Complete Solutions to Protect Availability, Safety and Reliability of Industrial Facilities
WE HEAR ABOUT CYBER INCIDENTS EVERY DAY IN THE NEWS, BUT JUST HOW RELEVANT ARE THESE EVENTS TO YOUR BUSINESS? IF YOU’RE AN INDUSTRIAL MANUFACTURER WITH CRITICAL PLANT ASSETS, THEY’RE MORE RELEVANT THAN YOU MAY THINK.
Security Demands from the Control Room to the Board Room

Today’s Industrial Automation and Control System (IACS) is more advanced and complicated than ever before. No longer are plant automation assets and critical infrastructure truly isolated. With automation suppliers implementing new open technologies and communication protocols, controls systems are increasingly vulnerable to attack, disruption and damage.

Information derived from the IACS is invaluable to plant managers to ensure efficient processes and safe operations. It also assists company executives in decision making to advance their profitability and gain an advantage in a competitive marketplace. However, the growth of data acquisition systems accessing this information, coupled with the adoption of open architectures, increases risks to the control network.

For Industrial Sites, Vulnerabilities Can Include:
- Lack of defined security zones, and insecure conduits/connections between zones
- Unsecured staff access for internal maintenance, retrieval of historian data, etc.
- Remote third-party contractor and vendor access
- Removable media brought onto the site, including USB drives, external hard drives, and even laptops and smart phones
- Out-of-date malware signatures
- Obsolete or unpatched operating systems
- Poorly configured, inadequate or missing cyber security countermeasures.

Industry-Leading Experience and Expertise

As new threats emerge and the cyber security landscape evolves, you need an experienced and trusted partner to help protect the availability, reliability and safety of your control system assets, as well as safeguard people and processes involved in all facets of your operation.

Honeywell’s Industrial Cyber Security Solutions are specifically designed to defend your IACS and plant operations. These solutions leverage our process control and cyber security experience, expertise and advanced technology to provide industry-leading offerings. Strategic relationships with technology players including Intel® Security, Cisco™, Microsoft and others, further extend the value of these solutions.

Honeywell has a 50-year history as a leader in industrial safety and security, and as an innovator in the field of plant automation. Years of providing industrial cyber security solutions have resulted in proprietary methodologies, best practices, and a comprehensive understanding of cyber security requirements for the process control domain.

When it comes to applying technology to solve some of the most critical challenges related to safety and security, few companies can claim Honeywell’s record of achievement:
- The International Society of Automation (ISA)
  - ISA99 active committee participation for 10+ years
  - Honeywell best practices incorporated into ISA standards
- First Supplier to Earn ISA Secure Embedded Device Security Assessment (EDSA) Certification
- Founding Member of ISA Security Compliance Institute (ISCI).

Honeywell Industrial Cyber Security professionals have an unrivaled track record in process control and operational technology, cyber security and IT— an essential skill set combination for protecting plants and critical infrastructure.

Certifications held by our global team include Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Cisco Information Security Specialist (CISS), Certified Ethical Hacker (CEH) and GIAC Certified Incident Handler (GCIH).
Proven Know-How to Protect Your Organization

From refining, petrochemicals, power and oil and gas, to pulp and paper and metals and mining, Honeywell is committed to helping customers anticipate and resist future classes of cyber attacks. Indeed, cyber security is a key element of Honeywell’s entire product development strategy. We’re foremost in the automation industry in our investment in cyber security technology for process control systems, including our state-of-the-art Industrial Cyber Security Lab. This investment enables us to maintain our leadership in the industry, serving as a single source for protection at all levels of the IACS infrastructure.

Honeywell Industrial Cyber Security Lab, Atlanta, Georgia, USA: A world-class environment for proprietary cyber security research and development, test and certification, training and collaboration with partners and educators.

Honeywell leverages a long history in plant safety and physical security to offer comprehensive cyber security solutions that ensure multiple layers of defense to help organizations:

- Meet regulatory compliance requirements
- Defend against emerging cyber security threats specific to the IACS
- Establish secure connections between plant networks and the IT network
- Extend internal staffs with industrial control system cyber security expertise
- Ensure ongoing awareness of new vulnerabilities and Advanced Persistent Threats (APTs)
- Improve production performance and reduce plant downtime
- Timely response to, and fast recovery from, cyber incidents.
Complete Solutions for Industrial Environments and Critical Infrastructure

Leading companies worldwide partner with Honeywell to achieve robust cyber security capabilities enabled by advanced technology, comprehensive training, and best practices. With recognized domain expertise in the process industries, we deliver end-to-end solutions designed for the specific needs of control system environments and critical infrastructure sectors.

