CASE STUDY

Moxa

Increasing Cybersecurity Endpoints Protection with Moxa V2406C Series Industrial Computers

Defend against cyber threats and protect sensitive data with a more secure computing platform and Intel hardware-enabled security solution

Table of Contents:

Introduction

In today's age, data has undoubtedly become a lifeblood of modern businesses, providing valuable insights to optimize real-time management over critical processes and operations. Every day, large amounts of data are routinely collected in real-time from sensors and IoT devices operating in remote locations or harsh environments around the world. This virtual ocean of data is ever-growing, and it is changing the way businesses operate as well as their IT infrastructure. A traditional computing paradigm that is built on a centralized data center, coupled with internet bandwidth limitations no longer fits the growing flow of fast-paced real-time data. Latency and unpredictable disruptions can compromise operations. Today, businesses are adopting edge computing architecture as a response to these data challenges. Edge computing is a distributed computing paradigm that moves a portion of the computation and data storage closer to the location where the data is produced, such as the IoT devices or local edge servers.

The adoption of edge computing can significantly reduce the latency of applications while enabling AI-powered functionality and user experience. However, with the proliferation of edge computing, more devices are placed in dispersed locations, leading to a greater risk of interference or damages from unauthorized access or physically tampering with devices if cybersecurity measures are not adjusted to fit the new paradigm. Defending endpoints from the malicious activity is crucial as it can prevent hackers from stealing data, sabotaging critical operations, or gaining access to the corporate infrastructure and systems. Without proper Operational Technology (OT) endpoint protection, companies will be at significant risk of cyberattacks which can severely affect the entire business operations and IT infrastructure. In recent years, the railway sector has increasingly come under attack from cyberthreats.[1] Experts believe the risk of cyberattackers disrupting the public railway systems is growing, as malware may be lurking in critical safety systems which can pose significant threats to the operations.[2] In 2020, a Swiss rolling stock manufacturer's IT network was attacked by malware and when the company refused to pay a $6m ransom, documents stolen during the cyber-attack was published online.[3]

As cyberattacks are evolving, software alone is no longer sufficient to protect against these security threats. Software can be spoofed by breaches that allow hackers to gain access to a business system. Partnering with Intel, Moxa provides solutions that are designed to be both breach-resistant and breach-ready through the combination of software and hardware-based security features to support their partners in their cybersecurity framework and help keep data center infrastructure secure in the OT space.

About Moxa*

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service.

Intel Hardware Security: The Foundation to Next-Generation Secured Industrial Computers

Security is a system property rooted in hardware, with every component from software to silicon playing a role in helping secure data and maintain device integrity. We have a suite of technologies to build and execute on a defense-in-depth strategy, with solutions spanning threat detection, data/content protection, memory protection, and more.

Intel's hardware security technologies meet specific challenges centered around three key priorities:

- Foundational Security
  Ensuring a critical base of protection across the platform, and focused on identity and integrity. Intel has a long history of delivering technology to help ensure the platform comes up correctly and runs as expected. Our security engines have been used more than a billion times worldwide, and our processors feature enhanced cryptography to accelerate performance and help secure global commerce.

- Workload and Data Protection
  Providing every legitimate workload with a trusted execution environment for hardware-isolated protection of data in use, scaled to fit workloads of varying sizes. Once we have a solid foundation, security technologies extend to help protect virtual machines and operating systems against targeted attacks.

- Software Reliability
  Intel delivers hardware platforms with protections against common and emerging software attacks, which increases efficiency and preserves performance. We are working to harden the software and move select security capabilities to hardware, adding more layers of verification.

Intel hardware-enabled security technology found with Intel® processors in Moxa V2406C Series:

1. Intel® Boot Guard
   Intel® Boot Guard provides a key element of hardware-based integrity that meets Microsoft Windows requirements for UEFI Secure Boot to mitigate unauthorized BIOS boot block modifications. It verifies the correctness of this code before the CPU runs the IBB. When booting with Intel Boot Guard enabled, the boot integrity is unalterable since it is anchored in hardware fuses. Intel Boot Guard becomes a hardware root of trust adding robustness to the chain of trust process where the UEFI boot process cryptographically verifies and/or measures each software module before executing it. The result of the Intel Boot Guard process is a reduction in the chance of malware exploiting the hardware or software components on the platform.

