Mercury

WHITE PAPER

Meeting the Challenges of Cybersecurity in Access Control: A Future-Ready Approach

The Cybersecurity Imperative in PACS

Physical access control systems (PACS) have evolved from isolated, hardware-centric deployments to connected systems integrated into enterprise IT networks. This evolution enables real-time management, mobile credentialing and cloud scalability. These capabilities support operational efficiency and policy alignment across complex environments. However, connected systems introduce new cybersecurity requirements that legacy PACS were never designed to address.

Achieving long-term resilience requires systems that integrate encryption, authentication and integrity into their core architecture. These capabilities cannot be appended; they must shape design, deployment and lifecycle strategy. This paper outlines how each function contributes to a secure access control environment and how organizations can align with Zero Trust principles, meet compliance demands and improve threat visibility.

Encryption: Protecting Communication and Stored Data

In modern PACS, every interaction between the reader and controller, as well as between the controller and host, presents a potential attack surface. Securing these interactions requires strong encryption of data in transit and at rest.

System architectures must utilize established cryptographic protocols, such as TLS 1.3, to protect controller-host communication. Credential data and command sets must remain encrypted throughout transport, with each component authenticating its peer. Within the controller itself, partition encryption ensures that configuration data and access logs are protected from tampering or exfiltration.

Bus-level encryption on IO modules and secure reader channels (e.g., using protocols like OSDP Secure Channel) prevents eavesdropping and command injection at the edge. Taken together, these practices form the baseline for securing sensitive data throughout its lifecycle.

Authentication: Trust in Devices and Identity

Credential verification alone is no longer sufficient for high-assurance access control. Secure systems must also authenticate the devices that process, relay and act on that credential. This involves establishing trust among the host system, the controller and the edge components.

Effective authentication strategies employ mutual validation protocols that verify both the user's identity and the legitimacy of the requesting device. Secure boot mechanisms verify that only signed and authorized firmware executes on the hardware. Runtime protections, such as hardware-enforced isolation of sensitive processes, further reduce the risk of compromise.

Support for advanced credentials, including those that use cryptographic certificates, mobile devices or biometric input, adds a second layer of defense. These credentials are difficult to spoof, and when paired with device-level validation, they provide strong assurance of intent and identity.

System Integrity: Lifecycle Security

System integrity involves maintaining trusted behavior from deployment through the full operational lifecycle. This begins with secure initialization, where each controller validates firmware before execution. Boot-time checks detect and reject unauthorized changes, preserving the system's known-good state.

Ongoing system health depends on timely updates and continuous code scrutiny. Secure firmware distribution models, supported by structured testing such as static and dynamic analysis, protect against vulnerabilities introduced through third-party libraries or rapid iteration. Tools such as software bill of materials (SBOM) and common vulnerabilities and exposures (CVE) monitoring are crucial for maintaining visibility and enabling rapid responses.

Operational integrity also relies on reliable execution under stress. Edge-based enforcement allows access policies to persist even during network disruption, ensuring that system trust is not dependent on real-time connectivity.

Zero Trust: A Security Model Without Assumptions

Zero Trust security models eliminate implicit trust within network boundaries. Applying these principles to PACS requires that all devices and credentials be continuously authenticated and authorized, regardless of their network origin or role.

Zero Trust-aligned systems validate every access transaction against real-time policy and device status. No credential or device is assumed valid based on location, past behavior or system proximity. This demands encrypted ommunication paths, identity-aware access controls and detailed audit trails.

Enforcement at the edge enables localized decisions that reflect current policy and contextual risk, reducing the attack surface and minimizing reliance on centralized control points. This distributed approach enhances system resilience while upholding strict trust standards.

Compliance: Meeting Technical and Regulatory Standards

Organizations face increasing pressure to meet formal security requirements related to data privacy, access logging and system auditability. Whether driven by frameworks such as FIPS, HIPAA or GDPR, compliance demands are reshaping the design of PACS.

Compliant systems include built-in encryption, secure credential management and tamper-evident logs. These systems must also support access role segmentation, audit record export and secure administrative functions.

Code quality, transparency and continuous improvement play a central role. Security-focused development practices, such as secure software development lifecycles (SSDL), vulnerability analysis and third-party testing, demonstrate organizational readiness and help reduce downstream risk.

Detection and Response: Visibility Into Access Behavior

Cybersecurity strategy requires both prevention and detection. In access control, this means being able to observe, log and analyze access attempts, system changes and anomalous behavior.

Modern PACS include capabilities for real-time alerting, anomaly detection and configuration monitoring. Events such as repeated failed access attempts, out-of-schedule badge use or unauthorized firmware updates should trigger a review and, where appropriate, an automated response.

Integration with broader enterprise security tools enhances value. When PACS telemetry feeds into security information and event management (SIEM) systems, physical access patterns can be correlated with digital threat indicators. This unified visibility supports faster incident response and more informed risk decisions.

A Strategic Framework for Secure PACS

The capabilities that define modern PACS — real-time access, mobile integration and open architecture — are only viable when built on a foundation of security. Encryption, device and identity authentication and system integrity are not optional features; they are structural elements required for long-term system trust.

As threat models evolve and compliance expectations increase, organizations must adopt architectural strategies that support secure, scalable and policy-driven access control. Systems that enforce security at the edge, validate behavior throughout their lifecycle and align with Zero Trust principles offer the best path forward.

Mercury MP Intelligent Controllers meet these demands by integrating secure boot and digitally signed firmware to ensure startup integrity, TLS 1.3 and encrypted bus protocols to protect communications and ARM TrustZone for runtime isolation of critical functions.

They support authenticated device communication via OSDP Secure Channel and enable real-time policy enforcement at the edge, ensuring access continuity even during network disruptions. Built on a unified OS platform with continuous CVE monitoring and a published software bill of materials, they offer lifecycle security and transparency aligned with modern compliance and threat management requirements.

For organizations seeking a reliable, standards-based foundation for secure physical access, Mercury MP Controllers offer the architectural depth, integration flexibility and cybersecurity rigor necessary to support evolving enterprise environments.

To learn how Mercury MP Controllers align with your security strategy and infrastructure plans, visit mercury-security.com.

Mercury Security
11165 Knott Avenue, Suite AB
Cypress, CA 90630
mercury-security.com

part of HID