

Securing the Future: SDI CyberSecurity for ICS and OT Systems

White Paper

Industrial CyberSecurity is no longer a reactive measure but a strategic pillar for business continuity and operational safety. As cyber threats increasingly target Operational Technology (OT) and Industrial Control Systems (ICS)—especially across sectors such as energy, oil & gas, critical infrastructure, manufacturing, water treatment, and renewable energy—organizations must adopt a proactive and layered defense strategy.

This white paper presents SDI's comprehensive CyberSecurity approach, built on 50 years of experience in automation and control systems. It outlines how SDI integrates protection "by design", aligns with global regulatory frameworks, and addresses the growing convergence between IT and OT domains. Special emphasis is placed on evolving threat vectors, the need for real-time monitoring, and resilient architectures tailored for complex industrial environments.

SDI product supplies are developed in collaboration with customers, adopting CyberSecurity policies at the application and architectural levels that are based on risk assessment and take into account the Directives and Regulations in force in the country hosting the supervised and controlled system — e. g. NIS 2 and the recently adopted Cyber Resilience Act in Europe, along with international and local Frameworks — such as NIST and ISO 27001 certification.

Through a structured paradigm of five protection layers—Design, Protection, Maintenance, Surveillance, and Response—SDI delivers robust security solutions capable of mitigating risk across the entire Purdue Model. This document serves as both a strategic overview and a technical reference for organizations aiming to secure their industrial ecosystems against current and emerging threats.



Our CyberSecurity Vision: Reliability, Security, and Operational Continuity

Industrial CyberSecurity has become a key enabler for operational resilience and strategic protection. In a context where Operational Technology (OT) and Industrial Control Systems (ICS) are increasingly exposed to cyberthreats, SDI ensures a CyberSecurity posture focused on three essential pillars: reliability, security, and operational continuity.

Evolving Threat Landscape: ICS and OT Under Attack

Cyberattacks targeting ICS and OT systems have steadily increased in both complexity and frequency. Industrial sectors such as energy, oil & gas, critical infrastructure, manufacturing, and water treatment are now in the crosshairs of ransomware groups and state-sponsored attackers. Notably, the expansion of smart grids, distributed generation, and renewable energy sources—such as solar farms and wind turbines—has introduced new surfaces for attack and complexity in securing highly distributed assets.

Cyberattacks against OT/ICS are growing steadily across key sectors. Ransomware campaigns continue to increase in volume and sophistication, with new malware strains specifically developed to disrupt industrial protocols and compromise field devices. Attackers frequently exploit insecure remote access, legacy credentials, and exposed services like Modbus TCP or VNC. The consequences often include loss of control and operational visibility. The ongoing convergence of IT and OT domains amplifies risks, underscoring the urgent need for dedicated industrial CyberSecurity strategies based on visibility, segmentation, and layered protection.

Threats are no longer confined to the perimeter or enterprise zones—they now span the full extent of the Purdue model, from enterprise systems to field-level devices.

Our Architectures: Resilient and Customizable

With 50 years of field experience, SDI has developed intrinsically resilient architectures that incorporate system-level and network-level redundancy. These include hot-backup mechanisms and Parallel Redundancy Protocol (PRP). Upon request, customized disaster recovery architectures are provided, including geographically separated hot-backup replicas of the main system.

Security by Design: Tailoring Protection from the Ground Up

Every SDI solution integrates security by design and by default. This means that protection is embedded from the earliest design phases, including risk assessment, secure architecture planning, and pre-configured hardening policies. This is especially critical for plants operating with high levels of automation and intermittency, such as those integrating renewable energy sources, where the control logic must remain secure despite external volatility.

Regulatory-Conscious Solutions

SDI's CyberSecurity policies are aligned with both customer needs and applicable Regulations, Frameworks and Standards, including ISO/IEC 27001, IEC 62443, the EU Cyber Resilience Act, NIS 2 Directive, NIST SP 800-82, and other regional and international Frameworks.

