Journal of Radiation and Nuclear Applications
An International Journal

http://dx.doi.org/10.18576/jrna/050102

An Approach to Basic Requirements for Maintaining the Software Applications used in Nuclear Facilities

Mazhar Mahmoud Hefnawi

Siting and Environmental Dept., Egyptian Nuclear & Radiological Regulatory Authority, (ENRRA), Cairo, Egypt.

Received: 2 Nov. 2019, Revised: 4 Dec. 2019, Accepted: 11 Dec. 2019.
Published online: 1 Jan. 2020.

Abstract: In nowadays the software applications of computers systems in nuclear facilities have expanded. These applications became very important and very necessary for operating the existing systems and upgrading current systems. Although the characteristics of software applications used with nuclear facilities have a high degree of similarity with software applications used in industrial control systems, specifications are different with both of them in terms of architecture and function. Therefore in order to increase the degree of safety in nuclear facilities and sites of nuclear facilities, basic requirements for maintaining the software applications must be determined and implemented. This paper introduces an approach in describing and implementing these requirements in all stages of lifecycle process in computer system used in nuclear facilities. These stages are stage while designing the computer system, stage before installing software applications, stage while operating software applications, and stage after shutting down software applications. These requirements include security risk assessments of software applications, the activities and considerations necessary for assessments during the system design phase or component design and equipment supply phase are presented in the following 6 steps: 1) System Identification, 2) Asset and Impact Analysis, 3)Threat Analysis, 4) Vulnerability Analysis, 5) Security Control Design, and 6) Penetration test. The results from this approach to a nuclear facilities protection system are described.

Keywords: Software Maintenance, Software Lifecycle Process, Nuclear Facilities, Technical Security Controls, Software for Nuclear Facilities.

1 Introduction

Instrumentation and control (I&C) systems, which are important for the safety and performance of nuclear Facilities, have been digitalized for the purpose of the maintenance and precise operation. The control systems perform data acquisition, control actuation, and information indication based on software. Existing operator actions, such as the monitoring of hardwired panels and the manual control of hand switches, have been replaced with computer-based visualization and automatic actuation. It also supports faster responses in plant operation and reduces the human resources and costs. However, there are a few disadvantages induced by computer-based systems. One of the most severe disadvantages is the security vulnerability of Ethernet-based communication and a rise in software threats.

The main differences between nuclear specific software and general purpose software are the safety functions which include failure that may cause a significant economic loss and physical damage to the public. There are many safety regulations and standards in the nuclear industry which guide a design and development processes of safety functions such as 10 CFR 55, IEEE Std. 2791971, IEEE Std. 603-1991, IEEE Std. 7-4.3.2-2003, U.S. Nuclear Regulatory Commission (USNRC) revised Regulatory Guide (RG) 1.152-2011 [1], and USNRC issued RG.5.71-2010 [2]. But, these regulatory guidelines focus on a main part of safety function which is secure development activity and system security activity, i.e., systematic maintenance of safety systems are not specific enough.

There are many studies on developing the reliability and safety of critical software [3-5] and addressing the security problem [6, 8] in the software development process. Currently, the most important part of the software development process for the achievement of safety system security is security engineering, which describes how to integrate security activities into a software lifecycle model. Recently, Chou [9] proposed a regulatory-based development process that describes the specific

*Corresponding author e-mail: mmaazz_2222@yahoo.co.uk

development stages for the software security of safety systems. It is a well-structured process based on RG.1.152-2006 [9].A new development process that integrates both RG.5.71-2010 and RG. 1.152 -2011 is required.

This paper is organized as follows: the most famous accidents which were caused by software applications in nuclear power plants in next Section. Section 3 introduces the relevant nuclear regulations and regulatory guidelines of software security. Finally, introducing an approach to basic requirements for maintaining the software applications used in nuclear facilities.

2 The most famous accidents which were caused by software applications in nuclear power plants

On January 25, 2003, the Davis-Besse nuclear power plant in Oak Harbour, Ohio, was infected with the MS SQL 'Slammer' worm. This lead to traffic overload on the site network which caused both of Safety Parameter Display System (SPDS), and the plant process computer inaccessible for over than 6 hours. The reason for this accident is a malicious code via a secondary pathway into the control network. Fortunately the plant was off-line at the time the attack occurred, so there was no financial loss or safety risk as a result [10].

On August 19, 2006, Unit three at the Browns Ferry nuclear plant near Athens,
Alabama, critical reactor components were disrupted and disabled. Therefore unit three was manually shutdown. Both of programmable logic controller (PLC) for the condensate demineralizer and the recirculation pumps depend on variable frequency drives (VFD) to modulate motor speed were prone to failure in high traffic environments. High traffic network of the Browns Ferry's control network reached of the level of traffic more than the PLC and VFD controllers could handle. This level of high traffic network may be caused by the PLC malfunctioned and flooded the Ethernet with spurious traffic. By disabling the VFD controllers and testing conducted after the incident were inconclusive showed that the failure of these controllers was not the result of a cyber-attack. However, it demonstrates the effect that one component can have on an entire process control system network and every device on that network [10].

