ei3

Find the right Cyber-Physical Systems Protection Platform

FOR YOUR MANUFACTURING SHOP FLOOR

Cyber-Physical Systems (CPS) are vital to modern manufacturing, driving productivity and efficiency across plants. But as digital technologies and interconnected systems grow, so do the vulnerabilities. Remote connectivity–a core feature of CPS–adds significant risks that must be managed.

This eBook underscores the importance of CPS Protection Platforms in mitigating those risks while unlocking the full potential of IoT in manufacturing. It covers key features and benefits, providing a comprehensive checklist to help you assess vendors.

With 25 years of experience protecting industrial machines, ei3 checks every box–delivering the security and capabilities manufacturers need to stay ahead in an increasingly connected world.

Spencer Cramer
CEO & Founder of ei3

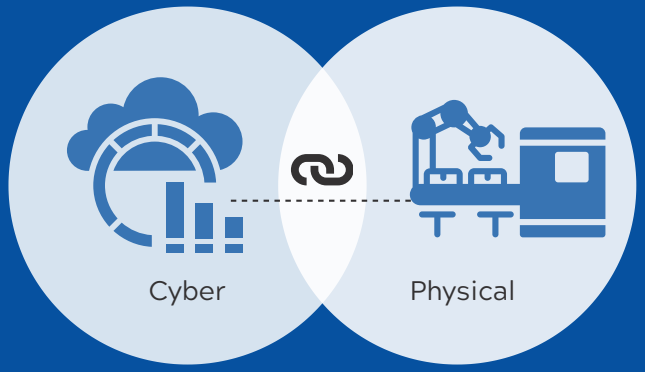
Contents

Understanding **CPS in manufacturing**

Cyber-Physical Systems (CPS) in manufacturing combine computational and physical components, using advanced computing and communication to monitor, control, and interact with physical processes in real-time. This integration enables smart, responsive manufacturing machinery.

Key components include:

- **Physical:** Sensors, actuators, and mechanical parts
- **Computational elements:** PLCs, Industrial PCs, embedded systems, and software
- **Data storage and processing:** Local storage, edge computing, and cloud integration
- **Communication interfaces:** Industrial protocols and internet connection



CPS are crucial for driving **innovation**, **efficiency**, and **competitiveness** in manufacturing

They support Industry 4.0 by using IIoT, AI, and cloud computing for predictive maintenance, reducing downtime, and improving Overall Equipment Effectiveness (OEE) to enhance manufacturing agility and productivity.

The need for **CPS Protection Platforms**

While CPS offers significant benefits, they also introduce vulnerabilities. Manufacturing has been the most-attacked industry for three consecutive years, with 63% of manufacturers already experiencing cybersecurity incidents that have impacted their operations. With over 1.5 million devices connected to the internet, the risk of attack is more prevalent than ever.[1] Remote connectivity, a key advantage of CPS, continues to introduce cybersecurity risks.

Traditional methods of remote access, such as "black boxes," direct VPN access, and cellular modems, come with significant vulnerabilities:

- **Black boxes** lack management and auditing capabilities.
- **Direct VPN access** poses challenges in user management and access control.
- **Cellular modems** incur high data costs and may lack reliability.

CPS Protection Platforms offer a comprehensive solution to these challenges, providing centralized management, auditing, and control. They ensure the security of manufacturing processes, data, and assets while addressing the vulnerabilities in traditional methods.

#1

Manufacturing ranks as the #1 most-attacked industry for three consecutive years [2]

63%

of manufacturers have had factory operations affected by cybersecurity incidents [2]

3 out of 4

industrial organizations have suffered OT cyber attacks [3]

Key features of CPS Protection Platforms ⇲

- Improved safety and reliability
- Data protection
- Operational efficiency
- Informed decision-making
- Future-proofing for smart manufacturing advancements

By adopting a CPS Protection Platform, manufacturers can safeguard their operations, protect sensitive data, and prepare for future technological advancements, ensuring long-term success and resilience in their manufacturing operations.