SDI product supplies are developed in collaboration with customers, adopting CyberSecurity policies at the application and architectural levels that are based on risk assessment and take into account the Regulations and Directives in force in the country hosting the supervised and controlled system—such as ISO 27001 and the recently adopted Cyber Resilience Act in Europe, along with other international and local CyberSecurity Laws and National Plans.

ISO/IEC 27000 Family

Defines the requirements for implementing and continuously improving an Information Security Management System (ISMS). Some standards in this family can be adapted to meet the specific security needs of Industrial Control Systems (ICS). SDI is ISO/IEC 27001:2022 certified for the design, development, implementation, commissioning, and post-sales support of computerized control systems (hardware and software) for industrial processes and dedicated microprocessor-based systems.

BSI 100-2

Guidelines from the German Federal Office for Information Security for managing information security within organizations.

NIST SP 800-82

Guide to Industrial Control Systems (ICS) Security (USA) An extension of the NIST CyberSecurity Core Framework, providing security guidelines for Industrial Control Systems (ICS) while considering performance, reliability, and safety requirements.

IEC 62443

A global standard designed to secure ICS and Operational Technology (OT) networks, offering CyberSecurity guidelines for manufacturers, system integrators, and industrial plant operators.

NIS 2 Directive (EU Directive 2022/2555)

Effective since 2022, this update to the 2016 NIS Directive strengthens CyberSecurity measures for critical infrastructures and essential sectors across the European Union.

ENISA Good Practice Guide on National Cyber Security Strategies (EU)

In line with the regulatory requirements of the NIS 2 Standard, the ENISA Good Practice Guide on National Cyber Security Strategies provides a framework for EU member states to create and maintain consistent, robust security strategies capable of responding to emerging threats.

Security at Every Level



EU Regulations

SDI is ready to comply with the new EU regulations that will come into effect on Oct. 17, 2024, under which companies operating critical infrastructure and essential services must take into account the security requirements defined by the European Union with the new NIS2 directive focused on network and information system security and the Cyber Resilience Act (CRA) directive that sets requirements.



Non-EU regulations

SDI ensures compliance with the most stringent CyberSecurity policies worldwide, adapting to local regulations and specific client needs.



CyberSecurity Policies

SDI applies comprehensive CyberSecurity policies to ICS systems that manage energy production and distribution as well as SCADA systems used for critical infrastructure supervision and control.



From Compliance to Strategic Governance

SDI does not see compliance as a final goal, but rather as the foundation of a broader governance strategy. Regulatory alignment is integrated into the development and maintenance lifecycle, supporting customers' auditability, traceability, and long-term cyber resilience.

IT-OT Convergence: A New Attack Surface

As IT and OT environments continue to merge, organizations must recognize and mitigate the new risks stemming from shared networks, remote access paths, and cloud integration. SDI addresses this challenge by deploying segmented architectures, DMZs, secure remote access, and endpoint identity enforcement, reducing the exposure of industrial systems to threats originating in the IT domain. In sectors such as renewable energy, where distributed assets are monitored and managed remotely, this convergence requires additional layers of secure orchestration and centralized visibility.

Lifecycle-Based Security

SDI applies comprehensive CyberSecurity policies to ICS systems that manage energy production and distribution as well as SCADA systems used for critical infrastructure supervision and control.

CyberSecurity in industrial environments is not a one-time implementation, but a continuous process that must follow the entire lifecycle of the system—from initial design and deployment, through daily operations, maintenance, updates, and finally to decommissioning. Each stage introduces specific risks and opportunities for mitigation, making it essential to embed security as an ongoing discipline across the system's full operational span.

Our approach is structured into five protection layers



1 - Design

- Redundancy: Implementation of redundant systems to ensure operational continuity.
- Disaster Recovery: Planning of disaster recovery strategies.
- Recovery Strategies Planning: Definition of detailed recovery plans.
- Network Architecture: Design of secure network architectures.
- Firewalling: Implementation of firewalls to protect networks.
- Segmentation: Network segmentation to limit the propagation of attacks.

