Access Control Whitepaper



Protect your access control systems from cyber threats

The power of preventative maintenance

dormakaba



Executive Summary

Access maintenance has become a critical part of cybersecurity

As access control shifts from mechanical infrastructure to connected digital and cloud-based systems, the risks facing organizations have fundamentally changed. Cyberattacks now routinely target devices that were never designed with modern threat landscapes in mind, especially when firmware is outdated or hardware has drifted past its supported lifecycle.

Traditional reactive maintenance cannot keep pace with these developments. In a cyber-physical world, waiting for faults to appear simply leaves too much to chance. A preventive, intelligence-led maintenance model closes vulnerabilities earlier, enhances operational stability and provides the documentation required for compliance.

This whitepaper explores how modern maintenance strategies protect systems against emerging cyber risks, extend the life of existing infrastructure and prepare organizations for the next generation of access control technologies.

The new risk landscape

Access control is a front line in the defence against cyber threats

Modern facilities run on an interconnected network of IT systems, operational technology and smart devices. Access control is at the heart of that network, making it increasingly attractive to attackers looking for pathways with lower visibility and weaker update governance.

Older devices, legacy encryption schemes and unsupported firmware can create structural weaknesses that extend far beyond a single door. A compromised controller or improperly maintained reader may expose sensitive personal data, interrupt operations or provide a route into the wider network.

Regulation has responded accordingly. GDPR's expectations for "appropriate technical measures" apply directly to access systems handling credential data, while ISO 27001 and NIS2 emphasize active vulnerability management. Compliance is no longer about configuration alone; it demands continuous, evidence-based maintenance.

30%

year-on-year increase in cyberattacks targeting network connected physical security systems in the past year

Source:
https://ciosea.economictimes.indiatimes.com/news/security/critical-infrastructure-cyberattacks-increase-30-percent-in-one-year-report/112854335



Maintenance as a security strategy

Closing vulnerabilities starts with continuous oversight

Most security incidents involving access control are preventable. They do not hinge on sophisticated exploits but on gaps that accumulate when updates are missed, firmware ages or configurations are left unchanged for too long.

Smart maintenance reframes the role of upkeep from task-based servicing to an ongoing security discipline. Regular updates ensure that known vulnerabilities are resolved as soon as fixes become available. Configuration and encryption reviews maintain a consistent security baseline. Lifecycle tracking prevents silent obsolescence and health checks provide a clear understanding of emerging risks before they escalate.

dormakaba's approach brings these elements together into a structured framework. Our Security & Health Check offers a complete assessment of access infrastructure, from firmware maturity and encryption strength to compatibility, integrations and event logging. Coordinated patch management and lifecycle tracking ensure no component drifts outside a secure state. Targeted support helps reduce vulnerability windows during incidents.

60%

of IoT breaches can be traced to unpatched firmware

Source:
https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025





Staying compliant and avoiding penalties

Compliance requires proof of security, not assumptions

Access control systems routinely process personal data, from credentials and access logs to biometric identifiers. As such, they fall squarely within GDPR's definitions of sensitive digital infrastructure. Regulators increasingly expect organizations to demonstrate that systems are up to date, securely configured and actively monitored.

Failure to maintain equipment, whether through outdated encryption, unsupported firmware, missing audit trails or undocumented update cycles, can create significant compliance exposure. Maintenance agreements help address these gaps by providing clear, traceable records of updates, interventions and system health. This creates the evidential foundation required for GDPR, ISO 27001 and NIS2 alignment.

For organizations with distributed estates or critical operations, having this documentation readily available is not simply a convenience. It is a safeguard against reputational and financial risk.



The ROI of maintenance

The securest systems pay for themselves

Preventive maintenance has measurable financial impact. Predictable updates reduce the likelihood of emergency interventions and unplanned downtime. Systems last longer when firmware, drives and controllers remain within their supported lifecycle and staff productivity improves when access works reliably without bottlenecks or manual overrides.

Well maintained systems also offer smoother modernization pathways, reducing the cost and complexity of future upgrades.

