Research and Application of Supply Chain Security Detection Technology for Imported DCS in Nuclear Power Plants

Junkai Wang, Haoyang Qing
Cybersecurity Technology Center, China Nuclear Power Operation Technology Co., Ltd., Wuhan, Hubei, China

Abstract: The security of imported distributed control systems (DCS) in nuclear power plants is difficult to establish: the core technology is closed, the security state of the equipment cannot be verified, and conventional detection rarely reaches the hardware or firmware layer. This paper develops a full-dimensional, multi-mode detection system to close that gap. The system combines a four-dimensional architecture covering hardware, software, firmware and operation and maintenance (O&M) tools with a trinity of white-box, black-box and gray-box techniques. It was then applied to the imported DCS systems of five operating plants of China National Nuclear Power (CNNP), where detection ran through the product itself, communication protocols, interaction links and O&M services. No abnormal electromagnetic emission was found in the hardware. Among 35 software sets, a large number of third-party components and known vulnerabilities were identified, concentrated in outdated component versions and vendor design defects, and no poisoned component or malicious backdoor was detected. The 15 O&M tool sets showed privilege-control weaknesses, chiefly unauthorized Internet access and unauthorized USB devices. The 2025 campaign confirms that the scheme is feasible and effective on operating units, and shows that the remaining risk lies less in deliberate tampering than in component ageing and O&M tool control.

Keywords: Nuclear Power Plant; Imported DCS; Supply Chain Security; Security Detection; White-Box Testing; Black-Box Testing; Gray-Box Testing

1. Introduction

With the deep integration of informatization and industrialization, the distributed control system (DCS) of a nuclear power plant has become the "nerve centre" for the safe and stable operation of the unit, and its security, reliability and availability are of vital importance [1].

Within China's nuclear power industry, the DCSs of the five CNNP operating plants are all rated as critical systems. Imported systems make up 77% of them, and the core technologies sit mainly with foreign vendors. Such heavy dependence on imports makes supply chain risk stand out. Hardware may be tampered with during procurement, transport or integration; a software package may carry a poisoned dependency or a hidden backdoor; firmware may be shipped with undisclosed interfaces and covert backdoors; and O&M tools are used every day with little security control. Each of these points can become the way in for an attacker, and each threatens the safe operation of the plant.

Industrial control systems around the world have suffered repeated supply chain incidents, and the threat is getting worse. In 2010 the Stuxnet virus reached Iran's nuclear facilities on USB flash drives and other removable media and severely damaged the centrifuge control system, the first case of a cyber weapon destroying physical equipment [2]. In 2015 BlackEnergy malware hit the Ukrainian power grid and caused a large-scale blackout, a second warning for the sector. In recent years supply chain attacks on critical information infrastructure in energy, electric power and nuclear power have become more covert, more destructive and harder to trace, and they are now a routine instrument of state-level cyber confrontation[3-5].

China's nuclear safety regulator has therefore given supply chain security high priority [6,7] and has called for stronger detection capability. CNNP has responded by bringing supply chain security into its overall cybersecurity framework, launching a dedicated detection programme, and looking for a detection technology system that suits the nuclear power industry.

Imported DCS supply chains in nuclear power

 Copyright @ STEMM Institute Press

suffer from black-box core technologies, covertly implanted backdoors, unknown vulnerabilities that cannot be controlled and incomplete coverage by conventional detection. This paper builds a full-element, multi-paradigm, full-chain detection technology system to deal with these problems. It works around the limits of conventional industrial control detection, inspects the whole domain, locates risk precisely and controls it in advance, and closes the technical gap in in-depth detection of imported DCS supply chains.

2. Status Quo and Objectives

2.1 Current Status of Security Detection

CNNP has established a security detection system covering both operating and pre-commissioning systems, and routinely carries out penetration testing, vulnerability scanning and baseline checks, which has played an important role in safeguarding nuclear power cybersecurity. However, obvious blind spots remain in supply chain security detection [8,9], mainly in the following aspects.

First, the detection scope is incomplete. Existing detection mainly targets deployed information systems and focuses on system configuration, network boundaries and application vulnerabilities, whereas no dedicated detection is performed on supply chain objects such as hardware devices (e.g., controllers), software packages, firmware and O&M tools. Risks introduced through the supply chain fall outside the scope of routine detection, which creates blind spots.