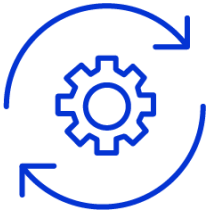
The foundation of secure industrial systems is laid during the design phase. SDI implements redundancy at both the system and network levels to ensure continuous operation, even in the event of component failure. This includes disaster recovery strategies, secure network architectures with strict segmentation, and the deployment of firewalls to limit unauthorized access. Planning begins with risk analysis and is supported by tested recovery strategies to maintain availability and safety.



2 - Protection

- Vulnerability Assessment: Evaluation of system vulnerabilities.
- Malware Protection: Protection against malware and other threats.
- White-listing: Use of whitelists to control software execution.
- Hardening: Strengthening system security.

Once a system is designed, its protection mechanisms must ensure integrity and resistance to compromise. SDI conducts thorough vulnerability assessments and implements hardening procedures to reduce the attack surface. Malware protection tools, allow-listing controls, and system-level configuration controls are applied to block unauthorized software and suspicious behaviors.



3 - Maintenance

- Asset Management: Management of IT assets.
- Operative System Patching: Application of patches to operating systems.
- Software Patching: Updating software to correct vulnerabilities.

Security is not static—it must evolve as threats and systems change. The maintenance layer includes continuous asset management, ensuring visibility into all components of the ICS landscape. Timely patching of both operating systems and application software is essential to mitigate known vulnerabilities, supported by configuration management and version control.



4 - Surveillance

- Devices or Software Probes: Use of devices or software for monitoring.
- Event Logging: Logging of security events.
- SIEM Log Management: Log management through SIEM systems.
- KPI Calculation: Calculation of key performance indicators.
- XDR/EDR AI Pattern Recognition/Prognostic: Pattern recognition and prognostics through AI in XDR/EDR platforms.

Monitoring is critical to detect threats before they impact operations. SDI deploys probes and sensors across the OT environment to collect telemetry, log events, and identify anomalies. Advanced threat detection platforms (such as SIEM or XDR) analyze data and apply AI-driven pattern recognition to detect early indicators of compromise. KPIs are calculated and monitored to support real-time decision-making.



5 - Response

- Containment: Containment of threats.
- Mitigation: Mitigation of attack effects.
- Blocking: Blocking of malicious activities.
- Collaboration with Client CERT: Collaboration with the client's Computer Emergency Response Team (CERT).
- Recovery Strategies Execution: Execution of recovery strategies.

Effective CyberSecurity also means being prepared to react. SDI enables swift threat containment and mitigation through automated and manual procedures. Malicious activities are blocked, and coordinated response protocols—often in collaboration with the client's CERT—ensure quick restoration of services. Recovery plans are executed to resume operations with minimal impact.

