



WHITEPAPER 16

Cybersecurity for Connected Panel PCs

Secure Boot, TPM, OS Hardening and Lifecycle Maintenance

A practical defence-in-depth architecture for industrial HMI endpoints



An engineering framework for trust anchors, device identity, signed software, patching, network segmentation, monitoring, recovery and secure decommissioning.



Created by Crystal Display Systems Limited

Technical whitepaper | August 2026

Executive summary

Industrial HMIs increasingly connect production equipment to plant, enterprise and cloud systems. This improves visibility and service but exposes long-lived endpoints to vulnerabilities, credential theft, unauthorised software and remote disruption.

A practical architecture starts with a hardware root and controlled software image, then layers hardening, identity, segmentation, patching, monitoring and recovery. Security controls must respect offline and production-continuity requirements.

Core recommendation

Use a hardware-backed trust chain, signed recoverable updates and segmented least-privilege networking. Fund OS/BSP and vulnerability maintenance for as long as the panel PC remains deployed.

How to use this whitepaper

- Use the requirement table to convert connected-HMI cybersecurity expectations into measurable pass/fail criteria.
- Use the comparison matrix to shortlist architectures without allowing one headline specification to dominate.
- Apply the weighted scorecard using the actual operating environment, duty cycle and commercial lifecycle.
- Validate the preferred approach in the final mechanical, optical, electrical and software implementation.

Contents

1	Define assets, connectivity and support life before selecting controls
2	Security architectures for connected panel PCs
3	Comparative decision matrix
4	Engineering trade-offs that change the answer
5	Application-led recommendations
6	Qualification and sourcing checklist
7	Beyond endpoint hardening
8	Working with Crystal Display Systems

Key decision principles

- Build a hardware-backed chain of trust and signed update path before connecting the HMI to operational networks.
- Minimise services, accounts and interfaces; every enabled function becomes a maintenance obligation.
- Design patching and recovery around production availability rather than assuming office-IT update behaviour.
- Segment the panel PC from higher-risk networks and use authenticated, least-privilege remote support.
- Maintain an SBOM, vulnerability triage and defined end-of-support route for the full deployed life.

1. Define assets, connectivity and support life before selecting controls

A useful cybersecurity requirement states protected assets, consequence, interfaces, users, physical access, network zones, update constraints, recovery time, software support horizon and responsible organisations. These inputs determine the required assurance profile.

Requirement domain	Questions to resolve
Assets and consequence	Machine control, credentials, recipes, safety information, personal data, intellectual property, availability and recovery-time objectives.
Threat surface	Ethernet/Wi-Fi/cellular, USB, serial/fieldbus, browser, remote support, cloud agents, removable storage, physical access and supply chain.
Trust foundation	Secure/measured boot, TPM or hardware root, keys, firmware protection, device identity and manufacturing provisioning.
Software lifecycle	Supported OS, SBOM, application dependencies, patch cadence, signed update, rollback, vulnerability response and end-of-support.
Network architecture	Zones/conduits, firewall allowlists, service ports, certificates, remote access, logging, time synchronisation and segmentation.
Recovery and disposal	Golden image, offline recovery, backup, incident response, credential rotation, data erasure and secure decommissioning.

A practical weighting model

Assign each criterion a weight from 1 (low importance) to 5 (critical). Score each candidate from 1 (poor fit) to 5 (strong fit), then multiply score by weight. The arithmetic does not replace engineering judgement, but it exposes where the security architecture and maintenance model depends on assumptions, incomplete test evidence or optimistic supplier data.

Do not average away a fatal constraint

A candidate that fails a non-negotiable requirement for connected-HMI cybersecurity should be removed before weighted scoring. Typical fatal constraints include unsafe operation, an unachievable environmental limit, incompatible interfaces, unacceptable field reliability or no credible supply route.

Recommended process

- Set pass/fail gates for the mandatory connected-HMI cybersecurity requirements before comparing desirable features.
- Agree criterion weights with electronics, mechanical, software, product, service and procurement stakeholders.
- Score only from controlled data, supplier evidence or representative testing; mark unknowns explicitly.
- Run sensitivity checks by changing the highest weights and identifying whether the preferred architecture changes.
- Document assumptions, test conditions and revision status so the decision can be revisited after a component or firmware change.

2. Security architectures for connected panel PCs

2.1 Basic hardened endpoint

A basic industrial hardening profile removes unused services, applies secure configuration, limits accounts, enables host firewalling and protects local storage. It materially reduces commodity exposure but depends on firmware integrity and disciplined maintenance.

- Strengths: low hardware impact, broad platform compatibility and immediate reduction of attack surface.
- Limitations: limited protection against boot-chain compromise, credential theft or physical storage extraction.
- Best fit: isolated or low-consequence HMI with controlled physical and network access.