Second, the risk identification capability is insufficient. Existing means can hardly discover deep-seated risks introduced by the supply chain, such as hardware tampering, chip backdoors, software poisoning and firmware backdoors. Routine vulnerability scanning only finds known system vulnerabilities and cannot identify malicious implants at the supply chain level. Traditional detection is single-mode and mostly stays at the system and application layers, failing to reach the physical hardware layer and the firmware layer [10].

Third, the detection techniques are constrained. Imported DCS core technologies are closed and the source code is not available, so traditional white-box detection cannot be applied. In addition, nuclear power systems have extremely high availability requirements and must not be shut down for detection at will; many in-depth techniques cannot be implemented because they may affect system operation, so there is a conflict between detection depth and detection safety.

Fourth, standardized detection methods are lacking. Supply chain security detection involves hardware, software, firmware and tools, with diverse technical routes and high detection difficulty. The nuclear power industry has not yet formed standardized specifications and a methodological system for supply chain security detection [11], and understanding and practice vary from unit to unit.

Higher-level regulators share this concern and are already promoting supply chain security detection. Building a systematic detection technology system for the imported DCS supply chain is therefore both timely and useful to the industry.

2.2 Detection Objectives

The overall objective of nuclear power DCS supply chain security detection is to actively prevent and control supply chain security risks, close cybersecurity gaps and guarantee the safe and stable operation of nuclear power units by building a full-dimensional, multi-mode detection system. The specific objectives are as follows.

(1) Identify supply chain security risks comprehensively. Systematic security detection is carried out on the four object categories of hardware, software, firmware and O&M tools to obtain a complete picture of supply chain security and to identify all potential hazards and weak links, so that risks can be found and handled early.

(2) Close the technical gaps in supply chain detection. Conventional detection looks at one dimension at a time and treats the layers as separate, so this work instead sets up a three-dimensional architecture that reaches the physical layer, the program layer, the firmware layer and the tool layer. White-box, black-box and gray-box technologies are then combined to deal with core technologies that cannot be controlled, source code that is hard to obtain and vulnerabilities that are hard to expose [12].

(3) Verify the feasibility of the detection methods. Empirical research is conducted on the five operating plants to verify the feasibility, effectiveness and safety of the technical scheme in real scenarios, forming an implementable

Copyright @ STEMM Institute Press

detection plan and laying a practical foundation for subsequent full-scale promotion.

(4) Make supply chain security a routine practice. Experience from the dedicated detection is summarized, standardized detection procedures are compiled and a continuous detection mechanism is established, so that supply chain security detection changes from a one-off campaign into routine work and upgrades from passive response to active prevention and control.

(5) Create a demonstration effect for the industry. A replicable, promotable and sustainable supply chain cybersecurity governance model for the nuclear power industry is explored to provide a reference for other nuclear power plants and even other industrial control industries, thereby raising the overall supply chain security protection level of the industry.

3. Detection Content for Nuclear Power Supply Chain Security

Rather than looking at one dimension at a time as conventional detection does, this work treats hardware, software, firmware and O&M tools as a single architecture and screens the physical, program, firmware and tool layers one after another, so that hidden hazards can be located precisely (Figure 1).

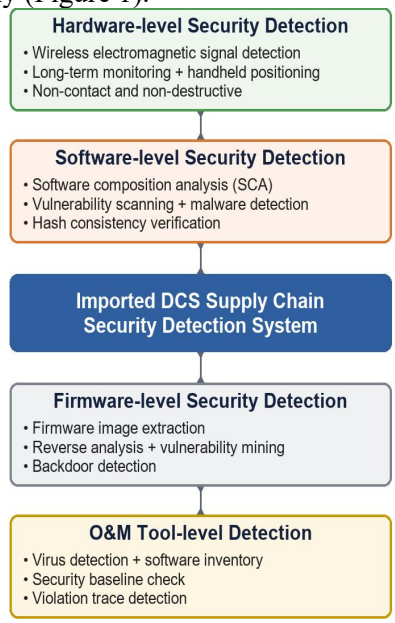

Figure 1. Four-Dimensional Detection Architecture for the Imported DCS Supply Chain in Nuclear Power Plants

3.1 Hardware-level Security Detection

3.1.1 Detection content and objectives

The core objective of hardware detection is to determine whether a wireless communication module has been maliciously implanted in the equipment, since such a module can establish a covert channel that breaks through physical isolation. Hardware tampering is the most covert and most harmful risk in the supply chain and cannot be detected by conventional protection at all. All detection is performed by non-contact, non-intrusive wireless electromagnetic signal probing, without disassembly or shutdown; it is fully non-destructive and can be applied directly to equipment in operation.

