Implementation of cyber security for computerized operator support system of nuclear facilities

Wei Zheng , Lei Mao

Shanghai Nuclear Engineering Research and Design Institute, China (E-mail: zhengwei2@snerdi.com.cn)

Abstract: Computerized operator support systems are deployed within Plant Monitor and Control Level, include computer-based procedure system, alarm management system and nuclear performance calculation system, and provide decision support for operators during all plant conditions, including normal condition and accident condition. Cyber security attack will adversely affect the reliability, availability, confidentiality and integrity of computerized operator support system, leading to deny access to system, services or data, and adversely impact the operation of systems, networks, and associated equipment. So computerized operator support system should be adequately protected against cyber attacks.

The paper will describe a software security development Life Cycle method while enhancing verification and validation (V&V) during development and incorporating the cyber security considerations into the software development process from design phase to test phase. The life cycle of cyber security plan and activities of implementation of cyber security for computerized operator support system of nuclear facilities, including concepts phase, requirements analysis phase, design phase, implementation phase and test phase are explained in detail. Requirements development and V&V process concerning cyber security methods including account management, access control, session management, authorization and password management, log and audit, communication security, hardware configuration, software and service and fault tolerance mechanism are implemented in computerized operator support system. Cyber security test for computerized operator support system will also be described in this paper, including black box testing, penetration testing and vulnerability scan and etc. It also explains experiences resolving security vulnerabilities of the system and summarizes considerations and experiences in the development process.

Keyword: cyber security, computerized operator support system

1 Introduction

Computerized operator support systems (COSS) are deployed within plant monitor and control level, include computer-based procedure system, alarm management system and nuclear performance calculation system, and provide decision support for operators during all plant conditions, including normal condition and accident condition. Our work is to incorporate cyber security into development of COSS system, treating COSS system as target of evaluation (TOE). In this project, we use the protect profile (PP) method described in GB/T 18336 to define the system boundary, threat, security hypothesis, security target in the application software used in nuclear power plant environment. GB/T 18336 equally adopts ISO/IEC 15408. We check the input and output of the application software of the whole life cycle from the perspective of cyber security. Then for each stage of the life cycle of the application software, we select the security components for the input and output of the software, and adopt these components into the development of the software.

2 I&C System Security Design

I&C system security requirement should be established from the following:

- Regulation , standards & guides
- Security risk analysis
- Security function and I&C function requirement
- Security controls, including account management, access control, session management, authentication strategy, log and audit, communication security, hardware configuration, software and services, heartbeat and fault tolerance mechanisms and etc.

The main security design principle is:

1) System Harden: harden network, host, application, data reinforcement, using enhanced access control, user authentication and identification, authorization mechanism, data and communication integrity protection.

2) System isolation and separation: through technical means for physical and logical isolation and separation according to division of security Zones and Levels.

3) Audit and monitoring: All the network traffic monitoring, control system within the control system command-level audit and monitoring, deployment of host intrusion detection system.

4) Cyber security features shall not adversely impact Safety features and the required performance (including response time), effectiveness, reliability or operation of functions important to safety supported by I&C systems.

The security design includes two parts, one is I&C system related functional security design, the other is general security design. I&C related functional security design focus on function design within I&C system itself.

3 I&C System Security Design and Development Process

The life cycle of cyber security plan and activities of implementation of cyber security for computerized operator support system of nuclear facilities includes concepts phase, requirements analysis phase, design phase, implementation phase and test phase. During each phase, security design and development activity should be lunched with software design and development simultaneously. As I&C software should conduct its fundamental V&V activity while the security function should also conduct its V&V activity as indicated in Fig 1.

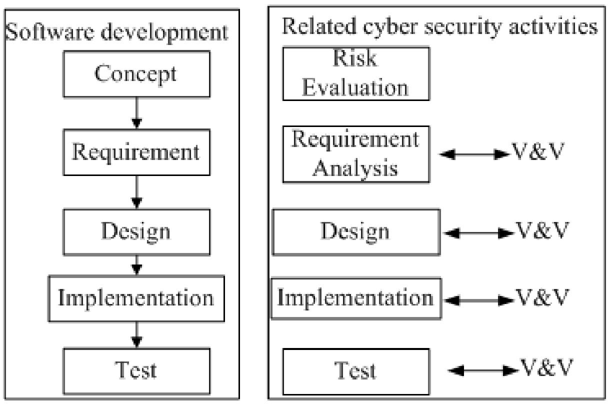

Fig 1 Security Development Activity

4 System architecture of system

Alarm Management System provides computerized alarm information for the operation staffs to monitor the plant under normal, abnormal, and emergency operating conditions, when parameters deviate from specified limits or components are in a fault condition.