2. Intel® Trusted Execution Technology (Intel® TXT)
   Intel® Trusted Execution Technology is a set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. Intel Trusted Execution Technology provides hardware-based mechanisms that help protect against software-based attacks and protects the confidentiality and integrity of data stored or created on the client PC.[4]

3. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
   Intel® AES-NI improves on the Advanced Encryption Standard (AES) algorithm and accelerates the encryption of data in the modern Intel processors for endpoint computing devices. Composed of seven new instructions, Intel AES-NI makes pervasive encryption feasible in endpoint computing devices.[5]

Moxa V2406C with Industrial OT Security in Mind

1. Secure Boot with Moxa V2406C
   Secure Boot is a security protection mechanism that is designed to ensure the computer always boots from a validated and authorized bootloader and operating system. This helps in preventing unauthorized software like malware from taking control of the computer during the boot-up process. Moxa V2406C adopted TPM 2.0 as the hardware Root of Trust (RoT). The hardware adopted a secure boot chain with Intel® Boot Guard to have digital signatures signed at all critical booting stages, from processor to BIOS to Linux operating system. This helps ensure the root of the validation process is always trusted. The Moxa V2406C series is designed for confidential information protection and meets the IEC 62443-3-3 and IEC-62443-4-2 system security requirements.

2. Full Disk Encryption with Moxa V2406C
   Full disk encryption is mainly used to prevent exposure of confidential data from stolen hard disk by completely encrypting the entire hard disk. Moxa Computer uses TPM 2.0 to store and protect each computer's unique disk decryption key. The decryption key from TPM 2.0 only becomes accessible when the secure boot process has been validated. Therefore, creating a chain-of-trust validation process to help ensure the data in the hard disk can only be accessed from the specific Moxa computer. Powered by Moxa Industrial Linux (MIL) 2.0, the Moxa V2406C series is designed for confidential information protection, in meeting IEC 62443-3-3 system security requirements.

Moxa Industrial Linux (MIL) 2.0 is a high-performance industrial-grade Linux distribution developed by Moxa for Industrial applications. MIL 2.0 is based on Debian 10 with kernel 4.19, and is integrated with several feature sets designed to strengthen and accelerate user's application development, as well as ensuring the reliability and security of the system deployment. MIL 2.0's key features include secure boot, secure update, backup and recovery, Input-Output (I/O) interface and network connection management.

As railway networks get busier and busier, Intel and its ecosystem are driving the future of railway industries. Working with our industry partners, our solutions help railway industries achieve safety and security from trackside to control center through secure boot, attestation, and content protection.

Case Study: V2406C Industrial PC for Reliable Railway Passenger Information System (PIS) and Gateway Network Video Recorder (NVR), Start with Security in Mind

