Mercury

Migration Decision Tree

Plan Your PACS Modernization Strategy With Confidence

Physical access control systems (PACS) manage who can enter specific doors, elevators and areas within a facility. As technology evolves and systems age, organizations must assess whether their current solutions meet the increasingly complex requirements for security, integration and operational efficiency. This decision tree helps you determine the next step, whether it involves a firmware update, a phased upgrade or a complete system replacement. A modernized system will support the integrations and workflows necessary to adapt and scale to future security needs.

Start Here

Is your access control infrastructure ready for modern security demands?

This includes support for:

- Secure and encrypted network (TCP/IP) communication
- Secure and encrypted device communication
- Measures to secure data at rest and in transit
- Capable of integration with cloud-based applications and tools
- AI capabilities

YES

Is your system aligned with today's security best practices?

Factors to consider:

- Use of strong encryption (e.g., AES-128, AES-256, follows FIPS 140-3 guidelines)
- Secure communication standards (e.g., OSDP Secure Channel, HTTPS, TLS1.3)
- Firmware updateability and vendor support
- Integration with identity management, video, intrusion or building systems

YES

Recommended Path:
Software and Firmware Updates

- Apply the latest firmware
- Review configurations
- Use embedded app support
- Plan future feature expansions

NO

Is replacing legacy hardware feasible without significant disruption or cost?

Factors to consider:

- Downtime risk
- Access control continuity
- Facility restrictions or regulatory constraints

YES

Recommended Path:
Phased Migration

- Upgrade key security components
- Replace outdated endpoints
- Maintain compatible elements
- Enable edge-based intelligence
- Add third-party apps for monitoring, analytics, intrusion and authentication
- Use open SDKs to extend functionality

NO

Recommended Path:
Stabilize and Plan

- Harden the existing environment with updated firmware if possible
- Monitor risk and performance
- Develop a staged transition plan aligned with budget cycles using modern, open-platform hardware to reduce future risk

NO

Is replacing legacy hardware feasible without significant disruption or cost?

Factors to consider:

- Downtime risk
- Access control continuity
- Facility restrictions or regulatory constraints

YES

Recommended Path:
Full-System Upgrade

- Replace outdated architecture
- Adopt controllers designed for intelligent edge applications
- Consider a system that supports open architecture to protect your investment
- Consider app extensibility, cloud readiness and unified security

NO

Recommended Path:
Stabilize and Plan

- Harden the existing environment with updated firmware if possible
- Monitor risk and performance
- Develop a staged transition plan aligned with budget cycles using modern, open-platform hardware to reduce future risk

Modernizing a PACS system presents technical and operational challenges, including compatibility, integration, security and cost. Mercury's open-architecture and migration tools help reduce that complexity. Contact us to evaluate your current system and map out a clear, efficient upgrade path.

TALK TO AN EXPERT