A CPS Protection Platform is a holistic approach that combines various security technologies, policies, and practices to protect CPS from cyber threats, unauthorized access, and malicious activities

Essential components include:

- ✓ **Enhanced security:** Multi-layered security with network segmentation, encryption, authentication, and access control.
- ✓ **Threat detection and response:** Advanced capabilities for identifying and addressing security breaches in real-time.
- ✓ **Secure remote access:** VPNs and multi-factor authentication for authorized personnel.
- ✓ **System integrity validation:** Firmware checks and code signing to prevent unauthorized modifications.
- ✓ **Data protection:** Secure protocols and encryption for safeguarding data transmission.
- ✓ **Centralized management:** Security management, logging, and reporting capabilities for monitoring and compliance.

CPS Protection Platform **evaluation checklist** ↘

Choosing a CPS Protection Platform is a critical decision that will impact your operations for years to come. With many options in the market, it can be challenging to determine what's essential for your specific needs.

This comprehensive checklist will help you evaluate potential platforms, ensuring you select a solution that aligns with your organization's security requirements and business objectives. Use this checklist to assess CPS Protection Platforms for robust security, data collection, analytics, and integration capabilities. Your choice will be crucial in securing a successful digital transformation journey.

Download the printable checklist here →

Evaluate top-tier security platforms across these 7 critical areas

1. Enhanced security features
2. Seamless integration with existing security infrastructure
3. Data collection and analytics
4. CPS intelligence and AI integration
5. Middleware and integration with existing databases and data analytics
6. Ease of use and management
7. Vendor support and ecosystem

CPS Protection Platform **Evaluation Checklist**

1. Enhanced security features	Priority	ei3	*Evaluated Vendor B*	*Evaluated Vendor C*
Multi-layered security (network segmentation, encryption, authentication, access control)		✓		
Advanced threat detection and response capabilities		✓		
Continuous monitoring and alerting		✓		
Compliance with industry security standards (ISO 27001, IEC 62443, NIST)		✓		

CPS Protection Platforms employ network segmentation, encryption, authentication, access control, and continuous monitoring to make remote access more secure, no matter the method (black boxes, cellular, VPN, DMZ-hosted apps, etc.).

2. Seamless integration with existing security infrastructure	Priority	ei3	*Evaluated Vendor B*	*Evaluated Vendor C*
Compatibility with existing security tools (firewalls, IDS, SIEM)		✓		
Use of open standards and APIs for easy integration		✓		
NAT used to support existing machine control networks		✓		
Unified visibility and control across the entire manufacturing environment		✓		
Ability to leverage existing investments in security technologies		✓		

CPS Protection Platforms seamlessly integrate with firewalls, IDS, and SIEM tools, using open standards and APIs for smooth data exchange while preserving existing investments.

3. Data collection and analytics	Priority	ei3	*Evaluated Vendor B*	*Evaluated Vendor C*
Secure and reliable data collection from CPS devices		✓		
Support for various communication protocols including legacy (e.g., OPC UA)		✓		
Secure data transmission and storage		✓		
Integration with cloud-based analytics platforms		✓		
Role-based access control for data access and manipulation		✓		

CPS Protection Platforms securely collect and transmit plant floor data to the cloud, driving digital transformation for improved decision-making, process optimization, and predictive maintenance, while reducing inefficiencies and downtime.

4. CPS intelligence and AI integration	Priority	ei3	*Evaluated Vendor B*	*Evaluated Vendor C*
Edge computing capabilities for real-time data processing and decision-making		✓		
Support for machine learning and AI algorithms		✓		
Secure deployment of AI models at the edge and in the cloud		✓		
Continuous learning and adaptation to changing conditions		✓		
Scalability to handle large volumes of data and complex analytics workloads		✓		

CPS Protection Platforms enable real-time decision-making and autonomous operations with AI, using secure edge computing for fast data processing. They aggregate and process data, supporting AI deployment at the edge and in the cloud.

