WHITE PAPER

# The New Standard for Serial Connectivity: Longevity, Adaptability, and Cybersecurity in Industrial Networks

## - Part III: Cybersecurity -

**Ken Lee**
*Product Manager*

**Simon Chen**
*Product Manager*

MOXA®

## Part III: Cybersecurity

As digital transformation accelerates, the need for secure and reliable industrial communication networks has never been greater. Evolving demands require most industries to upgrade existing systems. Serial connectivity, a cornerstone of industrial automation, continues to be crucial for bridging legacy and modern systems in this transition. Businesses across energy grids, critical infrastructure, transportation, and manufacturing need secure, lasting serial connectivity solutions to bridge traditional and next-generation digital operations.

To meet the challenges of modern industry, the new standard for serial connectivity must embrace three key principles.

Challenges arising in modern industries mandate a new serial connectivity standard based on three key principles.

- **Longevity:** Extending existing serial systems and enhancing their lifespan
- **Adaptability:** Integrating a new design with an updated green policy and improved interoperability
- **Cybersecurity:** Upgrading serial-based systems so that they are ready to be connected to cyber-resilient networks

Released on July 31, 2025



Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 35 years of industry experience, Moxa has connected more than 111 million devices worldwide and has a distribution and service network that reaches customers in more than 91 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

**How to contact Moxa**
Tel: 1-714-528-6777
Fax: 1-714-528-6778

In a series of white papers, we explore the rationale and approaches for building durable, secure serial connectivity solutions that adapt to modern digital infrastructures while preserving backward compatibility. Amidst increased hyperconnectivity, they enable data-driven, value-creating applications like digital twins and industrial edge AI. These technologies optimize industry efficiency and outcomes, shaping the future of industrial communications. This series also highlights the need for a trusted serial partner that adheres to these standards.

Where we explored longevity and adaptability respectively in Part I and Part II in our white paper series, this white paper highlights the growing threat of cyberattacks on industrial edge control systems and underscores the need for robust serial connectivity security. The increasing interconnectedness of industrial control systems (ICS) and operational technology (OT) environments makes cybersecurity a fundamental requirement. Needless to say, organizations must make cybersecurity an integral part of their industrial infrastructure, no matter if they're adding new technology or connecting new devices to old systems. Encryption, authentication, event logging, role-based access control, secure firmware updates, and IT security integration are key security measures that reduce risks. Meeting standards like IEC 62443 ensures operational security and regulatory adherence. In this white paper, we also examine cybersecurity trends and challenges in industrial settings, highlighting the benefits of a secure-by-design approach.

## Cybersecurity Matters in Industrial Edge Connectivity

It's no secret that cyberattacks on critical infrastructure—energy grids, manufacturing plants, and transportation—are becoming more frequent and advanced as industrial settings become more interconnected. In 2023, industrial manufacturing, energy, and transportation were prime targets for cyberattacks, according to IBM's 2024 X-Force Threat Intelligence Index[1]. Censys Research[2] found over 145,000 exposed ICS, with 38% in North America, 35% in Europe, and 22% in Asia. What is of enormous concern is that these threats involve an ever-growing deep knowledge in leveraging industrial protocols and specialty in the critical infrastructure industries. These threats highlight the critical need for strong security systems throughout industrial operations, especially at the edge.

[1] https://www.ibm.com/reports/threat-intelligence
[2] https://censys.com/the-2024-state-of-the-internet-report/

## Cyberthreats at the Edge and the Cost of Inaction

Historically, attackers have focused on higher-level systems like SCADA workstations, which offer more access for exploitation. However, many breaches still stem from IT or network weaknesses, causing security investments to prioritize network infrastructure. But we're seeing a significant increase in attacks targeting ICS at the edge. New ways of exploiting the edge layer involve specialized expertise and a thorough understanding of industrial environments. These breaches can disrupt critical infrastructure operations and compromise sensitive production data, leading to severe consequences. The importance of a holistic defense-in-depth security strategy for ICS, covering edge to core, cannot be overstated.

To mitigate cyberthreats, global regulators are implementing tough new mandates. One example is the upcoming Cybersecurity Framework (CSF) 2.0 by NIST that outlines best practices across risk identification, protection, detection, response, and recovery. Additionally, the EU's NIS2 Directive (2022/2555) extends cybersecurity requirements to industrial entities within critical infrastructure, enforcing supply chain protection. Financial penalties and reputational damage from non-compliance are pushing industrial organizations towards robust cybersecurity strategies.