3.1.2 Detection techniques

Spectrum analysis is adopted: high-sensitivity receivers monitor the electromagnetic environment around the target, and the signal characteristics are analysed to determine whether an abnormal wireless emission source exists. Two types of equipment are used. Long-term monitoring devices are deployed in the equipment room for 24-hour continuous monitoring to capture intermittently emitted covert signals, covering common bands such as Wi-Fi, Bluetooth, mobile communication and the Internet of Things; handheld devices are used for close-range location of suspicious signals, being flexible, portable and well directional.

The signal analysis process is as follows: a background noise baseline is established, real-time data are compared with the baseline to identify abnormal signals, signal features such as frequency, bandwidth and modulation are analysed to determine the type, and the source is located step by step with a directional antenna. It should be noted that this method can only find implants that actively emit wireless signals; it cannot detect silent hardware Trojans or passive eavesdropping devices. A complex on-site electromagnetic environment may also drown weak signals, so detection should be scheduled in periods of low interference. Chip-level detection requires disassembly and is therefore destructive; it is only used for incoming acceptance and spare-parts inspection.

3.2 Software-level Security Detection

3.2.1 Detection content and objectives

Software is a core part of the DCS and an important carrier of supply chain risk. Software-level detection relies on software composition analysis (SCA) to identify poisoned components, malicious code and suspicious files and to establish integrity verification, so as to prevent software from being tampered with, replaced or maliciously implanted [12]. The detection covers:

 Copyright @ STEMM Institute Press

software package composition analysis to build a list of third-party components, component vulnerability scanning for known CVE vulnerabilities, component licence compliance checks for intellectual property risks, malicious code detection against viruses, Trojans and backdoors, and hash comparison to verify software integrity.

3.2.2 Detection techniques

SCA is the core technology of software supply chain detection: binary scanning and source code analysis are used to identify all third-party components and their versions, a software bill of materials (SBOM) is generated, and vulnerability matching and licence compliance analysis are then performed on this basis. Malicious code detection combines static and dynamic analysis: static analysis performs disassembly and signature scanning to identify suspicious behaviour, while dynamic analysis runs the software in a sandbox and monitors file, registry, network and process behaviour. Software consistency is verified by comparing SHA256 hashes with the vendor's official values, which prevents tampering and package substitution during transmission.

3.3 Firmware-level Security Detection

3.3.1 Detection content and objectives

Firmware is the low-level embedded software solidified in hardware; it runs with the highest privilege and is the deepest and most covert risk layer. Firmware detection performs in-depth inspection of the low-level firmware of key hardware such as controllers and network devices to find covert backdoors, undisclosed interfaces and native high-risk vulnerabilities [13]. The detection covers: firmware image extraction and integrity verification, reverse parsing of firmware structure and code logic, vulnerability mining for authentication bypass, command injection and buffer overflow, backdoor detection for hidden programs, debug interfaces and secret accounts, and configuration checks for default accounts and open ports.

3.3.2 Detection techniques

Firmware extraction is performed in different ways depending on the scenario. On-line extraction reads the firmware through an upgrade or debug interface while the device is running; it is non-destructive but gives limited completeness. Off-line extraction removes the flash chip and reads it with a programmer, obtaining a complete image but being destructive. Upgrade package analysis directly analyses the vendor-provided package, which must first be decrypted and unpacked.

Static firmware analysis includes: parsing the firmware file system format; disassembling and decompiling binary programs to analyse the code logic; extracting strings to find hard-coded passwords, keys, IP addresses and other sensitive information; and matching known vulnerabilities. Dynamic analysis includes: running the firmware in a QEMU emulation environment to observe start-up behaviour; fuzzing network interfaces and serial ports; and monitoring abnormal network, file and system-call behaviour.

At present, non-destructive firmware extraction is only applicable to some devices, and off-line extraction is not suitable for operating systems because of its destructive nature. Firmware detection is therefore currently used mainly for incoming acceptance of new equipment, spare-parts inspection, upgrade package inspection and off-line device analysis; the applicable scope will gradually expand as non-destructive extraction technology develops.

