KINECTRICS

www.kinectrics.com
info@kinectrics.com

Head Office
800 Kipling Ave., Unit 2
Toronto, ON M8Z5G5
416-207-6000

Canada
393 University Ave. 4th Floor
Toronto, ON M5G 1E6

USA
40 Shuman Blvd., Suite 340
Naperville, IL 60563

Germany
Freiberger Strasse 39
01067, Dresden, Germany

Denmark
c/o NJORD,
Advokatpartnerselskab Pilestræde
58 DK-1112, Copenhagen,
Denmark

Romania
59 Grigore Alexandrescu Street.,
2nd Floor
Bucharest 010623
Romania

CS250718

KINECTRICS

Cyber Security at Nuclear Power Plants

Providing engineering for the rapidly evolving cyber security landscape

CYBER SECURITY SERVICES

Kinectrics offers a wide range of Cyber Security services to our clients in the nuclear industry:

Cyber Security Program Planning, Development and Auditing

- Participation in Cyber Security Assessment Team meetings to determine Critical Digital Asset (CDA)/ Cyber Essential Assets (CEA) asset classifications and necessary remediation actions. Multiple employees have attended the Technical Assessment Methodology (TAM) training at EPRI and are capable of preparing assessments and providing input through the modification process using the TAM.
- Development and revision of Cyber Security assessments for direct and indirect CDA/CEAs
- Third party review of Cyber Security upgrade Design Changes and Work Packages, resulting in fewer field changes and ensuring compliance with regulations

Cyber Security Program Implementation

- Engineering, design and implementation support to specific Cyber Security Program Controls, including, but not limited to:
  - o Boundary Isolation Device Installation (Data Diodes, Network Taps)
  - o Defense-In-Depth Bypass Identification and Elimination
  - o Intrusion Detection, Intrusion Prevention, Real-time Network Monitoring and Logging Hardware Installation
  - o Cyber Security management system installation including, but not limited to, antivirus, whitelisting, and WSUS
  - o Time distribution utilizing NTP (UTC, EST, DST) and IRIG-B timecodes
  - o Installation of analog, deterministic KVMs to allow for switching between various layer workstations
- Evaluation of new or existing equipment for Cyber Program compliance and vulnerabilities
- Development of specifications for new equipment procurement
- Design and implementation of physical security requirements in support of Cyber Security Programs, e.g. lock and alarm devices
- Plant and Security Computer (including Video) upgrades to meet NEI 08-09 compliance
- Cyber security tool implementation including, but not limited to:
  - o Security Information and Event Management – including real-time network monitoring, alerting, and logging and syslog storage
  - o Antivirus
  - o Whitelisting
  - o NIDS and HIDS
  - o IPS and IDS
  - o Centralized Management
  - o WSUS
- Remediation for network connections that cross the Protected Area Boundary
- Movement and reclassification of CDA/CEA between various Cyber Security network levels/layers

Value-Added Solutions

- Development of Cyber Security One-Line Diagrams - Plants may have network components represented on dozens of plant configuration drawings. This can make it difficult to see the full defensive architecture, identify Cyber Level bypasses, or to prove that bypasses do not exist. Kinectrics has created drawings that succinctly map a plant's computer network by Cyber Security Level, identify network boarders and boundaries, and identify air-gapped and DMZ networks. These can be used as a permanent plant drawing or as an informational sketch to help with Cyber Security planning and audits.
- Development of contingency and manual actions used in the event of a cyber threat - This allows for proper planning and design development of permanent or automated Cyber Security solutions while ensuring compliance with regulatory deadlines.
- White paper evaluations to validate program elements in support of NRC submission – Kinectrics, for example, authored a white paper to obtain NRC concurrence that a specific network tap device was indeed deterministic. This prevented the need to seprate parts of a network which would have resulted in equipment outages, additional hardware and software, ongoing maintenance on new CDAs, additional licensing fees, etc.
- In-house team of Human Factors Engineering (HFE) specialists to provide input to Design Engineering based on HFE Analysis (Operating Experience Review, Function Analysis and Function Allocation, Task Analysis, Human-System Interface Design) and validation evaluation.
- Kinectrics has developed strong working relationships with vendors and suppliers to ensure that assets are classified and remediated properly. This includes obtaining schematics and interfacing with component manufacturer's engineers to ensure proper identification. We work hand in hand with the vendors who provide cyber compliant systems to validate the solutions being provided. This includes Factory Acceptance Testing and Site Acceptance Testing support.

Kinectrics has qualified engineers and analysts that in the US are badged, safeguards (SGI) and Critical Group qualified and in Canada hold the required CSIS clearance. This paired with our experience positions us to ensure all Cyber Security needs are met.

Kinectrics has been supporting the successful implementation of Cyber Security programs and modifications at plants across the US Nuclear fleet for over 10 years, and more recently in Canada. Our Cyber Security services are comprehensive and address all stages of program implementation.
Kinectrics engineers have experience with NEI 08-09, NEI 13-10 and CSA N290.7 guidelines, and regularly participate in NEI and CANDU Owners Group (COG) Cyber Security workshops. Kinectrics understands the challenges that face nuclear plants when addressing Cyber Security remediation. Combining this specialty knowledge with our extensive in-house experience executing design modifications allows us to deliver smart, useful and cost-effective solutions to our clients during the planning, design, implementation and regulatory inspections for Cyber Security.