Proactive maintenance can extend access control hardware lifespan by 20-40%

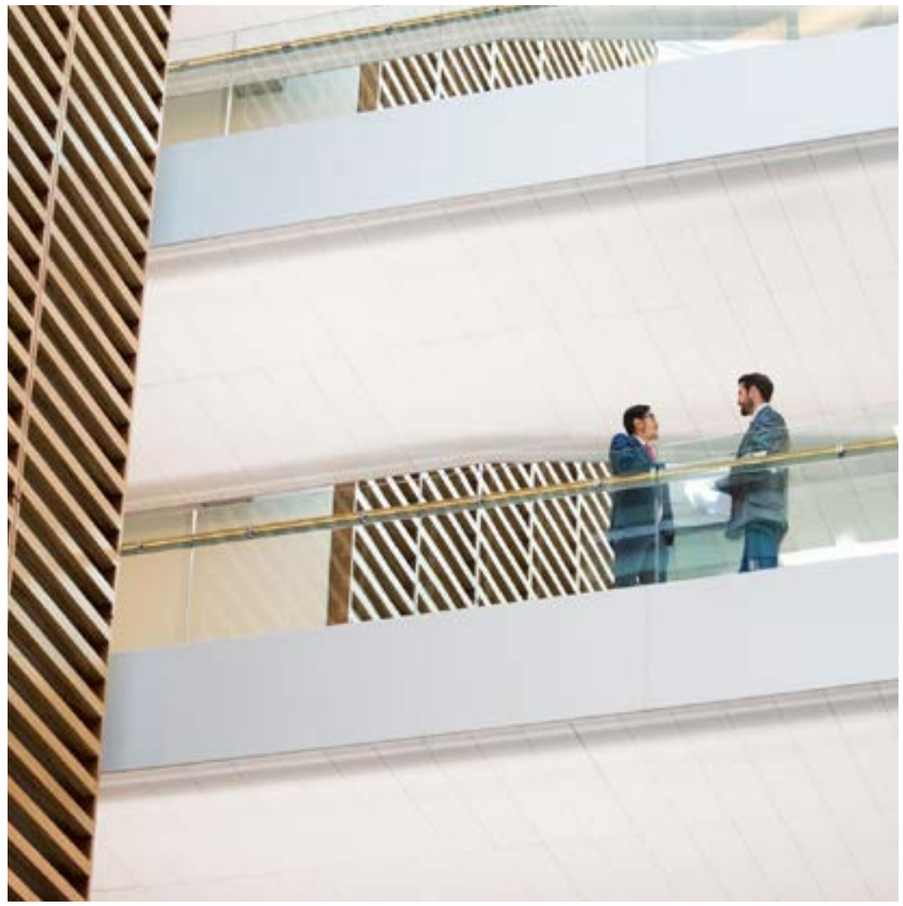
Source:
https://www.goworkwize.com/blog/it-preventive-maintenance-guide

Future-proofing access control

Maintenance is the foundation for next generation technology

Access control is transitioning towards cloud-based management, mobile credentials, biometric verification and AI-driven monitoring. These advances depend on systems being secure, compatible and updated to modern standards. When firmware or encryption falls behind, these integrations become difficult and, in some cases, unsafe.

Regular maintenance ensures organizations can adopt new technologies without exposing themselves to unnecessary risk. It keeps infrastructure aligned with emerging standards, reduces the cost of system upgrades, and ensures that when new capabilities are introduced, they are built on a stable, secure base.





The dormakaba advantage

A global partner for secure, compliant and future-ready access control

dormakaba combines deep expertise in cyber-physical security with a global network of service professionals. Our structured maintenance programmes provide system visibility, compliance support and lifecycle intelligence, helping organizations reduce risk while maximising the value of their infrastructure.

Equally important is our commitment to transparency and responsible vulnerability disclosure. Working closely with researchers, partners and customers, we continuously identify, validate and resolve security findings in a coordinated and safe manner. This ensures that improvements reach users promptly and consistently, reinforcing trust across the lifecycle.

Strengthen your security

Strengthen your security. Protect your business. Prepare for what's next.

Get a clear picture of your current risk exposure, your compliance position and the opportunities to future-proof your access control infrastructure – schedule a dormakaba Security & Health Check today.

Our Sustainability Commitment

We are committed to fostering a sustainable development along our entire value chain in line with our economic, environmental and social responsibilities toward current and future generations. Sustainability at product level is an important, future-oriented approach in the field of construction In order to give quantified disclosures of a product's environmental impact through its entire life cycle, dormakaba provides Environmental Product Declarations (EPD), based on holistic life cycle assessments.

www.dormakaba.com/sustainability

Our offering

Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and Repair



WN 5626051532, EN, 01/2026
Subject to change without notice

dormakaba
International Holding AG
Hofwisenstrasse 24, 8153
Rümlang, Switzerland
+41 44 818 90 11
info@dormakaba.com
dormakaba.com

dormakaba.com