

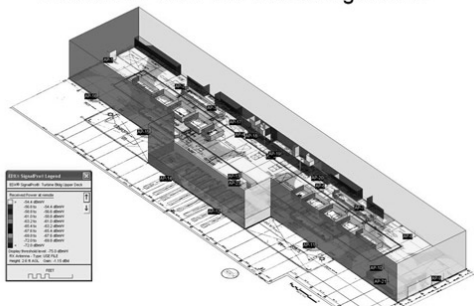
A 10 CFR 73.54-BASED ASSESSMENT OF SAIC'S NUCLEAR 802.11 WIRELESS SOLUTION

SAIC's 802.11 wireless development process enables success in designing, integrating and deployment of wireless infrastructures in the nuclear power plant environment. SAIC has deep expertise in integrating and deploying multiple wireless technologies to achieve the ubiquitous coverage required to seamlessly deliver voice, video, and data services throughout the plant environment. Our solutions are designed to help ensure that design and performance goals are met and that applicable compliance-driven security standards are satisfied.

SAIC has developed a standards-based architecture for effectively and securely deploying Wi-Fi (802.11x) wireless networks within the nuclear power plant environment. Utilizing commercial-off-the-shelf (COTS) products from vendors such as Cisco, Juniper, Redline and others. SAIC is able to create an integrated, common, secure, voice, video, and data network infrastructure that can be used by all operations within the plant in a highly secure and scalable architecture.

SAIC's wireless solution is set up to meet the following goals for plant operations:

Turbine Bldg and Heater Bay Upper Deck
Indoor 2.4 GHz WiFi Coverage in 3D



- *Site-wide communications capabilities for industrial and business applications.*
- *Furnish operations-wide value and utility.*
- *Implement common Internet Protocol (IP) access using standards supporting cybersecurity.*
- *Reducing lead-time and costs associated with wired cabling.*
- *Provision access for sensors, meters and instrumentation and control systems.*

SAIC's wireless implementation process consists of five aspects: design, integration, deployment, testing, and training.

SAIC's wireless **design** builds the radio frequency (RF) profile with theoretical and actual plant data and engineers' network coverage and capacity plans. This includes a physical site survey using an array of tools to collect needed information. The survey effort is normally preceded by an exchange of site diagrams that can be reviewed and processed by appropriate tools. SAIC performs physical measurements within and outside facilities to verify that the estimated square footage of the buildings is accurate and to check distances between key sites.

SAIC **integrates** new wireless technology components with legacy infrastructure and develops a prioritized, phased installation plan. To do this, SAIC stays current with the latest wireless technology and obtains, documents, and maintains an accurate view of the legacy

infrastructure of the client. The installation plan is developed to coordinate with all the client's environment and requirements.

SAIC **deploys** a wireless design by producing a comprehensive bill of material and providing staging, testing, and configuration services. SAIC's process carefully manages installation in coordination with plant resources. SAIC also provides careful and detailed quality assurance activity to assure that established design requirements are met.

SAIC provides two aspects of **testing**: Cable Plant Test and Verification (fiber/copper) and wireless performance testing and acceptance testing. In that way, it helps assure that neither communications mechanism creates a problem for the other and that each operates as planned.

SAIC provides **training** using system documentation that includes as-built and technical manuals, conducting user training, and supporting stakeholder adoption.

Each of these areas is significant in establishing compliance with the wireless-relevant Nuclear Energy Institute (NEI) 08-09 controls.

Compliance Standards and Their Application, Addressing, and Assurance

The essential standard to be met in establishing any form of digital, electronic, wired, or wireless infrastructure within the nuclear power plant environment is compliance with the Nuclear Regulatory Commission (NRC) regulation 10 Code of Federal Regulations (CFR) 73.54, "Protection of digital computer and communication systems and networks" requirements. The security controls needed to support the requirements specified by that regulation are based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 "Recommended Security Controls for Federal Information Systems and Organizations." Both frameworks define the security controls and those of NEI 08-09 [Rev. 6], "Cyber Security Plan for Nuclear Power Reactors." Both NIST and NEI documents serve as the direct basis for the SAIC process described in the present document. We have conducted an assessment of SAIC's wireless infrastructure design against the NEI 08-09 Rev. 06 requirements. Results of that analysis, summarized in Table 1, highlight the key technical and operational aspects of the network, which reflect the overall compliance of the solution. The SAIC solution has been designed to reflect applicable standards, regulations, and clients' needs for the nuclear power plant environment.