Computer-based procedure system is based on software technologies and driven by real-time operation data of a power plant. It provides information in a graphic way such as process diagrams and logic diagrams which are more easily to be understood. With this system the performance of operators will be greatly improved and their stress can be relieved when they monitor power plant or execute procedures in an emergency condition.

Nuclear Performance Calculation System is used to support the operator monitoring and operating the nuclear power plant. The system has redundant servers and a set of nuclear application programs run independently on each server. The Nuclear Application Program System software can call nuclear application programs to fulfill specific calculating function. All the calculation done by nuclear application programs are based on the data from real-time network of nuclear power plant.

All these application software use the same system architecture, which is C/S architecture. The servers are redundantly configured and hot standby. Since the three systems have the same architecture, we use alarm management system as an example.

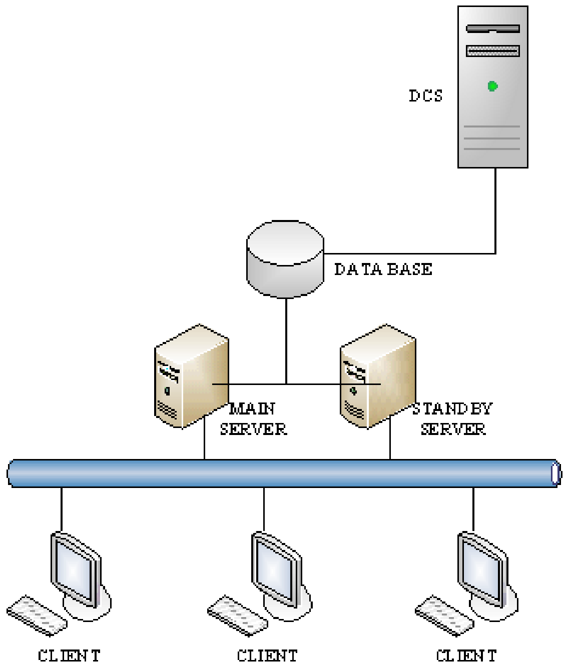

Fig 2 System Architecture

The calculation logic is running on the main server and the hot standby server, and provides data access services to the client terminals. The main server and the hot standby server backup each other. When the main server fails, the backup server automatically provides data access service, replacing the main server to become the new primary server.

Data base provides the database to read and write and interfaces with the field instrument and control system.

5 Security Environments and Security Objective

Cyber security attack will adversely affect the reliability, availability, confidentiality and integrity of computerized operator support system, leading to deny access to system, services or data, and adversely impact the operation of systems, networks, and associated equipment. So computerized operator support system should be adequately protected against cyber attacks. To achieve this goal, the system shall:

- Be able to resist logical manipulation or modification attacks.
- Be able to resist attacks to obtain security information by analyzing changes such as information flow.
- Enter the specified initial state after starting or restarting. This will prevent the system from entering an undefined state.
- Be able to resist repeated attacks of insertion of defective data.
- Provide functions such as one-time authentication mechanisms to protect against replay attacks.
- Be operated in an authorized or controlled manner to prevent the system device from being enabled before the software security mechanism is started.
- Provide access control rules based on the user or user group, and access control rules are consistent with data access in the organizational security policy.
- Protect unauthorized entities from repeated searches for data and files.
- Be able to provide security audit mechanism to record selected audit events in order to detect potential attack behavior and generate the necessary security response.
- Provide a means of controlling or restricting the use of a particular command at a particular stage.
- Have the ability to safely manage passwords.
- Prevent data from being intercepted during data transmission.
- Be able to prevent attackers from entering the system and stealing data and doing disruptive operations through the network.
- Have no-repudiation mechanism.
- Have the function of resisting information and malicious retransmission.
- Have the function of eliminating residual information.

6 Security components selection for software function

Based on the logic and architecture of the software, we select security components for the software. These components are defined in GB/T 18336. The life cycle model of the software is defined as initialization, running (including input, calculation and output) and exit. Then we select security components from five dimensions that are user, file, network, process and Operation

System, for each part of the life cycle of the software.