Despite increasing regulations and escalating cyberthreats, cybersecurity remains a fundamental, system-wide capability. It spans everything from policies and system architecture to the entire life cycle of each system component. Unlike IT networks, edge devices operate under constraints such as limited computational resources and real-time processing demands. As a result, the incremental development of secure industrial edge networks must overcome several unavoidable challenges.

1. **Capability Challenges Across the Industrial Value Chain**

   - **Stakeholder Challenges: Asset Owners and System Integrators**

     Asset owners excel at keeping systems at the edge operational but often lack the skills to assess their security, requiring both deep OT domain expertise and cybersecurity know-how. Similarly, system integrators must navigate differing governance requirements from asset owners, align security measures with the criticality of services, and apply their technical expertise to implement solutions that effectively address key risks.

   - **Vendor Compliance With Industrial Standards**

     To meet system integrators' needs, networking device manufacturers must deliver secure products and services and follow secure development frameworks like IEC 62443. These standards prescribe organizational and technical requirements, covering secure IACS design (IEC 62443-2-4, IEC 62443-3-3) and secure component development life cycles (IEC 62443-4-1, IEC 62443-4-2). Meeting these requirements helps vendors build governance structures and capabilities aligned with systematic security goals.

- **Comprehensive Secure Solutions From Edge to Core**

  Although Ethernet network products like firewalls, routers, and switches have strong security, edge devices lack similarly secure connectivity solutions. The maturity gap between networking and edge connectivity products can create vulnerabilities that compromise otherwise secure environments. Adding to the difficulty, the limited availability of end-to-end security solutions from vendors covering both the network and edge hinders asset owners and system integrators in creating comprehensive security strategies.

2. **Security Asymmetry in the Edge Layer**

- **Perceived Isolation at the Edge Layer**

  Despite the perception of edge zones as isolated and protected by robust infrastructure like switches and routers, they're still susceptible to attacks that exploit employees through social engineering. Phishing attacks bypass human defenses more easily than technological ones, letting attackers into supposedly secure areas. This discrepancy shows that isolation isn't enough for strong security, so we need a completely new approach, including better employee training.

- **Critical Data Protection Against Infiltration**

  Once inside the edge layer, attackers often face weaker security, increasing the chances of undetected activity. Therefore, attackers can secretly steal sensitive data from production systems over long periods, resulting in the loss of intellectual property or a competitive disadvantage. In more acute scenarios, they can sabotage operations by causing system malfunctions or outright production stoppages, thereby threatening both safety and productivity. This dual threat—stealthy data breaches and immediate operational disruptions—reinforces the need for stronger, proactive defenses within edge environments.

- **Visibility of Incidents and Responses**

  Keeping thorough incident logs helps auditing, ensures compliance, and provides key insights for better responses. Reducing the window of opportunity for attackers helps organizations prevent complex, multi-actor attacks across their networks.

Addressing these challenges requires device manufacturers, software providers, system integrators, and end users to collaborate and effectively implement security measures at every level.

## From Core to Edge: Defense-in-depth Strategy

Overcoming these challenges requires organizations implementing a multi-layered security strategy throughout their industrial operations. This includes qualifying value-chain partners and vendors, introducing future-ready secure products at the edge layer, and ensuring deeper integration with enterprise systems to maintain layered security. Here are key strategies for achieving a secure industrial future:

- **Compliance and Secure Product Development**

  To ensure secure systems and components, organizations providing security products or services in the value chain must meet industrial standards like IEC 62443-2-4 and IEC 62443-4-1. These certifications guarantee internal teams receive the necessary training and that a structured security design process, ongoing maintenance, and post-purchase support are in place. In addition, supportive structures like a Product Security Incident Response Team (PSIRT) enable coordinated incident responses and consolidate security needs. This approach improves internal alignment and ensures consistent communication throughout the value chain.

- **Secure Portfolio Offering: From Network to Edge Connectivity Products**

  A comprehensive portfolio—from core networking components to edge connectivity devices—should comply to IEC 62443-4-2 standards, simplifying vendor qualification processes, system and component requirement assessments, and after-sales maintenance. However, many vendors specialize only in networking-centric or computing platform–centric security solutions, often providing limited or no secure edge connectivity offerings.

  Edge connectivity products, including serial-to-Ethernet device servers, protocol gateways, and remote I/O, require security features compliant with IEC 62443-4-2 across various security levels (SL) to meet application and system needs. Following ISA Security Compliance Institute (ISCI) recommendations, ICS components should meet at least SL2 of IEC 62443-4-2, given current threats, needed resilience, and IT integration.

  Given the long life cycles of edge connectivity products, vendors must adopt secure-by-design principles and integrate security features that meet required protection levels.

