pre-boot authentication (PBA) software will load.
    a. The PBA software has been validated to meet FIPS CAVP, NIAP Common Criteria FDE_AA, and CSfC DAR Capabilities Package 5.0 requirements.
3. Upon boot, authentication will take place in a manual manner if an end user can be involved in the boot process. If infeasible, an autonomous manner, so as not to impede the boot process and facility operations, while still meeting best practices and compliance requirements as much as possible in this environment, will be used.
4. Multifactor Authentication is supported with factors including Trusted Platform Module (TPM) 2.0 detection/processing, Hardware Security Module (HSM) - FIPS where possible, a security key (i.e. YubiKey), and/ or detection of a specific network device. MFA for File Access. When a file is attempted to be accessed, the file filter driver will be engaged and determine whether to require MFA. This prevents malicious actors from extracting files from systems.

Protection while Device is In-use / Malware Prevention

Methodology and technology designed and tested for ICS will not impede operations while mitigating risk of unauthorized data exfiltration and minimizing malware compromise and eliminating risk of spread.Cigent utilizes separate ranges that can segregate apps, logs, and configuration files limiting access and mitigating risk of malware compromise.

CIGENT

Pre-Boot Authentication (PBA) provides robust security, ensuring the device is fully protected at rest. By loading secure authentication software from a locked Shadow MBR partition, **PBA prevents adversaries from manipulating the boot process and supports multifactor authentication**, including TPM 2.0, HSM, and security keys.

1. *Locked Ranges*. Devices can be configured where data, software, and configuration files can be stored separately providing the ability to create “read only” secure enclaves where software and configuration files will be sequestered. Devices will still be able to “write” collecting and processing data as their role requires. These partitions will also enable access controls defined by user requirements.
2. *File filter driver*. Once the O/S loads a file filter driver will be initiated. The file filter driver will provide a layer of runtime protection ensuring only appropriate (allow list) apps and processes can access and save files, preventing malicious access, data extraction, and compromise (such as modification, deletion, overwriting, etc.)
3. *App Whitelisting.* The appropriate file or application for accessing a file can be allow list preventing the MFA prompt. This ensures proper execution of the system functionality, while simultaneously preventing malicious access and data extraction.
4. *OS partition*. The O/S partition will further be mounted in read-only mode. This will ensure malware is not loaded on this partition and a reboot process will reload the system into a known good state.

Data Access Control

Access is controlled with 2FA/MFA. In the event an adversary attempts to access files in an unauthorized manner, a prompt will be displayed, requiring the user to authenticate. If they are unable to authenticate, they will not be able to access the file. An adversary attempting to access a file will not disrupt the allow list apps or processes from accessing the file. All access log attempts will be stored on the system in a secure location in a special log file designated for this purpose.

Recovery Capabilities

Effective recovery from a malware attack requires the ability to rapidly return systems to a “known good state. Standard base configurations would be secured in “read only” partitions with restricted access.If control system components were affected by malware or an unapproved change, these base configuration files could be accessed and used to “reboot” the system. The approach provides a failsafe against an attack to subvert ICS operations.

Insider Threat Protection.

Mitigation of risks associated with malicious insiders includes preventive protection and protected log files of data activity.

1. *File Level Encryption.* Preventive protection is delivered through file level encryption that encrypts data collected and stored on ICS devices. File level encryption sustains encryption protection if data is removed from the device. The approach prevents an insider from exfiltrating data in clear text.
2. *Secure Data Logs*. Document immutable records for all data activity. These tamper-proof records can be examined for potential malicious activities and used in forensic investigations.

Both system and firmware logs can be captured and uploaded to the enterprise management software for reporting, analysis, and suspected insider threat alerts. These can also be exported to a SIEM for ongoing analysis.

Data Sanitization

Data on ICS that are repurposed or at end-of-life needs to be sanitized. Sanitization solution will include the ability to both erase and verify data has been erased. The solution may provide an alternative to physical device destruction and can be used in emergency situations.

1. *Crypto and block erasure*. Crypto erase deletes encryption keys thereby rendering data permanently inaccessible. Block erase utilizes an electrical charge to erase data.
2. *Verified Data Erasure*. Firmware immediately verifies that all data has been erased with block-by-block analysis. Block erasure can be re-run until all data successfully sanitized.
3. Sanitization can be executed remotely or locally.

Maintenance Operations

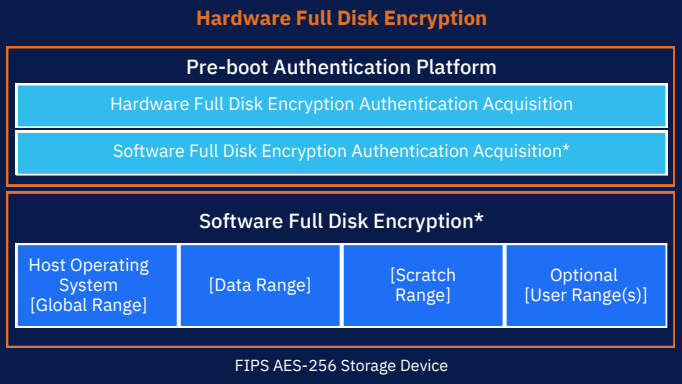
An effective data protection solution requires methodology for updates and management. Cigent capabilities include maintenance PCs and external media to support secure and efficient maintenance operations. This is to mitigate risk of the insertion of malware on ICS devices or the malicious utilization of these devices to exfiltrate data. Additionally, the solution will be capable of having engineering agents change software configurations both manual ISEA engagement or a secure ISEA approved remote update solution.