3.4 O&M Tool-level Security Detection

3.4.1 Detection content and objectives

O&M tools are the most easily overlooked but high-risk link, as they directly touch the production control system; well-known attacks such as Stuxnet were spread through O&M tools [2]. O&M tool detection establishes dedicated compliance specifications and performs privilege auditing, behaviour monitoring and malicious-feature screening on debugging tools, configuration software and remote maintenance programs. The detection covers: virus detection against malicious code, software inventory to identify unapproved software, security baseline checks of operating system configuration, and violation trace detection for unauthorized Internet access, USB use and wireless connections.

3.4.2 Detection techniques

Virus detection uses multi-engine cross-scanning to improve the detection rate, and suspicious files are analysed dynamically in a sandbox. The software inventory takes stock of all installed software and verifies its source, purpose and security, focusing on unauthorized software, software of unknown origin, vulnerable software and high-risk remote-control software.

Security baseline checks follow the requirements

Copyright @ STEMM Institute Press

of classified protection and verify operating system patch updates, account and password security, service port configuration, file sharing settings and audit log enablement. Violation trace detection uses system logs, the registry and network configuration to check browser history and network connections for unauthorized Internet access, USB usage records to identify unauthorized removable storage, and wireless configuration and connection history to reveal unauthorized wireless activity.

4. Key Detection Technologies

Source-code access differs from one imported DCS component to another, and so do the risk scenarios. White-box, black-box and gray-box detection are therefore combined into a single scheme and applied where each fits best, which raises the chance of finding risk (Table 1)[14]. Each mode has its own strengths and conditions of use; in practice they are selected and combined according to the characteristics of the object under test.

Table 1. Comparison of White-Box, Black-Box and Gray-Box Detection Technologies

Dimension	White-box	Black-box	Gray-box
Detection perspective	Internal code perspective	External attacker perspective	Semi-transparent integrated perspective
Source code requirement	Complete source code required	No source code required	Partial documentation and interfaces
Detection depth	Deepest; logic flaws can be found	Relatively shallow; only externally exploitable flaws	Moderate; balances depth and practicality
Detection coverage	Highest; covers all code paths	Relatively low; depends on test cases	Relatively high; strongly targeted
Applicable objects	Open-source components and self-developed modules	Fully closed imported core equipment	Commercial components with partial documentation
Main techniques	Code audit, SAST, static analysis	Penetration testing, DAST, dynamic scanning, fuzzing	Interface testing, semi-reverse architecture analysis
Advantages	Finds deep-seated problems with full coverage	Close to real attacks and no source code needed	High efficiency, balancing depth and practicality

4.1 White-Box Detection

4.1.1 Technical principles and applicable scenarios

White-box detection targets self-developed and open-source components whose source code is available and performs in-depth detection at the code-logic level. Since the detector can view all the source code and understand the internal structure, it is also called structural testing. Its advantages are great depth and high coverage, allowing deep logic vulnerabilities and design defects to be found; its limitation is the need for source code, which makes it inapplicable to fully closed imported core components. In nuclear power DCS detection, white-box is mainly used for open-source component analysis, self-developed module auditing, detection of third-party components whose source code is available, and code analysis after firmware reverse engineering.

4.1.2 Main techniques and practical application

White-box detection combines manual audit with automated tools. Source code security audit is performed manually by experienced engineers and focuses on input validation, authentication and authorization, key management, error handling, memory management and concurrency safety; it can find business-logic vulnerabilities that automated tools can hardly identify. Static application security testing (SAST) scans automatically for common code defects such as buffer overflow, injection, path traversal and resource leaks. Code quality and compliance assessment refers to CWE and industry secure coding standards to identify unsafe coding habits. Component dependency analysis builds a complete dependency graph and traces the impact scope of third-party component vulnerabilities.

The methods and experience of white-box detection can guide gray-box and black-box detection: white-box analysis of known open-source components reveals the vulnerability patterns of similar components, so that black-box test cases can be designed in a more targeted way and the detection efficiency improves.

4.2 Black-Box Detection

4.2.1 Technical principles and applicable scenarios

Black-box detection targets the fully closed imported core control units. Without knowing the internal implementation or obtaining the

 Copyright @ STEMM Institute Press

source code, it detects the system from an external perspective, treating it as a “black box” and finding problems only through input/output interaction. Its advantages are that no source code is required and that it applies to all kinds of closed systems; the results are closer to real attack scenarios and the problems found are more threatening in practice. Its limitations are limited coverage, difficulty in finding deep logic vulnerabilities and high requirements on the experience of the testers. Black-box is therefore the main detection mode for imported core control units, mining unknown risks from the outside without disrupting the operating logic.

