



## Summary

The overall protection and safety of a nuclear power plant is the primary objective of every facility. Inven·sys has the knowledge, expertise and resources to implement Nuclear Cyber Security Solutions that protect the digital assets of a plant's critical infrastructure.

## Business Value

Compromises to critical nuclear system infrastructure assets from cyber attacks can have a significant detrimental impact to plant safety and operations. Inven·sys' Nuclear Cyber Security Solutions offer:

- A holistic approach that addresses the core tenets of NEI 08-09
- A focus on the control automation layer first, then the corporate IT layer
- A proven, repeatable methodology

Real Collaboration.  
Real-Time Results.™

# Nuclear Cyber Security Solutions

Inven·sys' Critical Infrastructure and Security Practice (CISP) offers solutions that provide a cyber-secure network infrastructure, securing critical systems with two key areas of focus:

- A lifecycle approach as opposed to a point solution within the control automation area, and
- Optimization through network management and secure data acquisition

Nuclear Cyber Security Solutions address critical nuclear system infrastructure needs to help prevent security breaches, satisfy site-/fleet-specific cyber security plan commitments and meet the extensive requirements of the Nuclear Energy Institute's NEI 08-09. Though these solutions regularly complement control systems provided by Inven·sys, CISP brings the same expertise and benefits to any control system, plant or business. As a control system vendor, CISP has worked with many customers across the nuclear industry to identify NEI 08-09 compliance gaps, implement remediation required to meet the standard, and help customers manage their compliance programs.

Nuclear Cyber Security Solutions are hardware and platform agnostic. Solutions are designed specifically to protect industrial control systems, since increasing connectivity, proliferating access points, escalating system complexity and widening use of common operating systems and platforms have all contributed to heightened security risks.





## NUCLEAR CYBER SECURITY SOLUTIONS

Component	Functionality	Benefits
<b>Network Security Scanning and Patch Management</b>	Vulnerability Assessment	Automates discovery of all network devices, operating systems and infrastructure; performs ad hoc scans targeting one or many machines
	Patch Management	Allows processing of patches, auto scanning and inventory; enables multiple machine/patch deployment in schedulable jobs
	Network and Software Auditing	Detailed analysis of what is happening on the network; visibility of applications installed, the hardware on your network and the state of security applications
	Assets Inventory	Creates an inventory of every device on your network
	Change Management	Provides a complete history of network changes and change notifications
	Risk Analysis and Compliance	Security issues are rated by their severity level; provides numerous executive, technical and statistical reports
<b>Management Server</b>	Network Performance Monitoring & Alarming	Quickly detect, diagnose and resolve network performance problems; real-time dashboards enable at-a-glance network performance tracking and network topology maps
	Security Management Software, Anti-Virus, Backup Storage and Testing	Integrate, manage and monitor security programs such as anti-virus and firewall software via an interactive web-based console; centralized backup file storage
<b>Event Logging and Reporting</b>	Security Information and Event Management	Provides centralized event monitoring services collecting data from various systems, archiving events and providing notification capabilities with a central repository of data logs; supports network-wide control and management of Windows event logs, W3C logs, SYSLOG, and SNMP TRAPS
<b>Remote Relay Access Server</b>	Remote Access	Administrative function; diagnostics and configuration; non-operator observation
<b>Cyber Security Workshops</b>	Security Perimeter Workshop	Identify and classify plant's critical digital assets and define appropriate corresponding Electronic Security Perimeters that are easier to manage and maintain compliance
	Network Design and Road Mapping; Active Directory Workshop	Design and road map secondary network required to host security programs, technologies and solutions required for NEI 08-09 compliance
<b>Managed Secure Services</b>	Designs and implements specifically for process control networks; 24/7/365 monitoring of security devices with timely identification and remediation of security vulnerabilities	Eliminates need for expensive full-time security expertise; maximizes reliability and uptime; continues data analysis to identify existing and predict future security challenges; enforces policy management and change control; reduces staff workload; lower and more predictable cost of ownership
<b>Supporting Services</b>	Gap analysis; NEI 08-09 assessments; incident response; documentation policy and procedure creation, updates and assessments; network management	Customizable services that complement and extend Nuclear Cyber Security Solutions; services can be leveraged individually to identify and fill any gaps in client's compliance program or against their internal security posture

To learn more about Invensys' Critical Infrastructure and Security Practice solutions, contact your sales representative or visit: <http://iom.invensys.com/CyberSecurity>.



Invensys • 5601 Granite Parkway III, #1000, Plano, TX 75024 • Tel: (469) 365-6400 • Fax: (469) 365-6401 • [iom.invensys.com](http://iom.invensys.com)

Invensys, the Invensys logo, ArchestrA, Avantis, Eurotherm, Foxboro, IMServ, InFusion, SimSci-Esscor, Skelta, Triconex, and Wonderware are trademarks of Invensys plc, its subsidiaries or affiliates. All other brands and product names may be the trademarks or service marks of their representative owners.

© 2012 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by any information storage and retrieval system, without permission in writing from Invensys Systems, Inc.