Honeywell’s industrial cyber security know-how encompasses automation assets and their integrated communication networks—a distinct advantage in control system security. The Honeywell Cyber Security Architecture and methodology support IEC 62443 concepts, continually addressing cyber security throughout the IACS lifecycle—from design and implementation to commissioning—with vendor-agnostic solutions that include security assessments and audits, architecture and design, network security, endpoint protection, situational awareness, and response and recovery.

“When faced with conducting a cyber security vulnerability assessment for a power generation facility, the in-house audit team lacked the right combination of process control and IT security experience. This required a third-party expert with knowledge in both worlds.”

— Honeywell assisted with a collaborative review of IACS and SCADA risk assessment policies and procedures. This process identified high-level risks, with the information used to estimate, prioritize, and coordinate ongoing risk mitigation activities.
Assessments and Audits

Customers rely on Honeywell’s comprehensive cyber security assessments to identify and evaluate their current security posture, and then prioritize efforts to reduce risks. Recurring assessments allow cyber security teams to track their milestones and the maturity of their security program over time to indicate progress toward achieving their desired assurance level.

In addition to cyber security assessments, Honeywell offers network and wireless assessments aligned with leading standards and designed to satisfy the requirements of multiple security assurance levels, providing the right depth and detail to meet your specific needs.

Honeywell also conducts independent audits, which provide a review and examination of records and activities to assess the adequacy of system controls, determine compliance with established policies and operational procedures, and recommend necessary changes. Results from periodic audits provide a view of trends and are presented in the form of performance against predefined metrics.

Architecture and Design

Architecture design decisions determine system configurations and impact the performance characteristics of an automation system. For this reason, Honeywell’s products are designed with built-in security, and our secure architecture approach serves as a long-term baseline for availability, reliability and safety. We provide consultation on possible cyber security architectures and advise customers on the advantages and disadvantages of each topology based on proper segmentation of security zones and conduits.

Network Security

Network security is the first line of defense in providing industrial cyber security to an entire plant or site. But a number of potential pitfalls may arise if it is not implemented properly. Applying a solid understanding of IACS requirements, Honeywell’s network security services result in more secure perimeters and higher reliability for industrial process operations.

For instance, Honeywell offers turnkey solutions for the latest cyber security counter-measures, including next-generation firewalls, advanced threat detection, and security analytics. Honeywell will install, configure and validate the right security for your network. We also help customers develop their own policies and procedures to restrict unauthorized access to system resources and specify authorized users, programs and processes. Controls are set up to manage access, including establishing, activating, modifying, reviewing, disabling and removing access privileges.

Endpoint Protection

Within an industrial control system, every device is a potential entry point for security threats. Endpoint protection is designed to secure each endpoint on the network before device access is granted.

Honeywell’s Endpoint Protection solutions include a suite of services that fortify the network through patching and anti-virus protection, application whitelisting, and node hardening, and portable media security. Our tested and qualified signature files and patches reduce or eliminate time spent evaluating files and patches to verify release versions and correct configurations.

We provide protection management services that deliver qualified patches for Microsoft operating systems and Distributed Control System (DCS) software, as well as anti-malware signature file updates for McAfee and Symantec programs.
“With advancements in process automation for upstream oil and gas come greater cybersecurity risks. There are concerns about personnel safety, damage to expensive assets, loss of production, and impact on company reputation.”

— On a major upstream project, Honeywell delivered architecture and design solutions such as a DMZ leveraging virtualization, as well as endpoint protection, secure connectivity for vibration monitoring, enhanced network management capabilities, and security controls to reduce risk factors.

Situational Awareness
Honeywell’s goal is to ensure ongoing situational awareness of new vulnerabilities and the latest APTs. We help customers interpret and understand activity in a network through continuous monitoring, compliance and reporting, security analytics, security information and event management, and security awareness training.

Our full-day situational awareness workshop is designed to increase the overall security awareness of process control personnel. Three-day advanced training is available with additional material on identifying security violations, incident handling, and reporting. Plus, three-day hands-on training is held in the Honeywell Cyber Security Lab, covering secure network architecture and design, zones and conduits, configuration and use of network and endpoint security controls, and security monitoring.

Response and Recovery
Honeywell stands ready to assist customers develop a sound backup and restore strategy. Identifying an incident early and responding appropriately can limit the consequences of a cyber security event. Honeywell’s automated Response and Recovery Services help users quickly recognize symptoms of an incident such as attempts to reconfigure the IACS software or modify settings which could have various negative effects.

Our services help minimize data loss in the event of a cyber incident or other outage. Plus, we assist with incident and disaster recovery planning to increase your resilience and recovery capability. Additionally, these services help users document incident details for future reference and improve their ability to quickly recover and respond to future attacks.
Get Proactive with Risk Manager

Honeywell’s Industrial Cyber Security Risk Manager is the first solution to proactively monitor, measure and manage cyber security risk for industrial plants and systems, providing users of all levels with real-time visibility, understanding and decision support required for action.

