

Summary

The Invensys Critical Infrastructure and Security Practice (CISP) organization has developed a comprehensive cyber security compliant solution portfolio which takes a holistic approach to cyber security based on the four tenets of critical infrastructure compliance.

Business Value

The Secure Zone design approach can be deployed at any stage of current network development, providing the ultimate in network design flexibility. CISP's Secure Zone provides a unique approach that ensures full industry cyber security compliance with 10 CFR 73.54, NRC Regulatory Guide 5.71 and NEI 08-09.

Cyber Security Compliant Architecture for the Nuclear Industry

INCREASED PRESSURE

Nuclear power plants are facing increased pressure to address the challenges of cyber security. The Nuclear Regulatory Commission (NRC) Code of Federal Regulation (CFR) 10 CFR Section 73.54 provides guidance for the "Protection of Digital Computer and Communication Systems and Networks." The code is interpreted to include structures, systems, and components (SSC) in the balance of plant (BOP) having direct connection to radiological health. NRC Regulatory Guide 5.71 provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems and networks from a cyber attack as defined by 10 CFR 73.1. These regulations, in conjunction with the Nuclear Energy Institute's NEI 08-09, addressing digital security controls, make the nuclear power cyber security requirements some of the most stringent in the industry.

COMPREHENSIVE CYBER SECURITY

The Invensys Critical Infrastructure and Security Practice (CISP) organization has developed a comprehensive cyber security compliant solution portfolio which takes a holistic approach to cyber security based on the four tenets of critical infrastructure compliance:

- Information security
- Physical security
- Plant safety
- Business continuity

These solutions are unique in that they provide not only security for critical infrastructure, but also integrate seamlessly between manufacturing operations and corporate IT networks. Solutions that address all the needs of a comprehensive cyber security solution:

- Asset identification
- Access controls
- Change tracking and management
- Logging
- Patching
- Backup and restoration
- Anti-malware and anti-virus
- Platform hardening
- Network design and management
- Managed site security

Secure zone cyber security architecture

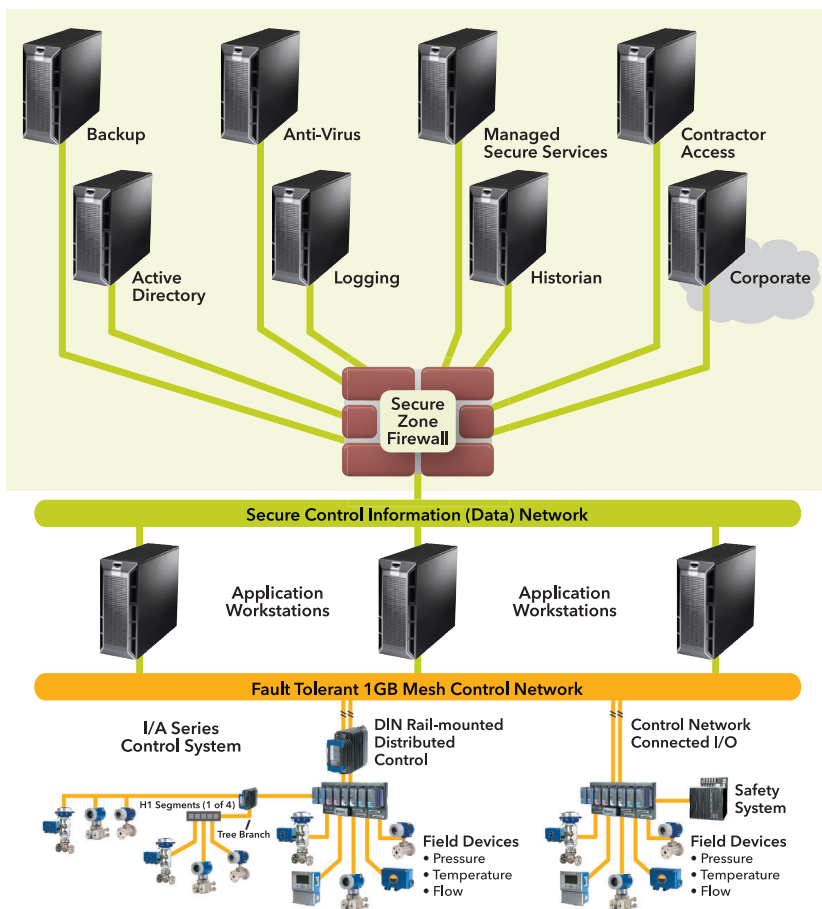
CISP's approach to cyber security design is to first identify all of the network systems elements and their respective functionality and to then design a network that integrates all of these systems, technologies, programs, equipment and supporting processes as set forth by the NEI's "Defense-In-Depth" strategy. The Defense-In-Depth strategy is analogous to CISP's own "Secure Zone" security approach.

Defense-In-Depth

- Allocates an appropriate degree of cyber security protection
- Controls and restricts remote access
- Facilitates one-way direct data flow from higher security levels down
- Enforces security policies and zones

The Secure Zone design approach can be deployed at any stage of current network development, providing the ultimate in network design flexibility.

CISP's Secure Zone provides a unique approach that ensures full industry cyber security compliance with 10 CFR 73.54, NRC Regulatory Guide 5.71 and NEI 08-09.



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

Invensys, the Invensys logo, ArchestrA, Avantix, 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.

© 2011 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.