5. Middleware and integration with existing databases and data analytics	Priority	ei3	*Evaluated Vendor B*	*Evaluated Vendor C*
Middleware components for data normalization, protocol translation, routing		✓		
APIs and connectors for integration with enterprise systems (ERP, MES, SCM)		✓		
Compatibility with both on-premises and cloud-based analytics tools		✓		
Ability to combine CPS data with other data sources for holistic insights		✓		

CPS Protection Platforms bridge CPS devices and enterprise systems, integrating databases and analytics for a complete operational view. APIs and connectors ensure seamless integration, optimizing processes and improving OEE.

6. Ease of use and management	Priority	ei3	*Evaluated Vendor B*	*Evaluated Vendor C*
Intuitive user interface for configuration and monitoring		✓		
Automated device discovery and provisioning		✓		
Centralized management and policy enforcement		✓		
Role-based access control for administrative tasks		✓		
Comprehensive reporting and auditing capabilities		✓		

CPS Protection Platforms provide user-friendly interfaces and centralized dashboards. They automate device discovery, provisioning, and role-based access control, streamlining management and reducing IT's administrative burden.

7. Vendor support and ecosystem	Priority	ei3	*Evaluated Vendor B*	*Evaluated Vendor C*
Proven track record and expertise in industrial cybersecurity		✓		
Responsive technical support and customer service		✓		
Regular software updates and security patches		✓		
Extensive partner network for integration and deployment services		✓		
Strong user community and knowledge sharing resources		✓		

These platforms include robust vendor support, regular updates, and security patches. Their broad partner ecosystem ensures seamless integration, with strong user communities enhancing effectiveness.

How ei3 checks every box on your checklist ✓

1 .Enhanced security features	ei3 advantage
Multi-layered security (network segmentation, encryption, authentication, access control)	Network segmentation, encryption, and robust authentication and access control implemented in the Amphion edge device to isolate critical machine networks and protect data
Advanced threat detection and response capabilities	Utilizes outbound-only VPNs to secure communication, with global ei3 security centers ensuring a proactive threat management approach
Continuous monitoring and alerting	Provide 24/7 monitoring and real-time alerts for instant threat detection and response
Compliance with industry security standards	Compliance with ISO 27001, IEC 62443, and NIST standards

2. Seamless integration with existing security infrastructure	ei3 advantage
Compatibility with existing security tools (firewalls, IDS, SIEM)	Integrates seamlessly with major firewalls (Cisco, Fortinet, Palo Alto) and existing IDS and SIEM solutions
Use of open standards and APIs for easy integration	Employs open standards and APIs for efficient deployment and integration
NAT used to support existing machine control networks	Supports NAT to connect existing machine control networks without major reconfigurations
Unified visibility and control across the entire manufacturing environment	Provides a single interface for centralized monitoring and management of all connected machines
Ability to leverage existing investments in security technologies	Enhances existing security investments by working alongside current firewalls, IDS, and SIEM technologies

3. Data collection and analytics	ei3 advantage
Secure, reliable data collection from CPS devices	Secures data from 35+ PLC families with local storage and processing
Supports communication protocols, legacy too	Supports a range of protocols including OPC UA, Profibus, Modbus, and DeviceNet
Secure data transmission and storage	Transmits data through secure tunnels and stores it in secure data centers
Integration with cloud-based analytics platforms	No-code apps for IoT and data integration with AWS, Azure, or Google Cloud
Role-based data access and control	Advanced data governance with role-based access for builders and owners

4. CPS intelligence and AI integration	ei3 advantage
Edge computing capabilities for real-time data processing and decision-making	Supports edge deployment with Docker containers for real-time decision-making and low-latency processing
Support for machine learning and AI algorithms	Provides a framework for ML and AI applications, enabling predictive solutions
Deployment of AI models at the edge and cloud	Enables flexible and secure deployment of ML and AI models on edge devices and in the cloud
Continuous adaptation to changing conditions	Employs Centralized Federated Learning (CFL) for continuous learning and adaptation
Scalability to handle large volumes of data and complex analytics workloads	Maintains a secure private cloud infrastructure designed for scalability and handling large volumes of data and complex analytics