Architecture

Overview

The foundation of security architecture is rooted in the storage itself. Storage devices that are equipped with hardware encryption (HW FDE) ensure that data, software, and files are protected within the drives.

In addition to HW FDE, advanced storage technologies within the drives offer further security through Pre-Boot Authentication (PBA), and software full disk encryption (SW FDE).



The SW FDE component can be implemented for Windows and Linux. Authentication acquisition for the hardware full drive encryption will be performed from the PBA application (discussed below). Once the hardware layer authentication is complete, the PBA application will hand off control to the software layer authentication acquisition application. Each layer will use an alternate acquisition system and credential set. The SW FDE layer will not use the same encryption code that provides the hardware based outer layer of protection.

There is support for additional file encryption that includes the following features: FIPS-validated, AES-256 encryption, extension specific encryption (all files in the set of protected extensions are automatically encrypted), folder-based encryption (all current and future files in the folder are protected), and multi-user shared file support.

Enterprise Management Software

The Cigent Data Defense Software and service will load on boot and can authenticate to the on-site Cigent Enterprise Management Software. The Management Software provides both centralized and decentralized management of all devices, including reporting on policy compliance, pushing policy and configuration updates, ensuring that systems maintain their configurations, and detecting the possibility of threats on the system.

The Management Software can also push logs to a SIEM. This integration would allow a place to consolidate threat events and logs in a single "pane of glass" for security analysts. If desired, this could lead to insider threat log analysis paving the way for early detection of espionage. Once established the user can also receive threat event notifications that would further speed up the time to catch and mitigate threat activity.

Drive Portfolio

Cigent portfolio of drives will enable coverage for PLCs, consoles and PCs.

	SATA 2.5 & M.2	M.2 2280	M.2 2230	SSD BGA	SD & Micro SD Cards
SED	Yes	Yes	Yes	Yes	Available HW encryption
TCG OPAL	Yes	Yes	Yes	Yes	No
AES 256	Yes	Yes	Yes	Yes	Yes
FIPS 140-2 Level 2 Validated	No	Yes	No	No	No
FIPS 140-2 Level 2 Compliant	Yes	Yes	Yes	Yes	TBD
NIAP CC FDE_EE Compliant	Yes	Yes	Yes	Yes	TBD
CSfC for DAR Compliant	Yes	Yes	Yes	Yes	TBD
Temperature	-40 to 85C	-40 to 85C	-40 to 105C	-40 to 105C	-40 to 85C
Tamper-proof	No	Epoxy	Inherent	Inherent	Inherent
Cigent Features	Verified Data Erasure Secure Data Logs	Verified Data Erasure Secure Data Logs	None (optional)	None (optional)	No

Compliance Regulations

FIPS Certifications

- Cigent Secure SSD M.2 2280 are AES256 and FIPS 140-2 Level 2 validated
- Cigent PBA Software is FIPS CAVP validated
- Cigent's File Encryption is FIPS 140-2 Level 1 validated

NIAP Common Criteria and CSfC DAR Capabilities Package 5.0

- Full Drive Encryption Engine: while the Cigent branded drive has not been through the NIAP and CSfC validation processes, the identical drive by partner drive manufactures has successfully completed certification. Therefore, drives meets all requirements.
- Authentication Authorization: the Cigent PBA Software has been certified by NIAP and the CSfC and is on the Product Compliant lists.

Executive Order (14028) on Improving the Nation's Cybersecurity dated May 21, 2021

- Implementation of both MFA and multiple layers of encryption, including file encryption, meets the EO requirements.

Cigent certifications include:

- NIST FIPS CAVP Cert 4388
- NIST FIPS 140-2 Level 1 Cert 4186
- NIAP Common Criteria FDE_AA Cert 11378
- NSA CSfC DAR Hardware Full Drive Encryption

For a comprehensive **list of compliance requirements** that can be achieved using Cigent solutions, please visit **https://www.cigent.com/compliance**.

CIGENT

Cigent Organization

Experience

Cigent Secure Storage Solutions are currently utilized with multiple US Federal Agencies employed in various use cases, form factors, and operating environments. The secure storage drives are utilized extensively in multiple DoD programs, are deployed in manned and unmanned vehicles, and are deployed within US military services and the Intelligence Community.

For the CSfC (Commercial Solutions for Classified) community and customers, Cigent provides a comprehensive range of services and support designed to meet the highest security standards for classified information. This includes assisting in the design and deployment of CSfC solutions tailored to specific mission requirements, ensuring alignment with NSA standards for classified communications. Cigent can also enable navigation of the certification process, ensuring solutions comply with CSfC program requirements and are ready for operational deployment.

Facilities

Cigent Technology, Inc.
2211 Widman Way, Suite 150, Ft. Myers, FL 33901

Main Research Laboratory: The facility contains a state-of-the-art laboratory equipped with advanced analytical instruments, including NVRAM chip reading equipment, high-performance bus analyzers and oscilloscopes. It will serve as the primary facility for conducting research and development, ensuring precise and accurate measurement of samples critical to the project's success.

Testing and Validation: The facility includes specialized equipment for stress testing and quality assurance. It will be utilized to validate the durability and effectiveness of the project outputs under various conditions, ensuring that all products meet the required safety and performance standards.

Data Analysis and Processing: This area is equipped with high-performance computing systems and advanced data analytics software. It will be used for processing large datasets generated during the project, enabling detailed analysis and modeling to support decision-making and optimize project outcomes.

Contact Us
Phone: 669-400-8127
Toll Free: 1-844-256-1825
Email: info@cigent.com