With Risk Manager, there’s no need to be a cyber security expert. Through a user-friendly interface, Risk Manager allows users to prioritize and focus efforts on managing risks that are most important for reliable plant operations. Risk Manager helps plant managers and engineers answer “what now” and “what to do” questions. It offers expert guidance on the potential impact of an event and possible resolutions—removing the complexities of cyber security event management.

Risk Manager provides users with a real-time assessment of information from devices throughout the process control network, enabling them to monitor, measure and manage their cyber security risks in a way not provided or possible before.
Focused on Industrial Control Systems

Risk Manager Focuses Exclusively on Industrial Control System Cyber Security Requirements:

• Monitors risk continuously, in real-time, to provide immediate notification when unacceptable risk is present.

• Translates complex indicators of vulnerabilities and threats into metrics that can be used by control engineers and operators without cyber security experience.

• Tracks and inventories assets on the network, including infrastructure devices, Windows® PCs and servers.

• Evaluates indicators of risk using patented algorithms to generate accurate risk scores in line with industry risk management standards from ISO, ISA and others.

Patented Technologies from People Who Know Industrial Control

Monitor
Continuously looks for indicators of threats and vulnerabilities, analyzes them, and communicates to plant personnel through real-time warnings and alerts.

Measure
Powerful algorithms continuously calculate risk, supporting the development of performance and outcomes-based metrics.

Manage
Supports a risk-based approach for managing overall site risk tied to business priorities and helps plants determine the maturity of their cyber security posture.
Managed Industrial Cyber Security Services

Increase overall security, improve system performance, reduce operational cost and expertly manage the essential elements of your process control infrastructure.

For those companies lacking the dedicated staff to fully benefit from real-time security monitoring and analytics, Honeywell offers a suite of Managed Industrial Cyber Security Services. These services provide the information needed to reduce the risk of security breaches and manage the essential elements of your process control infrastructure.

Supervising the operation of the DCS, Honeywell's sophisticated analysis and reporting solutions provide the insights needed to quickly ascertain the status of critical control system assets.

This approach enhances operating system security, robustness and stability, ultimately contributing to improved production and safety for complex industrial plant operations.

Managed Industrial Cyber Security Services

- Patch & Anti-Virus Automation Protection Management
- Security & Performance Monitoring
- Advanced Monitoring & Co-Management
- Activity & Trend Reporting
- Secure Remote Access & Support
Confidence from Secure Remote Access and Support

Honeywell takes your remote access concerns seriously. Our customers are assured of a virtual platform that’s secure and 100% owned and centrally managed by Honeywell. This guarantees optimization of resources, security, data protection, virus and patching control.

Honeywell’s Managed Industrial Cyber Security Services leverage our Secure Remote Access, which provides a customer-initiated connection to the Honeywell Security Service Center (HSSC). This solution employs a certificate-based, two-factor authentication process to create an encrypted tunnel—protecting data even through the site’s corporate network. Additionally, our Secure Service Node and Relay Server work together for hardened control network security.

The Secure Remote Access can serve as a single point of access for third-party vendors and contractors if desired. Providing policy-based, controlled communications with a record of all actions, it can be a useful tool in tracking third-party activities.

Honeywell Security Service Center, Houston, USA: Honeywell’s Security Service Centers deliver Managed Industrial Cyber Security Services. Centers in Europe and the U.S. provide global support and are the termination points for Honeywell Secure Remote Access.
Honeywell—A Single Source for All Your Needs

Honeywell Industrial Cyber Security is the leading provider of cyber security solutions that help protect the availability, safety and reliability of industrial facilities, critical infrastructure and the Industrial Internet of Things (IIoT).

Leveraging our industry-leading process control and cyber security experience, our expertise, and technology, Honeywell delivers proven solutions designed for the specific needs of process control environments and critical infrastructure sectors.

Our portfolio includes Managed Industrial Services for process control infrastructure protection, and the Industrial Cyber Security Risk Manager solution which proactively monitors, measures and manages industrial cyber security risk.

We also offer consulting and remediation services including security assessments and audits, architecture and design, network security, endpoint protection, situational awareness, and response and recovery.

These solutions are enabled by innovative technology and delivered by a global team of cyber security experts.

For More Information

To learn more about Honeywell's Industrial Cyber Security Solutions, visit www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions

Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Zunyi Road
Shanghai, China 200051

www.honeywellprocess.com

Experion® is a registered trademark of Honeywell International Inc.
*All other trademarks are the property of their respective owners.