5. Middleware and Integration with existing databases and data analytics	ei3 advantage
Middleware and Integration with existing databases and data analytics	Provides tools for normalizing data, translating protocols (e.g., OPC UA, Modbus), and routing data between systems
APIs and connectors for integration with enterprise systems (ERP, MES, SCM)	Offers APIs and connectors for seamless integration with ERP, MES, and SCM systems like SAP, Oracle, and Infor
Compatibility with both on-premises and cloud-based analytics tools	Compatible with on-premises tools (e.g., Tableau, QlikView) and cloud-based platforms (e.g., Power BI, Amazon QuickSight)
Ability to combine CPS data with other relevant data sources for holistic insights	Integrates CPS data with other sources (e.g., quality control systems, CRM) for comprehensive insights and improved operational efficiency

6. Ease of use and management	ei3 advantage
Intuitive user interface for configuration and monitoring	Provides an easy-to-use interface for configuring and monitoring devices, with tools for both machine builders and end customers
Automated device discovery and provisioning	Automatically detects and provisions new devices with appropriate security policies and settings, reducing manual effort
Centralized management and policy enforcement	Centralized console for defining security policies, configuring settings, and monitoring device status to ensure consistency and compliance
Role-based access control for administrative tasks	Includes granular RBAC features to control user permissions based on roles, enforcing the principle of least privilege
Comprehensive reporting and auditing capabilities	Offers detailed reporting and auditing to track user activities, configuration changes, and security events for compliance and analysis

7. Vendor support and ecosystem	ei3 advantage
Proven track record and expertise in industrial cybersecurity	With 25 years of experience, ei3 has established a strong reputation in industrial cybersecurity, trusted by major machinery builders and corporate IT departments
Responsive technical support and customer service	Provides comprehensive technical support and collaborates closely with partners to navigate industrial cybersecurity challenges
Regular software updates and security patches	Delivers frequent software updates and security patches to maintain the CPS Protection Platform's security against emerging threats
Extensive partner network for integration and deployment services	Partners with machine and equipment builders for seamless integration and deployment, ensuring comprehensive solutions across various devices
Strong user community and knowledge sharing resources	Supports a vibrant user community with access to events, whitepapers, case studies, and webinars

ei³: **A pioneer** in CPS Protection Platforms ↘

For over 25 years, ei³ has been at the forefront of delivering secure protection to industrial machines, long before the term "CPS Protection Platform" became mainstream. As a visionary in the field, ei³ recognized early on the critical importance of safeguarding connected devices and systems in manufacturing environments.

Tailored for top industrial machinery companies in the AI and Industry 4.0 era, ei³'s battle-tested platform meets global manufacturing standards and provides a secure, scalable foundation for connected operations. With robust security, seamless integration, advanced analytics, and AI-driven insights, ei³ empowers machine builders in digital transformation.

Explore ei3's CPS Protection Platforms →

Today, ei³ has crafted a **comprehensive solution that encompasses all the essential features of a CPS Protection Platform,** setting the standard for industrial cybersecurity.

Get started **with ei3** ⇲

Book a personalized discovery call

Take the first step towards unlocking the full potential of your manufacturing operations by scheduling a personalized demo or consultation with our team. Contact us

Review additional resources

Explore manufacturing optimization with ei³'s resource library. Download case studies, white papers, and product brochures for valuable insights into business transformation. Whether enhancing machine utilization, improving quality management, or promoting sustainability, find actionable strategies for success. Access our library of resources

For more information
contact@ei3.com
www.ei3.com

References ⇲

1. The State of Cybersecurity in the Manufacturing Industry. Retrieved from Ponemon Institute.
2. IBM X-Force Threat Intelligence Index 2024. Retrieved from IBM.
3. The state of OT Security 2024. Retrieved from ABI Research and Palo Alto Networks.