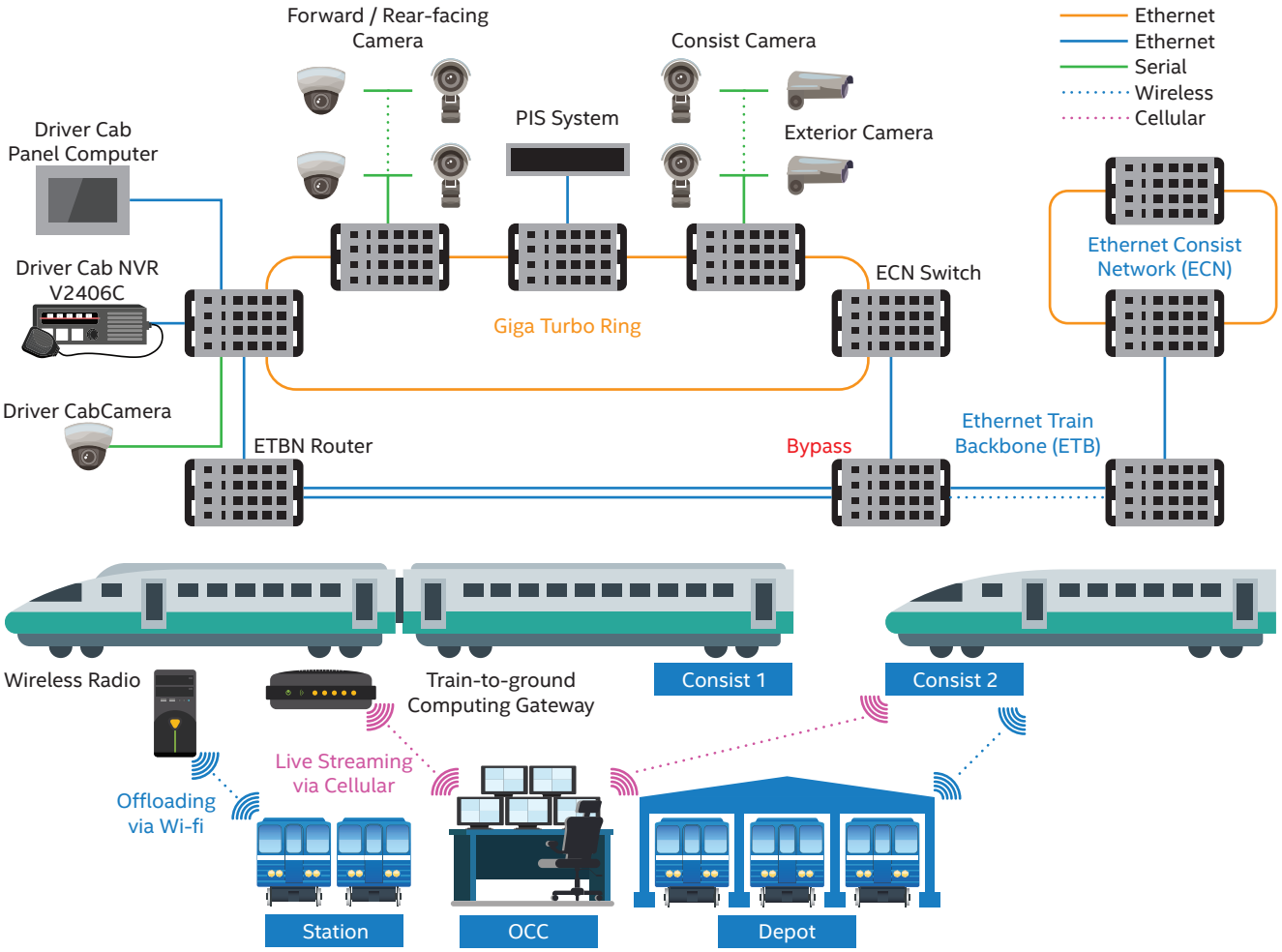

Figure 1. Rolling Stock NVR

Introduction on Moxa V2406C Industrial PC

Moxa's Industrial PC (IPC) V2406C series are rugged Artificial Intelligence of Things (AIoT) edge computers designed for tough environments. The high-performing, robust, and more secure V2406C series rail computers designed for IEC-62443-4-2 level 2 reachable are built around an Intel® Core ™ i7/i5/i3 or Celeron® high-performance processor and come with sufficient memory storage expansion and wireless connectivity support, all in a compact casing. As onboard train systems operate in harsh environments for extended periods of time, they must be sufficiently rugged and resistant to withstand high humidity, variable temperatures, and persistent vibration, while also fitting in restricted quarters with wire restrictions. Having passed rigorous tests and strictly adhering to industrial standards, the V2406C series can provide long-lasting, reliable operation even in harsh environments and on trains moving at high speed, making it perfect for AI and edge computing applications in the rail industries. Equipped with a rich set of interfaces including 2 Gigabit Ethernet ports, 4 RS-232/422/485 serial ports, 6 DIs, 2 DOs, 4 USB 3.0 ports, 2 mPCIe wireless expansion slots, and 4 SIM-card slots, the V2406C series is suitable for railway onboard and wayside applications. These interfaces help establish redundant LTE/Wi-Fi connectivity, ensuring solid bidirectional communications between a fast-moving train and the wayside applications.

Challenge: Legacy rolling stock requires manual maintenance

The V2406C series is deployed as a Network Video Recorder (NVR) computer on both new and legacy rolling stock for surveillance purposes. However, a reliable internet connection may not be available for legacy rolling stocks to synchronize the surveillance footage back to the Operations Control Center (OCC) in real-time. Hence, the two hot-swappable HDD/SSD on the V2406C Series containing the surveillance footage is periodically transferred to the server in the OCC through manual maintenance done by maintenance staff. In addition, other maintenance activities such as BIOS and OS upgrade via USB are performed by the maintenance staff as well. The surveillance footage captured in the V2406C series is regulated by General Data Protection Regulation (GDPR). Hence, any threats of data theft or unauthorized exposure have become a top concern for asset owners. Although the V2406 series is placed in a secure cabinet, a defense-in-depth strategy is required to mitigate threats from certain scenarios. For example, unauthorized data exposure may occur due to stolen or missing HDD during the maintenance period or in between the transfer from train to OCC. Besides that, unauthorized data exposure may occur during the decommissioning stage as well. Lastly, unauthorized data exposure can occur during an intentional or unintentional installation of malicious BIOS or OS by the maintenance staff.

Solution: Preconfigure measures to enhance security

The V2406C series features full disk encryption is designed to protect the storage of sensitive data, helping ensure that this data can only be read by the authorized device or personnel. By using Intel® Boot Guard as a hardware root of trust to initiate a chain of trust validation sequence during boot time, the V2406C series
helps ensure the integrity and authenticity of BIOS and OS during boot time before decrypting the storage for data access. Leveraging on Intel® Boot Guard, the Moxa public key is stored in the One Time Programmable (OTP) CPU fuse to help ensure the root of the validation process is always trusted.

