IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology

Kadam Shivam Rajendra[1], Dr. M. B. Jadhav[2], Prof. S. V. More[3], Dr. H. B. Jadhav[4]
Student, Department of Computer Engineering[1];
Guide, Department of Computer Engineering[2];
Co-Guide, Department of Computer Engineering[3]
Department of Computer Engineering[4]
Adsul Technical Campus, Chas, Ahilyanagar, India

Abstract: *Nuclear power plants rely on interconnected digital systems to monitor equipment, support plant operations, manage engineering activities, and protect people and the environment. These systems must be secured carefully because a cyber incident can affect operational reliability, safety functions, or the availability of essential services. This paper presents a technical assessment methodology for reviewing cybersecurity controls in a nuclear power plant. The approach considers governance, asset identification, network separation, access management, secure configuration, monitoring, incident response, backup and recovery, supplier security, and staff awareness. It proposes a structured process that begins with defining the assessment scope, collecting evidence, evaluating controls against recognised guidance, identifying gaps, and prioritising corrective actions according to risk and safety significance. The methodology is intended for authorised, non-disruptive assessment and emphasises coordination between cybersecurity specialists, instrumentation and control engineers, operations staff, and safety personnel. It does not recommend intrusive testing of live safety systems. A disciplined assessment can improve visibility of weaknesses, strengthen defence in depth, and support continuous improvement while preserving nuclear safety and operational continuity.*

Keywords: Nuclear Power Plant, Cybersecurity Controls, Technical Assessment, Industrial Control Systems, Defence in Depth, Risk Assessment, Operational Technology

I. INTRODUCTION

Nuclear power plants use digital instrumentation and control equipment, supervisory systems, engineering workstations, and supporting information technology. These technologies help operators observe plant conditions and manage complex processes. Their use also creates cybersecurity responsibilities: systems must remain reliable, access must be controlled, and changes must be managed without compromising safety.

Cybersecurity in a nuclear facility is different from security in an ordinary office network. Confidentiality remains important, but integrity, availability, predictable operation, and protection of safety-related functions are especially significant. Controls therefore need to be selected and assessed in a way that recognises plant design, safety classification, operating procedures, and regulatory requirements. A technical assessment is most useful when it combines documentary evidence with interviews, configuration reviews, and carefully approved observations.

II. PROBLEM STATEMENT

A nuclear facility may have a mixture of legacy equipment, specialised industrial protocols, restricted maintenance windows, and systems supplied by different vendors. These conditions can make it difficult to maintain a complete view of assets, verify that security controls are consistently applied, and determine whether corrective actions could

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, October 2026 Impact Factor: 8.2

affect safe operation. A control may exist on paper but be inconsistently implemented, poorly documented, or not tested at an appropriate interval.

The problem addressed in this paper is how to assess cybersecurity controls systematically, using evidence and risk-based priorities, while avoiding activities that could disrupt operational technology or safety-related systems.

III. OBJECTIVES

- To identify the main cybersecurity control areas relevant to nuclear plant information and operational technology.
- To outline a repeatable technical assessment process based on scope, evidence, control evaluation, and risk.
- To describe safe methods for identifying gaps without conducting unapproved or disruptive testing.
- To propose a practical way to rank findings and track corrective actions.
- To support coordination between cybersecurity, engineering, operations, and nuclear safety teams.

IV. REVIEW AND ASSESSMENT METHODOLOGY

This paper uses a structured, conceptual assessment methodology informed by established cybersecurity and industrial-control-system guidance. It is a review and framework proposal, not a report of an assessment performed at a named plant. Actual implementation must be tailored to the facility's licensing basis, safety analysis, regulatory obligations, system architecture, and approved procedures.

1. Define scope and authority. Document the systems, locations, networks, suppliers, and control families included. Obtain written authorisation and agree on restrictions, contacts, evidence handling, and escalation procedures before work begins.

2. Establish an asset and system baseline. Review approved inventories, system diagrams, data flows, system owners, criticality, dependencies, and maintenance arrangements. Reconcile records with authorised observations and record uncertainty rather than assuming the inventory is complete.

3. Collect assessment evidence. Use document review, staff interviews, approved configuration exports, access-control records, change logs, backup records, incident exercises, and observation of existing processes. Any technical probing should be explicitly authorised, risk-reviewed, and conducted only in a suitable test environment or under approved plant procedures.

4. Evaluate control design and operation. Compare documented requirements with available evidence. Determine whether each control is appropriately designed, implemented, maintained, and periodically reviewed. Record evidence, exceptions, and limitations in a traceable way.

5. Analyse risk and safety significance. Consider plausible threats, system exposure, potential consequences, existing safeguards, and dependencies. Coordinate with plant safety and engineering specialists so that cybersecurity recommendations do not undermine safety requirements.

6. Report and verify remediation. Describe each finding, its evidence, potential consequence, priority, accountable owner, and recommended action. Track corrective work to closure and verify completion using approved, non-disruptive evidence.

V. KEY CYBERSECURITY CONTROL AREAS

A. Governance and risk management. Maintain clear responsibilities, approved security policies, risk records, exception processes, and periodic management review. Cybersecurity decisions should be coordinated with nuclear safety and operational requirements.