Reference Architecture: Aligned with the Purdue Model

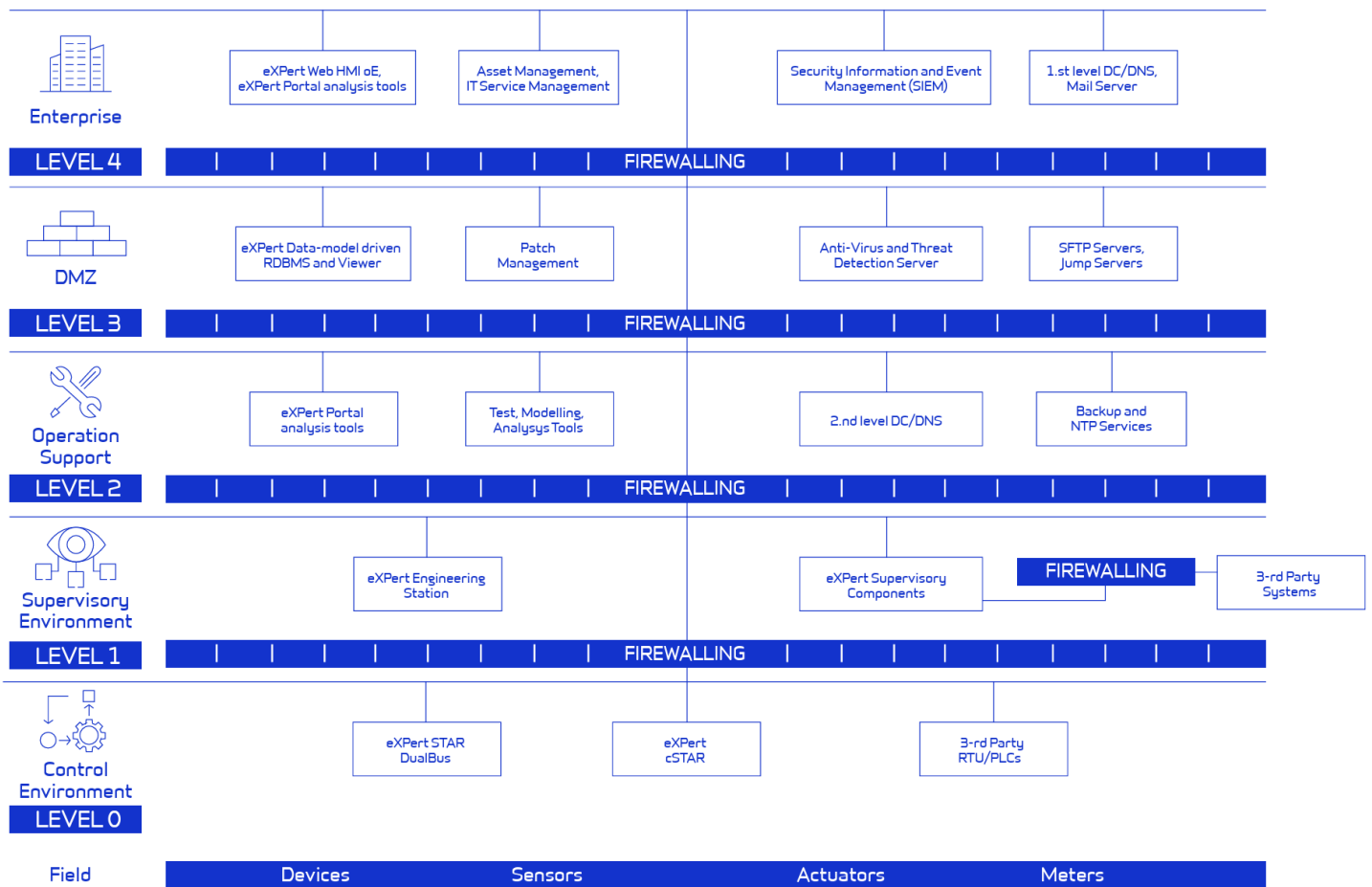
Our reference architecture aligns with the Purdue Model for Industrial Control System architecture, enforcing segmentation and control from enterprise to field levels.



Securing Industrial Future: SDI CyberSecurity for ICS and OT Systems



SDI solutions are deployed across all layers of the model, and security mechanisms are applied consistently—reflecting the reality that today’s threats are moving across all zones, from business systems to control logic and I/O.





Securing Industrial Future: SDI CyberSecurity for ICS and OT Systems

About SDI

Since 1973, SDI is the main Italian company in the field of automation, supervision, control and remote control of highly critical industrial plants.

SDI develops, builds and supplies complete DCS and SCADA systems and special application equipment to main Italian players like Eni, SNAM and ENEL Green Power.

More than 50 years of experience grant the know-how for continue innovation and evolution of SDI's offer.

Our value: ahead on Automation path

Flexibility & Integration at first place: we can provide a completely custom solution that meets every control, monitoring and remote-control need.

Field-proven reliability: hundreds of applications in the field of oil & gas, power production and distribution, public utilities, water, renewables, transport.

Our commitment to development: we invest every day in improving our solutions, thus creating a strong relationship with the customer.

Valuable data, everywhere: we can provide the information you need on every device, anytime.

For years, we have had a certified Management System in accordance with ISO 9001 (Quality), ISO 14001 (Environment), ISO 45001 (Occupational Health and Safety), and ISO/IEC 27001 (Information Security) standards. DNV - one of the leading global certification bodies - periodically verifies its effectiveness.



Contacts

mkt@sdiautomazione.com

<https://sdiautomazione.com/contact-us>