4.2.2 Main techniques and practical application

Several techniques are used. External penetration testing simulates the thinking of a real attacker and works from the network and application layers, following the standard process of information gathering, vulnerability probing, verification, privilege escalation and lateral movement to evaluate how well the system resists attack. Dynamic vulnerability scanning (DAST) sends probe packets to identify port services, operating system fingerprints, known vulnerabilities, weak passwords and configuration defects, and serves as a rapid, broad screen. Business function exception verification constructs over-long input, special characters, malformed packets and boundary values to test fault tolerance and security. Protocol security testing fuzzes industrial control and proprietary protocols with large numbers of malformed packets; it matters most for industrial protocols that lack authentication and encryption.

Safety deserves special attention in practice: detection is preferentially carried out in a test environment or on spare equipment, the detection intensity is controlled to avoid affecting system operation, and an emergency plan is prepared so that operation stops and recovers immediately in case of abnormality. Black-box detection can find externally exploitable vulnerabilities, insecure default configurations, weak passwords and protocol security problems, and is of great value for assessing the overall security posture of a system.

4.3 Gray-Box Detection

4.3.1 Technical principles and applicable scenarios

Gray-box detection combines the static analysis capability of white-box with the dynamic verification capability of black-box. Adopting a semi-transparent mode, it has internal information such as interface documents, architecture design and part of the code while still performing dynamic testing from the outside, balancing detection depth and practical relevance and greatly improving the detection rate of covert risks. Compared with pure black-box, gray-box is better targeted, more efficient and has better coverage; compared with pure white-box, it is closer to the real operating scenario and can find runtime vulnerabilities that static analysis cannot. Gray-box applies to scenarios where part of the technical documentation is available but the complete source code is not, which is the most common case in imported DCS component detection.

4.3.2 Main techniques and practical application

The main gray-box techniques include: interface-level security testing, which tests each interface according to the interface documentation for input validation, privilege bypass and exception handling; because parameter definitions and function descriptions are known, test cases are better targeted and the efficiency and coverage are better than in blind black-box testing. Code-assisted dynamic testing focuses on high-risk paths with the help of partial code analysis: for example, if reverse analysis suggests that a module may suffer from buffer overflow, fuzzing test cases are designed accordingly, combining white-box analysis with black-box dynamic verification. Architecture-level security analysis examines macro design defects such as trust boundaries, privilege architecture, data flows and network isolation, which often have a greater impact than a single vulnerability. Semi-reverse-assisted detection obtains internal information such as function lists, string tables and key algorithms through reverse engineering to support more targeted test design, significantly improving the result when source code is unavailable.

The three modes are not used in isolation but combined flexibly according to the object: open-source components and self-developed modules are handled mainly by white-box, fully closed imported core units by black-box, and commercial components with partial documentation by gray-box, while important objects are cross-verified with all three. The trinity system solves the pain points of uncontrollable core technologies, difficult source code acquisition and hard-to-find vulnerabilities

Copyright @ STEMM Institute Press

in imported DCS, and achieves full coverage of components with different degrees of openness.

5. Detection Results

The 2025 dedicated supply chain security programme for imported DCS systems at CNNP provided the setting for the field work. Using the four-dimensional architecture and the combined detection scheme described above, detection was completed for the imported DCS systems of the five operating plants of Qinshan, Jiangsu, Fuqing, Hainan and Sanmen. It covered the whole business chain of product entities, communication protocols, interaction links and O&M services, and it brought out many deep-seated and covert risks that conventional means could not detect. The data supported equipment rectification, policy hardening and supply chain access control, and the technical system was validated under field conditions.

5.1 Hardware Security Detection Results

5.1.1 Implementation

Hardware-level detection centred on the core objective of determining whether a wireless external-connection module had been maliciously implanted, and wireless electromagnetic signal detection was carried out. The detection consists of two stages.

Stage 1: on-site screening. Handheld devices covering 70 MHz to 6 GHz were used for close-range detection of the equipment in the room; the directional antenna and the high-sensitivity location function were used for approach localisation of target signals, quickly screening for obvious abnormal wireless signals. Handheld detection is flexible and efficient and allows the equipment to be checked one by one.