B. Asset management and zoning. Maintain an accurate inventory and group systems according to function and criticality. Document approved communication paths and enforce separation between business networks, plant networks, and safety-related environments as required by the plant's design and applicable rules.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

C. Access control and authentication. Apply least privilege, unique user identities where technically feasible, controlled privileged access, secure remote-maintenance arrangements, and timely removal of access that is no longer required. Emergency and vendor access should be authorised, logged, and reviewed.

D. Secure configuration and change management. Use approved baselines, control removable media, review configuration changes, and test changes through established engineering processes. Updates and patches should be assessed for compatibility and safety before deployment.

E. Monitoring and event handling. Maintain suitable logs and alarms, protect log integrity, define escalation criteria, and ensure that monitoring activities do not interfere with time-sensitive or safety-related functions. Establish clear roles for investigating and reporting suspected incidents.

F. Backup, recovery, and continuity. Protect configuration files, software images, engineering data, and other essential records. Keep recovery procedures documented and periodically validate restoration arrangements in a controlled manner.

G. Supplier and maintenance security. Review supplier access, support channels, software provenance, service agreements, and maintenance procedures. Require security-relevant changes to be documented and coordinated with the plant's responsible personnel.

H. Personnel and physical protection. Provide role-specific awareness training, protect equipment rooms and engineering stations, control visitor access, and establish clear procedures for reporting unusual activity or suspected compromise.

VI. TECHNICAL ASSESSMENT MATRIX

A practical assessment matrix can help ensure that the review is consistent and auditable. For each control, the assessor should record the requirement, evidence reviewed, implementation status, identified gap, risk rationale, responsible owner, and follow-up date.

Control area	Example evidence	Assessment question	Expected output
Asset management	Approved inventory and diagrams	Are critical assets and dependencies documented?	Verified inventory gaps
Access control	Account lists, access reviews, procedures	Is access authorised and limited to business need?	Access-control findings
Network separation	Approved architecture and rule reviews	Are permitted connections documented and justified?	Segmentation observations
Change management	Change tickets and approval records	Are changes reviewed, tested, and traceable?	Process exceptions
Incident response	Response plan and exercise records	Are roles, escalation, and communication clear?	Readiness improvements
Recovery	Backup records and approved test results	Can essential configurations be restored safely?	Recovery action items

VII. FINDING PRIORITISATION AND REPORTING

Findings should be prioritised using a documented method that considers the importance of the affected system, credible threat scenarios, likelihood, potential consequences, existing compensating controls, and safety implications. A simple high/medium/low label can help communicate urgency, but the reasoning behind each rating should be recorded. A technical weakness should not be assigned a priority solely because it is easy to fix or because it resembles a finding in another environment.

The final report should distinguish confirmed weaknesses from incomplete evidence and improvement opportunities. Recommendations should identify an accountable owner, a target date, any required engineering or safety review, and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, October 2026 Impact Factor: 8.2

the evidence needed to confirm closure. Where immediate remediation is not feasible, formally approved compensating controls and review dates should be documented.

VIII. CHALLENGES AND SAFETY CONSIDERATIONS

Assessment teams may face incomplete documentation, legacy devices, limited maintenance windows, vendor restrictions, and uncertainty about how a change could affect a process. Active scanning, penetration testing, or configuration changes can create operational risk when applied to sensitive industrial systems. Such activities must never be performed on live or safety-related systems without explicit authorisation, a documented risk assessment, and the facility's approved safeguards. When safe validation is not possible, assessors should record the limitation and rely on approved alternative evidence.

The assessment must also protect sensitive plant information. Access to diagrams, configurations, logs, and findings should be restricted to authorised personnel, stored securely, and handled under the facility's information-classification rules.

IX. FUTURE SCOPE

Future work can develop a repeatable scoring model that links control maturity, evidence quality, risk, and safety significance. Further study could examine how asset inventories, passive monitoring, secure configuration management, supplier assurance, and incident-response exercises contribute to resilience over time. Any proposed automation should be evaluated for false alarms, operational impact, and suitability for the specific plant environment. Validation with authorised subject-matter experts and non-production test environments would help establish the framework's practicality.

X. CONCLUSION

Cybersecurity assessment in a nuclear power plant requires more than a checklist of technical settings. It requires a clear understanding of assets, system boundaries, operational dependencies, safety obligations, and the evidence that demonstrates whether controls work as intended. The methodology presented in this paper provides a structured sequence: define scope, establish a baseline, collect authorised evidence, evaluate controls, analyse risk, report findings, and verify remediation. Its central principle is that cybersecurity improvements must strengthen resilience without creating new operational or nuclear-safety risks. Consistent documentation, multidisciplinary review, and continuous follow-up can help a facility maintain stronger and more accountable cybersecurity controls.

ACKNOWLEDGMENT

The authors express their sincere gratitude to the guide and co-guide for their guidance, suggestions, and encouragement during the preparation of this review. The authors also acknowledge the Department of Computer Engineering and Adsul Technical Campus, Chas, Ahilyanagar, for providing an academic environment that supported this work.

REFERENCES

[1] International Atomic Energy Agency, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 17-T (Rev. 1), Vienna: IAEA, 2021.

[2] International Atomic Energy Agency, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, Vienna: IAEA, 2018.

[3] National Institute of Standards and Technology, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Revision 3, 2023.

[4] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Revision 5, 2020, updated 2023.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

[5] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13, Vienna: IAEA, 2011.
[6] U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, Washington, DC, 2010