2.2 Hardware-rooted secure boot and device identity

UEFI secure boot, verified boot or an SoC root of trust validates firmware and OS components before execution. A TPM or secure element can protect keys, bind identity to hardware and support measured attestation. Key provisioning and recovery are as important as the device feature.

- Strengths: stronger integrity, protected identity and resistance to unauthorised software or cloned devices.
- Limitations: key-management complexity, firmware/vendor dependencies and risk of unserviceable units if recovery is poorly designed.
- Best fit: connected industrial equipment, regulated deployments and devices exposed to physical access.

Key lifecycle control

Document who creates, injects, backs up, rotates and revokes signing and device keys. Secure boot without an owned key and recovery process can lock the supplier and customer into an opaque trust chain.

2.3 Managed industrial endpoint

A managed profile adds signed remote updates, fleet inventory, certificate rotation, central logging, health monitoring and controlled remote support. It provides lifecycle visibility but introduces management infrastructure and network dependency.

- Strengths: scalable patching, asset awareness, faster incident response and consistent policy.
- Limitations: backend security, connectivity, operational coordination and privacy/data-governance burden.
- Best fit: fleets of connected panel PCs with central engineering or IT/OT operations.

2.4 High-assurance or safety-related architecture

Higher-consequence systems may add immutable boot stages, disk encryption, application allowlisting, dual-image recovery, independent watchdogs, signed configuration and strict network gateways. Assurance depends on evidence and operational process, not feature count.

2.5 Thin client or isolated display head

Moving application logic to a protected server can reduce local data and software, while an isolated HMI can minimise network exposure. Availability, network latency, server trust and local fallback must be addressed.

3. Comparative decision matrix

Criterion	Basic hardening	Hardware-rooted	Managed fleet	High assurance / thin client
Boot integrity	Limited	Excellent	Excellent	Excellent
Key protection	Limited	Excellent	Excellent	Excellent
Patch scalability	Limited	Moderate	Excellent	Strong
Offline resilience	Strong	Excellent	Strong	Excellent
Incident visibility	Limited	Moderate	Excellent	Strong
Physical attack resistance	Limited	Strong	Strong	Excellent
Operational simplicity	Excellent	Moderate	Limited	Limited
Recovery robustness	Moderate	Strong	Excellent	Excellent
Lifecycle evidence	Limited	Strong	Excellent	Excellent
Relative programme cost	Excellent	Moderate	Limited	Poor

Indicative only. Actual performance depends on the complete system architecture, supplier implementation, environmental conditions and validation method.

Example weighted scorecard

Criterion	Weight	Basic hardening	Hardware-rooted	Managed fleet
Connected to plant network	5	3	5	5
Ten-year patch obligation	5	2	4	5
Physical service access	4	2	5	5
Fleet size 1,000 units	5	2	3	5
Offline production continuity	5	4	5	4
Engineering simplicity	3	5	3	2
Incident response	4	2	3	5
Weighted total		86	126	141

For this 1,000-unit connected fleet, managed hardware-rooted endpoints lead because patching, inventory and response carry high weight. Hardware-rooted standalone units remain strong where connectivity is intermittent; basic hardening lacks lifecycle visibility and trusted identity.

Reading the result

- Basic hardening is a minimum baseline, not a complete architecture for long-lived connected fleets.
- Hardware roots add value only when keys, firmware updates and recovery are owned and tested.
- Fleet management should preserve offline operation and avoid turning the management backend into a single production dependency.

| 4. Engineering trade-offs that change the answer

4.1 Secure boot does not secure a vulnerable application

Boot integrity prevents unauthorised images but does not remove exploitable services, weak authentication or unsafe application logic. Defence in depth remains necessary.

4.2 Patching is an availability-control problem

Updates can interrupt production or break drivers. Use staged deployment, maintenance windows, compatibility testing, signed packages, rollback and an emergency path.

4.3 Legacy protocols create flat trust zones

Unauthenticated fieldbus or remote desktop services may be required. Isolate them behind allowlisted gateways and minimise routing rather than exposing them broadly.

4.4 Physical access changes the threat model

USB ports, removable storage, debug headers and service passwords can bypass network controls. Disable, lock, authenticate or monitor based on service needs.

4.5 Time, certificates and identity must survive outages

Certificate validation and logs depend on trustworthy time. Define RTC, time sync, expiry handling and recovery for disconnected equipment.

4.6 End-of-support is a security event

When OS, BSP or firmware updates stop, risk changes even if the hardware still functions. Plan upgrade, isolation or retirement before support expiry.

| 5. Application-led recommendations

Standalone machine HMI

Apply secure configuration, host firewall, least privilege, signed image and controlled USB/service access. Segment from corporate networks.

Fleet of connected panel PCs

Use hardware identity, signed staged updates, inventory, central logging and certificate rotation with offline operational fallback.

Remote service terminal

Use authenticated VPN/jump-host access, time-limited credentials, audit logging and local approval rather than open inbound ports.