Stage 2: long-term monitoring. On the basis of stage 1, long-term monitoring devices covering 9 kHz to 10 GHz were used to record the ambient background for comparison, so as to detect sporadically or periodically emitted signals. Long-term monitoring captures intermittent and periodic covert signals that handheld detection may miss when they are emitted only briefly.

5.1.2 Results

In the 2025 dedicated detection of imported DCS, each of the five operating plants was subjected to 12 to 24 hours of comparative electromagnetic detection in the powered-off and powered-on states, covering key hardware such as controllers, servers, network devices and security devices.

The results show that no obvious malicious electromagnetic emission was found from any tested hardware device in the five plants and that no maliciously implanted wireless external-connection module was detected. Background comparison between the powered-off and powered-on states revealed no abnormal additional signal generated during operation, and long-term monitoring did not capture any sporadically or periodically emitted covert signal. This indicates that the DCS hardware of the five operating CNNP plants had not been implanted with malicious wireless modules either at the factory or during deployment, and that hardware-level supply chain security is generally sound. It also verifies the feasibility and effectiveness of the two-stage wireless electromagnetic signal detection technique on nuclear power sites; being fully non-destructive and free of impact on system operation, the method is suitable for wide application in operating nuclear power plants.

5.2 Software Security Detection Results

5.2.1 Implementation

Software-level detection was carried out around two core objectives: first, software composition analysis to identify poisoned components, malicious code or suspicious files; second, integrity verification to check the consistency of software version, code and configuration and to prevent tampering, replacement and implantation of malicious logic. An example of software component composition detection is shown in Figure 2.



```
{
    "spdxVersion": "SPDX-2.3",
    "dataLicense": "CC0-1.0",
    "SPDXID": "SPDXRef-DOCUMENT",
    "name": "/code",
    "documentNamespace": "https://anchore.com/Moresec%20SCA/dir/code-ffa66bf6-93d0-44e8-8616-e66e2bc75eb6",
    "creationInfo": {
        "licenseListVersion": "3.25",
        "creators": [
            "Organization: Moresec, Inc",
            "Tool: Moresec SCA-1.9.0"
        ],
        "created": "2025-07-29T09:57:58Z"
    },
    "packages": [
        {
            "name": "bzip2",
            "SPDXID": "SPDXRef-Package-c-bzip2-f89516186fe9841d",
            "versionInfo": "1.0.5",
            "supplier": "NOASSERTION",
            "downloadLocation": "NOASSERTION",
            "filesAnalyzed": false,
            "sourceInfo": "acquired package info from the following paths: /CCS9.5-K0177BP.zip_/CCS9.5-K0177BP/3rd_party/MKSToolkit/oe/Toolkit64x.msi_/SOURCEDIR/Program Fil
            "licenseConcluded": "NOASSERTION",
            "licenseDeclared": "NOASSERTION",
            "copyrightText": "NOASSERTION",
            "externalRefs": [
                {
                    "referenceCategory": "PACKAGE-MANAGER",
                    "referenceType": "purl",
                    "referenceLocator": "pkg:generic/bzip2/1.0.5"
                }
            ]
        },
        {
```


Figure 2. Example of Software Component Composition Detection

 Copyright @ STEMM Institute Press

Detection combined SCA, vulnerability scanning, licence compliance checking, static and dynamic malicious code detection and SHA256 hash consistency comparison to inspect software packages comprehensively, including DCS system software, antivirus software, backup software and configuration software.

5.2.2 Results

In the 2025 dedicated detection, 35 software sets were subjected to supply chain security detection, covering the core system software of the five plants. The main problems found are concentrated in the following aspects.

(1) Outdated third-party components are prominent. A large number of third-party open-source components are obsolete, have not followed upstream security updates and have accumulated many known vulnerabilities. Because DCS version upgrades have long cycles and high verification requirements, lagging component updates are widespread.

(2) Vulnerabilities were introduced by earlier vendor design. Some vulnerabilities originate from design defects and coding problems in earlier vendor versions; they are native security risks and need to be fixed by the vendor in later versions.

(3) No malicious poisoning or backdoor program was found. No virus, Trojan, backdoor or other malicious code was detected in any tested software, no poisoned component was found and no malicious external connection was observed. Software consistency comparison showed that all core software packages matched the official vendor hash values, with no trace of third-party tampering.

Overall, the software itself is secure and controllable and shows no trace of malicious supply chain attack, but the cumulative vulnerability risk caused by outdated components cannot be ignored. A routine mechanism for tracking and responding to component vulnerabilities should be established, with disposal graded by risk level.