- **Secure Edge Connectivity: Edge Product Design Principles**

  Beyond compliance and portfolio breadth, three critical facets define secure edge connectivity products:

  1. **Secure by Design**

     Extending the concept of Longevity from Part I, cybersecurity must also be integrated throughout the entire product life cycle. A Secure Development Lifecycle (SDL) compliant with IEC 62443-4-1 is not just a requirement for the initial design; it is a guarantee for achieving long-term, stable operation. And because new vulnerabilities emerge daily, a continuous process for vulnerability assessment and patching is just as critical as a flexible hardware architecture. This commitment to long-term vigilance is a hallmark of a trustworthy vendor—ideally one recognized as a CVE Numbering Authority (CNA)—and is how the 'secure and effective' lifespan of a device is truly extended.

  2. **Secure Communications**

     Edge connectivity devices enhance data integrity and confidentiality by acting as a secure gateway between legacy systems and modern networked applications. Acting as gatekeepers, secure edge connectivity devices initially connect field-edge equipment to Ethernet networks, translating legacy data into networked applications. To maintain data integrity and confidentiality for fieldbus data and management interfaces, they need to authenticate and encrypt data streams (e.g., serial-to-Ethernet) with cutting-edge cryptography.

  3. **Secure Management and Enterprise Integration**

     Secure management aims to build trust between edge devices and the central management system. This includes mechanisms for device self-validation—ensuring only authenticated, signed firmware is executed—and robust device-to-system authentication management to establish trust across the enterprise. The device must assign and limit permissions to only what’s needed per user or process, log all user and unauthorized actions with timestamps, and use allowlists or denylists for incoming communications to stop unauthorized network access. Furthermore, to ensure real-time tracking and audit preparedness, devices must record system events using standardized, time-stamped formats.

     Many asset owners already use centralized enterprise management, such as Security Operations Centers (SOCs), Network Operations Centers (NOCs), Security Information and Event Management (SIEM) systems, and IT authentication servers. Therefore, seamless integration between edge devices and these systems is critical. Centralized authentication and policy enforcement extend to the edge through this integration, thus optimizing incident management by enabling timely responses to potential threats.

Consider the improvements needed in a next-generation secure serial-to-Ethernet device server.

- **Hardware-level root of trust:** The hardware platform needs to protect and check the authenticity of the software before execution.
- **Developed following a secure-by-design process:** It is necessary to integrate the security assessment and functional requirement into the product development process.
- **Role-based user management:** Supporting role-based access control (RBAC) gives users only the access they need, creating a zero-trust system.
- **Authenticated and encrypted serial-to-Ethernet data stream:** Supporting advanced encryption methods and authentication of devices during setup. This ensures that data remains confidential and is only accessible to allow users, preventing unauthorized access or data sniffing.
- **System incident logging:** Categorizing system logs, following the RFC3164 industrial standard, with ISO8601 timestamp to record edge connectivity events, including severity and details, for cybersecurity incident analysis and audits.
- **Enterprise server integration:** Supporting dual remote syslog with failover via NoCs, along with remote authentication through RADIUS servers, enhances overall security resilience.

## Securing a Resilient Future in Industrial Edge Connectivity

As industrial networks continue to expand and converge, safeguarding the entire ecosystem from core infrastructure to edge-layer connectivity remains a critical priority. Complying with evolving government cybersecurity regulations is just as important. Success on both fronts requires asset owners and system integrators expanding their cybersecurity capabilities beyond core competencies and forming partnerships with component vendors certified for industrial standards, including IEC 62443-4-1. It's also crucial to have a complete, secure product lineup built using secure development, strict life-cycle management, and design principles meeting enterprise security needs.

Next-generation edge connectivity solutions are needed for complex edge environments. These solutions must include hardened hardware, high-performance capabilities, secure data streams, robust logging, and ongoing service support. Organizations can mitigate both opportunistic and sophisticated attacks by encouraging collaboration between asset owners, system integrators, and vendors to implement a layered security approach. They ensure efficient and resilient operations while safeguarding the confidentiality, integrity, and availability of critical production data—ultimately preparing for the cybersecurity challenges of modern industrial environments.

Moxa, a certified IEC 62443-4-1 company and trusted industrial edge connectivity partner, will continue investing in its next-generation protocol gateways (MGate) and serial-to Ethernet servers (NPort) portfolios, with plans for flagship IEC 62443-4-2 secure level 2 certification. Moxa's commitment secures its position as a dependable ally in the decades ahead, ensuring the safety of today's edge-layer serial equipment during transition to tomorrow's secure networks.

To find out why Moxa is your trusted long-term serial partner and learn about their next-generation products, visit Moxa's Trusted Serial Partner site.