- Initialization: user open the software and the software initialize itself, so the user is not involved in the initialization security. The TSF self test (FPT_TST) is selected for file dimension to ensure the integrality and validity of the file. Resource allocation (FRU_RSA), Limitation on multiple concurrent sessions (FTA_MCS) and Session locking and termination (FTA_SSL) are selected for network dimension to ensure the communication establishment is safe.
- Running-input: Import from outside of the TOE (FDP_ITC), Non-repudiation of receipt (FCO_NRR), and Replay detection (FPT_RPL) are selected for use input and file input. Import from outside of the TOE (FDP_ITC), User attribute definition (FIA_ATD), Authentication failures (FIA_AFL), Replay detection (FPT_RPL), Non-repudiation of receipt (FCO_NRR), Inter-TSF trusted channel (FTP_ITC), TOE session establishment (FTA_TSE) and TOE access history (FTA_TAH) are selected for network input, so the communication can be authenticated and the communication is non-repudiation.
- Running-calculation: Access control policy (FDP_ACC), Access control functions (FDP_ACF), Internal TOE transfer (FDP_ITT) are selected for all five dimensions.
- Running-output: Non-repudiation of origin (FCO_NRO) is selected for file/network/process/OS, and Availability of exported TSF data (FPT_ITA), Confidentiality of exported TSF data (FPT_ITC) and Integrity of exported TSF data (FPT_ITI) are selected for network to ensure the availability, confidentiality and integrity of the output data, and ensure the non-repudiation of origin.
- Exit: Residual information protection (FDP_RIP) is selected.

After these security components are selected for each part of the software life cycle, we implement these components requirements during the development of the software. Verification and validation (V&V) is also implemented during development and incorporating the cyber security considerations into the software test phase.

7 Security components selection for security function

General security control method is also considered during the development of the software, including identification and authorization, access control, fault tolerance, audit and role management. The recommendation control methods in RG 5.71[3] are also considered.

- Identification and authorization: user must take identification action (for example, login interface) before operation. Authentication mechanism can detect and prevent the use of forged or copy the identification of the data. During authentication, only limited feedback is available for user.
- Access control: scope of the access is defined. The access scope includes three parts that is user, data and operation. Ensure that all users, data and operations within the application system are covered by the information flow control policy. Behavior of each control policy must be verified, and allow or prohibit actions according to the control policy.
- Fault tolerance: the system can deal with fault handling and failure handling in the event of errors in all processes. There should be a detailed design of the exception capture mechanism, that is, when an application has an exception, a known exception should be caught and an unknown exception should be dropped. Specifies the exception list for the system to continue running and the handling function when an exception occurs.
- Audit: when auditing events are detected, the application system automatically implements the associated audit function to record the events. System should provide comprehensive query filtering capabilities for all audits. Audit data should be protected from unauthorized modification or deletion. Export of the audit data should be implemented.

- Role management: define security related roles and the functions that role should have. Give limited and necessary authorization functions for each role based on the task they perform.

8 Security architecture design

According to the security design principal described in section 2, modified system architecture is provided as follows:

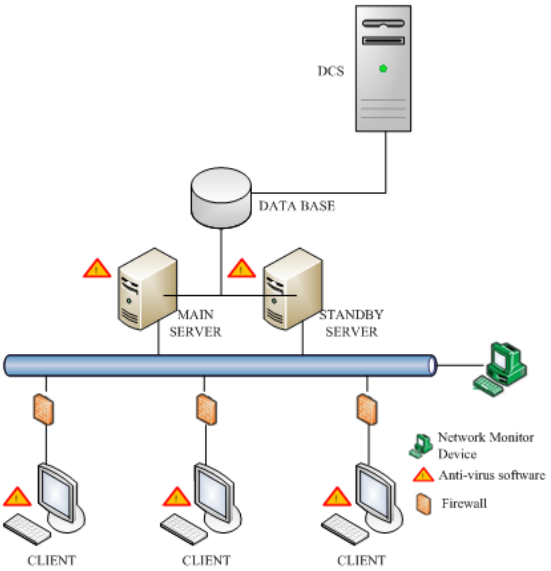

Fig 3 Cyber Security Architecture

9 Security Test

The goal of security test is to mitigate potential vulnerabilities in the field of system confidentiality, integrity and availability.

The security test can be done in two ways. One is standard function test including black box and white box test while the others are attack patterns, vulnerability scan and abuse fuzzy test.

10 Summaries

In this paper, we incorporate cyber security into development of computerized operator support systems (COSS), and implement the security components and general security controls for the whole life cycle of the software used in nuclear power plant environment.

References

[1] IAEA NSS 17, “Computer Security at Nuclear Facilities”.

[2] IEC 62645, “Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems”.

[3] Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”

[4] IEC 62443, “ Industry Network and System Security”