5.3 O&M Tool Security Detection Results

5.3.1 Implementation

O&M tool detection focused on compliance, including usage trace detection, O&M software detection and security baseline detection, concentrating on whether violations and hazards exist in the daily use of O&M tools so as to eliminate supply chain risks introduced through the O&M chain.

5.3.2 Results

In the 2025 dedicated detection, 15 O&M tool sets, mainly O&M laptops, were tested, covering the main O&M equipment used by on-site personnel in the five plants. The problems found are concentrated in privilege control, mainly as follows.

(1) Unauthorized use of external devices. Many unauthorized USB device connection records, including personal flash drives and portable hard disks, were found on some O&M laptops. Connecting removable storage to O&M tools without approval is a high-risk route for viruses to enter the production network.

(2) Unauthorized Internet access. Traces of Internet access were found on some O&M tools, and browser history showed that external websites had been visited. For dedicated O&M tools in a physically isolated environment, any Internet connection is a serious violation that may bring external network risks into the production control area.

(3) Non-compliant security configuration. On some O&M tools the antivirus signature database had not been updated for a long time, real-time protection was disabled, operating system patches were not updated in time, and account passwords and service configurations did not meet the security baseline, so the overall protection capability was insufficient.

The problems found provide clear technical support and a rectification direction for strengthening the control of personnel O&M tools in nuclear power plants. As the bridge between the external environment and the production system, O&M tools are a key node of supply chain security management and urgently require stronger control at both the institutional and the technical level.

5.4 Comprehensive Analysis of Detection Results

Combining the hardware, software and O&M tool results from the five operating plants, the distribution of the supply chain problems detected in the five plants is shown in Figure 3, from which the following conclusions can be drawn.

First, the security posture of the imported DCS entities is generally controllable. No malicious wireless implant was found in hardware and no trace of poisoning, backdoor or tampering was found in software, which shows that the DCS equipment of the five plants is secure at the

Copyright @ STEMM Institute Press

factory and delivery stages and that there is no obvious sign of a targeted malicious supply chain attack.

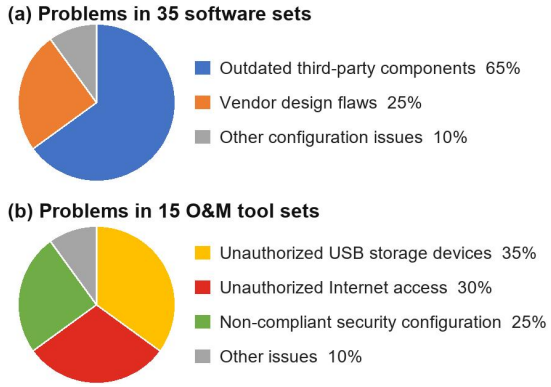

Figure 3. Distribution of Supply Chain Problems Detected in the Five Power Plants

Second, the cumulative vulnerability risk of third-party components cannot be ignored. The 35 software sets commonly suffer from outdated components and numerous vulnerabilities, which will persist for a long time because DCS upgrade cycles are long. Although physical isolation reduces the risk of remote exploitation, these vulnerabilities could be exploited once an attacker breaks through the boundary by other means, so graded vulnerability management and continuous tracking are required.

Third, O&M tool control is currently the biggest weakness. The 15 O&M tools commonly show management problems such as unauthorized Internet access, mixed use of USB devices and non-compliant security configuration. These are low-level management errors but carry extremely high risk and are the most easily breached link in supply chain security. Famous industrial control attacks such as Stuxnet used O&M tools and removable media as a springboard, so this issue must be taken seriously and rectified first.

Fourth, the detection technology system has been verified as effective. The dedicated detection in the five plants successfully applied the four-dimensional architecture and the trinity technology, comprehensively identified the supply chain security risk baseline of imported DCS in CNNP, verified the feasibility, effectiveness and on-site applicability of the methods, and laid a solid practical foundation for routine detection and full-scale promotion.

6. Conclusion

6.1 Conclusions

Imported DCS supply chain security is a problem shared across the nuclear power industry. This paper has met it with a four-dimensional system of hardware, software, firmware and O&M tools and with the combination of white-box, black-box and gray-box detection, and has tested the approach on the five CNNP operating plants. The main conclusions are as follows.