Furthermore, during the manufacturing stage, each Moxa V2406C series's unique software and hardware footprint are bound with Trusted Platform Module (TPM) 2.0 secure storage access, which helps ensure the encrypted storage can only be decrypted on this very specific Moxa device. The decryption keys from TPM 2.0 are only accessible once the secure boot process has been validated. Therefore, creating a chain-of-trust validation process that helps ensure data in the hard disk are only accessed from the specific Moxa device, which helps in preventing unwanted exposure of confidential data from stolen hard disk. (Refer to figure 2)

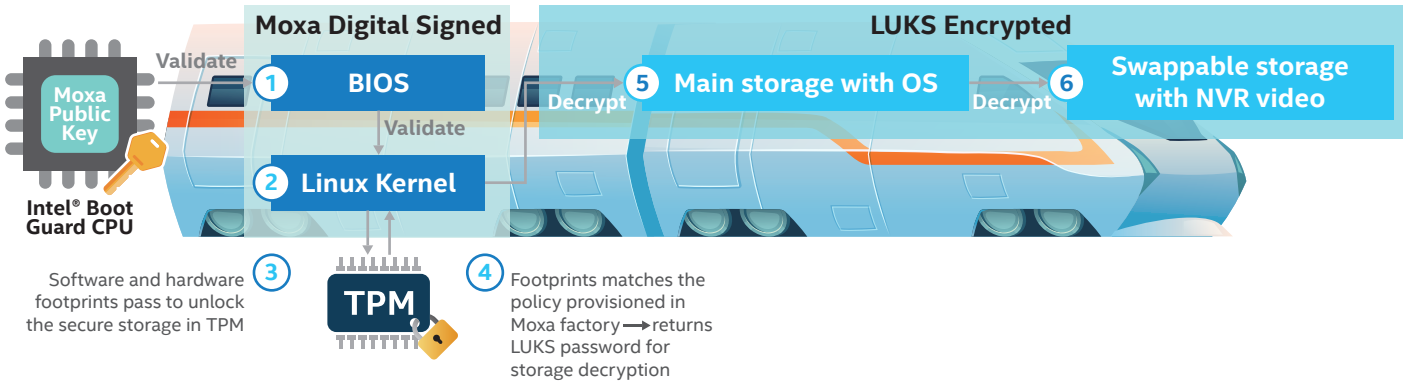

Figure 2: Moxa Chain-of-Trust Validation during Boot Up

Conclusion

OT security carries out security measures through stacks of hardware and software. They are crucial in monitoring, detecting, and controlling the physical systems within the business. As railway networks get busier and malicious attacks continue to increase, it is becoming increasingly important to protect sensitive data and other sensitive assets to guarantee the integrity of IT systems at run-time.

Today, Intel and Moxa are driving the future of the railway industry with smart solutions that allow businesses to help protect their transportation networks and systems against malicious attacks. With Intel Trusted Execution Technology, we provide hardware-based mechanisms that help protect against software-based attacks and protect the confidentiality and integrity of data stored or created on the Moxa V2406C series industrial-grade computer. These capabilities provide the protection mechanisms, rooted in hardware, that are necessary to provide trust in the application's execution environment. In turn, these mechanisms can help protect vital data and processes from being compromised by malicious software running on the platform. For business partners who want to bring the end solution to meet industry security standards like IEC 62443, Moxa V2406C is designed to meet the security objective in alignment with IEC 62443-4-2, the host component requirements.

For more information, contact your Intel sales representative.

Learn More

- To know more about Moxa industrial PC https://www.moxa.com/en/products/industrial-computing/x86-computers/v2406c-series
- Engage your Intel representative and find the resources your organization needs.

References and Resources:

1. Is cybersecurity in rail more important now than ever? https://www.railway-technology.com/analysis/is-cybersecurity-rail-important-now-ever/
2. Rail transit vulnerable to cyberattacks, experts say https://www.cybersecuritydive.com/news/rail-transit-cyberattacks/619123/
3. Cybersecurity in rail: three lessons we learnt from the IRS webinar https://www.railway-technology.com/analysis/cybersecurity-rail-three-lessons-irs-webinar/
4. Intel® Trusted Execution Technology (Intel® TXT) Overview https://www.intel.com/content/www/us/en/support/articles/000025873/technologies.html
5. Use Intel Virtualization Technologies to Help Protect Endpoint Applications and Data without Impacting the User Experience White Paper https://www.intel.com/content/www/us/en/architecture-and-technology/cybersecurity-virtualization-technologies-paper.html
6. Moxa Industrial Linux (MIL) https://www.moxa.com/en/products/industrial-computing/system-software/moxa-industrial-linux

0622/KSW/In2/PDF