Regulated or high-consequence system

Add documented threat modelling, hardware root, encrypted storage, allowlisting, dual-image recovery and formal vulnerability response.

Legacy application platform

Compensate for unsupported software with network isolation, application allowlisting, restricted media and a funded migration plan.

6. Qualification and sourcing checklist

	Area	Verification action
☐	Threat model	Document assets, actors, access paths, consequences, assumptions and trust boundaries.
☐	Boot / firmware	Verify signed boot chain, firmware write protection, TPM/root functions and recovery image.
☐	Identity / keys	Test provisioning, certificate use, rotation, revocation, backup and device replacement.
☐	OS / application	Audit services, accounts, permissions, firewall, encryption, SBOM and dependency versions.
☐	Updates	Demonstrate signed staged update, interrupted update, rollback, offline update and compatibility testing.
☐	Network	Verify segmentation, allowlists, remote support, logging, time sync and behaviour with unavailable services.
☐	Resilience	Test power loss, watchdog, storage corruption, backup restore and factory recovery.
☐	Lifecycle	Define vulnerability intake, severity decisions, patch SLAs, customer communication and end-of-support.

Questions to ask a display partner

- Who owns the secure-boot keys, device certificates and recovery credentials?
- What OS/BSP/application components are in the SBOM and how are vulnerabilities monitored?
- How are updates signed, staged, rolled back and applied to intermittently connected units?

- Which network services and physical interfaces are enabled, and why are they necessary?
- How does the HMI continue safely if identity, time, management or update services are unavailable?
- What is the support horizon and migration/isolation plan when patches end?

Minimum evidence pack for design approval

- Approved threat model and security requirements mapped to architecture controls.
- Hardware/firmware trust-chain and key-provisioning documentation.
- Controlled OS/application image, SBOM, hardening baseline and account/service inventory.
- Signed update, rollback, recovery and power-failure test evidence.
- Network segmentation, remote-access and logging configuration with penetration/robustness results.
- Vulnerability-response, patching, incident, end-of-support and secure-disposal procedures.

7. Beyond endpoint hardening

Industrial HMI security is moving toward verifiable device identity, continuous posture and hardware-enforced isolation. These capabilities must be integrated with operational safety and maintainability.

Remote attestation

Measured boot values can prove device state to a verifier. Privacy, baseline management and action on failed attestation need definition.

Memory-safe and sandboxed applications

Modern languages and isolation can reduce exploit classes, but legacy libraries, drivers and operational validation remain.

Confidential computing

Hardware isolation can protect selected workloads or keys, although platform support, performance and recovery complexity must be assessed.

Zero-trust remote maintenance

Per-session identity, device posture and least privilege can replace broad VPN access. Plant availability and break-glass procedures remain essential.

Security telemetry at the edge

Local anomaly detection can identify unexpected services or traffic, but false alarms, resource use and response authority must be controlled.

Adoption gate

A new security control should enter production only when its trust assumptions, keys, update path, offline behaviour, recovery and operational ownership are documented and tested.

8. Working with Crystal Display Systems

Crystal Display Systems Limited supplies and customises industrial panel PCs and embedded platforms with secure-boot, TPM, OS, networking, storage and lifecycle options that can be configured within a customer security architecture.

Relevant CDS resources

Resource	Purpose
Industrial Panel PC Solutions	Integrated industrial HMI and panel PC solutions with customisation options.
Industrial Panel PC Range	Current panel PC platforms, processors, I/O and rugged configurations.
Industrial Boxed PCs and Panel PCs	Industrial computing platforms, customisation and long-life support.
Industrial Automation Displays	Display, monitor and computing solutions for automation and machine HMI.
CDS Knowledge Centre	Display guides and technical training documents.
Request a Quote	Submit project requirements for technical and commercial review.
Contact CDS	Contact details and enquiry routes.

Contact Crystal Display Systems Limited

Crystal Display Systems Limited

Address: Unit 6 M2M Park, Fort Bridgewood, Maidstone Road, Rochester, Kent, ME1 3DQ, United Kingdom

Telephone: +44 (0)1634 791 600

Email: info@crystal-display.com

www.crystal-display.com

Conclusion

Connected panel PC security is a lifecycle system, not a one-time hardening checklist. Hardware trust, minimal services, identity, segmentation, signed updates, monitoring and recovery must operate together without compromising production availability. The defensible design includes funded software maintenance and a controlled end-of-support path.

Final engineering rules

- Establish assets, threats and trust boundaries before selecting security features.
- Use hardware-backed boot and identity with owned key and recovery processes.
- Minimise and segment interfaces, accounts and network services.
- Test signed updates, rollback, offline operation and disaster recovery.
- Maintain SBOM, vulnerability response and end-of-support planning for the deployed life.

Disclaimer

This whitepaper provides general engineering guidance and does not replace application-specific design review, supplier specifications, regulatory assessment or formal product qualification. Performance depends on the exact components, implementation, environment and usage profile.