(1) The four-dimensional architecture achieves full coverage of supply chain security. Breaking the limitation of a single detection dimension, three-dimensional detection is carried out at the hardware physical layer, the software program layer, the firmware layer and the O&M tool layer, which comprehensively identifies risks in every link of the supply chain and closes the gap of traditional detection that only addresses the system layer.

(2) The trinity technology effectively solves the detection problem of imported DCS. In view of closed core technologies and difficult source code acquisition, the three modes are flexibly combined and the optimal strategy is selected according to the openness of each object, achieving full coverage of components with different degrees of openness and greatly improving the detection rate of covert risks.

(3) The dedicated detection in the five plants verified the feasibility and effectiveness of the system. Supply chain security detection was completed for 35 software sets, 15 O&M tool sets and all key hardware in the five operating plants of Qinshan, Jiangsu, Fuqing, Hainan and Sanmen, giving a complete picture of DCS supply chain security and accurate data support for rectification and hardening. The detection caused no impact on system operation, proving that the scheme is applicable to operating nuclear power plants.

(4) O&M tool control is currently the biggest weakness in supply chain security. The detection found management problems such as unauthorized Internet access, mixed USB use and enabled wireless functions on O&M tools. These problems carry high risk and are easy to rectify, and should be the priority breakthrough in near-term supply chain security governance.

6.2 Outlook

Based on the successful experience of the five plants, the full-process work specifications will be further optimized and the technical standards for imported DCS detection in the nuclear power industry will be unified. The detection mode will

 Copyright @ STEMM Institute Press

then be promoted to other plants in an orderly manner, extending supply chain security detection from a "single-point pilot" to "full-domain coverage" and upgrading it from "passive response" to "active prevention and control".

Technically, future work will strengthen research on non-destructive firmware extraction to expand the applicable scope of firmware detection, deepen the application of artificial intelligence in supply chain security detection to improve the efficiency and accuracy of vulnerability discovery, and explore a supply chain threat intelligence sharing mechanism to enhance the threat awareness of the whole industry.

Through continuous technical innovation and management improvement, a replicable, promotable and sustainable supply chain cybersecurity governance model for the nuclear power industry will gradually take shape, comprehensively raising the supply chain security protection level of the industry and providing a solid guarantee for the safe and stable operation of nuclear power units.

References

[1] Ayodeji A, Di Buono A, Pierce I, et al. Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system. Nuclear Engineering and Design, 2024, 424: 113277.

[2] Huang Min, et al. Analysis of the Stuxnet attack and its lessons. Information Security and Communications Privacy, 2011(6): 58-61.

[3] Wu Shizhong, et al. Research on supply chain security assurance of critical information infrastructure. Bulletin of Chinese Academy of Sciences, 2019, 34(10): 1141-1149.

[4] Humayed A, Lin J, Li F, et al. Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 2017, 4(6): 1802-1831.

[5] Cho H S, Woo T H. Cyber security in nuclear industry–Analytic study from the terror incident in nuclear power plants (NPPs). Annals of Nuclear Energy, 2017, 99: 47-53.

[6] Topping C, Dwyer A, Michalec O, et al. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security, 2021, 108: 102324.

[7] Park J K, Suh Y S, Park C. Implementation of cyber security for safety systems of nuclear facilities. Progress in Nuclear Energy, 2016, 88: 88-94.

[8] Nocera S, Romano S, Di Penta M, et al. On the adoption of software bill of materials in open-source software projects. Journal of Systems and Software, 2025, 230: 112540.

[9] Williams L, Benedetti G, Hamer S, et al. Research directions in software supply chain security. ACM Transactions on Software Engineering and Methodology, 2025, 34(5): 1-38.

[10] Wang Yingjian, Zhang Tao. Supply chain security risks and protection of industrial control systems. Journal of Information Security Research, 2020, 6(8): 701-708.

[11] Kampourakis V, Kavallieratos G, Gkioulos V, et al. Cracks in the chain: A technical analysis of real-life supply chain security incidents. Computers & Security, 2025, 159: 104673.

[12] Liu Xinran, et al. Research on software supply chain security detection technology. Chinese Journal of Computers, 2021, 44(5): 965-985.

[13] Chen Xingyuan, et al. Research progress on firmware security of industrial control devices. Journal of Software, 2022, 33(3): 1070-1092.

[14] Zhou Shijie, et al. Comparative study of white-box and black-box testing technologies. Application Research of Computers, 2019, 36(S1): 321-324.

Copyright @ STEMM Institute Press