Addressing NEI 08-09 Controls requirements

Table 1 describes SAIC's approach for compliance with the NEI 08-09 cybersecurity controls so that the requirements of 10 CFR 73.54 are met. All the sections of Appendix D of NEI 08-09 (Technical Cyber Security Controls) and selected technical control-relevant sections of Appendix E (Operational and Management Cyber Security Controls) are considered while evaluating the SAIC wireless security solution.

The table is expressed in terms of the NEI 08-09 controls (columns 1 and 2). The third column, priority, expresses the criticality of compliance. The control applicability and compliance column are part of the compliance evaluation process. Control applicability defines the applicability of the controls to the overall solution. The second column reflects if the controls have been addressed in the proposed solution, and the third column indicates methodology, through which the control has been addressed in the proposed solution.

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL APPLICABILITY AND COMPLIANCE		
			Applicable	Control Addressed	SAIC Compliance Methodology
Access Control (Technical)					
1.1	Access Control Policy and Procedures	P1	YES	YES	Implementation
1.2	Account Management	P1	YES	YES	Design-based
1.3	Access Enforcement	P1	YES	YES	Implementation
1.4	Information Flow Enforcement	P1	YES	YES	Implementation
1.5	Separation of Duties	P1	YES	YES	Architecture
1.6	Least Privilege	P1	YES	YES	Implementation
1.7	Unsuccessful Login Attempts	P2	YES	YES	Implementation
1.8	System Use Notification	P1	YES	YES	Design-based
1.9	Previous Logon (Access) Notification	P0	YES	YES	Design-based
1.10	Session Lock	P3	YES	YES	Design-based
1.11	Supervision and Review	P1	NA	YES	Architecture
1.12	Security Attributes	P0	YES	YES	Implementation
1.13	Permitted Action Without Identification or Authentication	P2	YES	YES	Implementation
1.14	Automated Marking	P1	YES	YES	Architecture
1.15	Automated Labeling	P2	YES	YES	Implementation
1.16	Network Access Control	P1	YES	YES	Architecture
1.17	Open/Insecure Protocol Restrictions	P1	YES	YES	Architecture
1.18	Insecure and Rogue Connections	P1	YES	YES	Architecture
1.19	Access Control for Mobile dDevices	P1	YES	YES	Architecture
1.20	Proprietary Protocol Visibility	P1	YES	YES	Architecture
1.21	Third-party Products and Controls	P1	YES	YES	Implementation
1.22	Use of External Systems	P2	NA	YES	Implementation
1.23	Public Access Protections	P2	YES	YES	Implementation
2.1	Audit and Accountability Policy and Procedures	P1	YES	YES	Design-based
2.2	Auditable Events	P1	YES	YES	Design-based
2.3	Content of Audit Records	P1	YES	YES	Design-based

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL APPLICABILITY AND COMPLIANCE		
			Applicable	Control Addressed	SAIC Compliance Methodology
2.4	Audit Storage Capacity	P1	YES	YES	Architecture
2.5	Response to Audit Processing Failures	P1	YES	YES	Architecture
2.6	Audit Review, Analysis, and Reporting	P1	YES	YES	Implementation
2.7	Audit Reduction and Report Generation	P1	YES	YES	Implementation
2.8	Time Stamps	P1	YES	YES	Implementation
2.9	Protection of Audit Information	P1	YES	YES	Implementation
2.10	Non-repudiation	P1	YES	YES	Design-based
2.11	Audit Record Retention	P3	YES	YES	Design-based
2.12	Audit Generation	P1	YES	YES	Design-based
OP1.1	Configuration Management Policy and Procedures	P1	YES	YES	Process-based
OP1.2	Baseline Configuration	P1	YES	YES	Process-based
OP1.3	Configuration Change Control	P1	YES	YES	Process-based
OP1.4	Security Impact Analysis	P2	YES	YES	Process-based
OP1.5	Access Restrictions for Change	P1	YES	YES	Process-based
OP1.6	Configuration Settings	P1	YES	YES	Process-based
OP1.7	Least Functionality	P1	YES	YES	Process-based
OP1.8	Configuration Management Plan	P1	YES	YES	Process-based
OP2.1	Identification and Authentication Policy and Procedures	P1	YES	YES	Architecture
OP2.2	Identification and Authentication (Organizational Users)	P1	YES	YES	Architecture
OP2.3	Device Identification and Authentication	P1	YES	YES	Architecture
OP2.4	Identifier Management	P1	YES	YES	Architecture
OP2.5	Authenticator Management	P1	YES	YES	Architecture
OP2.6	Authenticator Feedback	P1	YES	YES	Implementation
OP2.7	Cryptographic Module Authentication	P1	YES	YES	Implementation
OP2.8	Identification and Authentication (Non-organizational Users)	P1	YES	YES	Implementation
OP3.1	Media Protection Policy and Procedures	P1	YES	NA	Policy-based
OP3.2	Media Access	P1	YES	NA	Policy-based

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL APPLICABILITY AND COMPLIANCE		
			Applicable	Control Addressed	SAIC Compliance Methodology
OP3.3	Media Marking	P1	YES	NA	Policy-based
OP3.4	Media Storage	P1	YES	NA	Policy-based
OP3.5	Media Transport	P1	YES	NA	Policy-based
OP3.5	Media Sanitization	P1	YES	NA	Policy-based
3.1	System and Communications Protection Policy and Procedures	P1	YES	YES	Implementation
3.2	Application Partitioning	P1	YES	YES	Implementation
3.3	Security Function Isolation	P1	YES	YES	Implementation
3.4	Denial of Service Protection	P1	YES	YES	Implementation
3.5	Resource Priority	P0	YES	YES	Design-based
3.6	Transmission Integrity	P1	YES	YES	Design-based
3.7	Transmission Confidentiality	P1	YES	YES	Design-based
3.8	Trusted Path	P0	YES	YES	Design-based
3.10	Cryptographic Key Establishment and Management	P1	YES	YES	Design-based
3.11	Use of Cryptography	P1	YES	YES	Implementation
3.12	Public Access Protections	P1	YES	YES	Architecture
3.13	Collaborative Computing Devices	P1	YES	YES	Architecture
3.14	Transmission of Security Attributes	P0	YES	YES	Architecture
3.15	Public Key Infrastructure Certificates	P1	YES	YES	Architecture
3.16	Mobile Code	P1	YES	YES	Architecture
3.17	Voice Over Internet Protocol	P1	YES	YES	Implementation
3.18	Secure Name /Address Resolution Service (Authoritative Source)	P1	YES	YES	Design-based
3.19	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	YES	YES	Design-based
3.20	Architecture and Provisioning for Name/Address Resolution Service	P1	YES	YES	Design-based
3.21	Session Authenticity	P1	YES	YES	Implementation
3.22	Fail in Known State	P1	YES	YES	Implementation
OP4.1	System and Information Integrity Policy and Procedures	P1	YES	YES	Implementation
OP4.2	Flaw Remediation	P1	YES	YES	Implementation
OP4.3	Malicious Code Protection	P1	YES	YES	Architecture
OP4.3	Information System Monitoring	P1	YES	YES	Design-based

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL APPLICABILITY AND COMPLIANCE		
			Applicable	Control Addressed	SAIC Compliance Methodology
Op4.5	Security Alerts, Advisories, and Directives	P1	YES	YES	Design-based
OP4.6	Security Functionality Verification	P1	YES	YES	Design-based
OP4.7	Software and Information Integrity	P1	YES	YES	Architecture
OP4.8	Spam Protection	P1	YES	YES	Implementation
OP4.9	Information Input Restrictions	P2	YES	YES	Implementation
OP 4.10	Information Input Validation	P1	YES	YES	Architecture
OP 4.11	Error Handling	P2	YES	YES	Architecture
O P4.12	Information Output Handling and Retention	P2	YES	YES	Architecture
5.1	Removal of Unnecessary Services and Programs	P1	YES	YES	Architecture
5.2	Host Intrusion Detection Systems	P2	YES	YES	Architecture
5.3	Change of File and Operating System	P1	YES	YES	Architecture
5.4	Hardware Configuration	---	YES	YES	Architecture
5.5	Installation of Operating System, Application and Third-party Software Updates	P3	YES	YES	Architecture

Table 1 - NEI 08-09 Rev. 06 Summary Assessment of SAIC Wi-Fi Solution

In Conclusion

Introduction of a secure wireless system into the nuclear power plant environment will allow significant operational and business opportunities. Nonetheless, there is a perceived security challenge and concern around the deployment of 802.11-based wireless systems. SAIC has demonstrated that a considered design, based on nuclear cybersecurity requirements can be implemented and provide the bandwidth, availability and resiliency for mission-critical applications. Furthermore, SAIC’s approach to an 802.11 wireless deployment has been based around 10 CFR 73.54 compliance and is demonstrated to provide an integrated, secure and compliant communications fabric for today’s and tomorrow’s nuclear power plant needs.

Success Starts Today

SAIC is a world leader in critical infrastructure security. With a vision for the future and an understanding of the nuclear industry, SAIC understands energy and helps our clients protect it.

To learn more contact us today.

Tel: 888.409.SAIC (7242)

Visit us online at www.saic.com