Unexpected results can be resulted from seemingly simple actions. On March 7, 2008, Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, automatically shut down after applying a software update to a single computer on the plant's business network. The software application on this computer was used to collect diagnostic data from the process control network; the update was designed to synchronize data on all available networks. After rebooting the computer, the synchronization program reset the data on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown. This kind of mistake showed shows how malicious hackers could make simple changes to a business network that end up affecting a nuclear reactor. It also shows that plant operators in this case did not fully understand the dependencies between network devices [10].

3 Nuclear Regulations of software applications

In 2010, U. S. Nuclear Regulatory Commission (NRC) issued new guidelines, RG. 5.712010, which shows the technical methods and security activities that should be taken for the operation and maintenance of a nuclear plant.

These guidelines do not provide specific lifecycle-based processes but they prompt the security controls to be planned, designed, and implemented during the safety system development phase before the site installation of the systems for avoiding any later treatment of the systems for security or safety may cause unpredicted defects in the systems or may be implemented with less effective security or safety measures. Therefore RG.5.712010 is divided into two sections [9,10].

Section 1: Before the site installation of the systems which includes:-

a. Establishment of security and safety team.

b. Establishment of training plan.

c. Establishment of defense strategy.

Section 2: After the site installation of the systems which includes

a. Continuous monitoring.

b. Periodic analysis of monitored data.

c. Security program review.

U S NRC issued a revision of RG.1.152-2011 in 2011.This regulation put criteria for software applications used in nuclear power plants for safety purpose. This regulation includes five aspects which are as following

1. Concept: - Which include

   a. Creating a secure environment

   b. Determining all possible weak points

   c. Creating a facility to enable remote access

2. Requirements: - which include

   a. Defining the requirements for all security functions.

   b. Verification and Validation (V&V) during the requirements and high level design processes.

   c. Creating a secure development process

3. Design: - which include

a. Covering all items which is included in concept and requirements

b. The design should enable a developing as required from future needs.

4. Implementation: - implementing and testing all security procedures.

5. Test: verify and test all security functions which cover all the system.

4 An Approach to basic requirements for maintaining the software applications used in nuclear facilities

A proposed Approach to basic requirements for maintaining the software applications used in nuclear facilities uses a mixing of RG. 5.712010 And RG.1.152-2011 to meet these requirements. These activates for maintaining the software applications used in nuclear facilities are as following [1, 2, 9]:-
1) Establishment of a will trained security team. This security team responsible for:-

a) Creating a secure environment during design phase which defines the requirements for all security functions and supports all suitable tools for every requirement.
b) Performing a security assessment to identify potential vulnerabilities based on the architecture design.
c) - Implementing and testing all security procedures.

2) Establishment of a will trained safety team. This safety team responsible for:-

a) Defining in details all processes which are done by any software component.
b) Install, operate, shutdown, and uninstall any software component in a safety manner.
c) Performing a backup of all necessary data in automated way.
d) Supporting a Quality Assurance (QA) to verify the correctness and completeness of the overall software lifecycle.
e) Preparing standard development procedures to prevent the introduction of unwanted or unnecessary functions and codes during the development process. That is, the main outputs at this stage are software functional requirements and security-related procedures [11, 12].

3) Creating a periodic testing and monitoring, a review of software logs, and real-time monitoring. An incident response and recovery plan for responding to digital system security incidents should be developed by both of security team and safety team during normal operation.

4) If any change is happened according to future need, the security team may changes in the operating environment due to a potential threat induced by this change. In addition, the safety team in this case must evaluate the impact of the safety systems for software changes in the operating environment.

5) During operation phase. Both of security team and safety team review the all activities to ensure that vulnerabilities are not introduced into the plant environment.

6) During the acceptance test and installation phase, the security team and safety team should conduct hardware configuration, integration, qualification and installation tests to verify the software security features. Conducting security tests or drills is useful to identify the actual security capability of the system. The safety team should be in charge of the verification and validation of the overall software [13- 15].

5 Conclusion

As nuclear safety systems have managed and adopted by computer systems via software applications. Maintaining these software applications becomes an important issue for the nuclear industry. However, there is still no clear development process regarding maintenance which includes safety activities and security activities for the nuclear software applications.
This paper proposes integrated basic requirements for maintaining the software applications used in Nuclear Facilities. that combines the security activities of the major regulatory guidelines, RG. 1.152-2011 and RG. 5.71-2010.
The contributions from this work are as follows:
• Introducing a comprehensive development process based on both the secure development regulations and the security regulations for nuclear safety software. It can be used to determine the security requirements early during the software development process.
• Emphasizing software design and engineering for meeting nuclear regulation requirements. For example, remote access to the software design of safety systems should not be allowed.
• following the instructions of basic requirements for maintaining the software applications introduced in this paper are useful for software developers and licensees to better understand the regulatory requirements. Basic requirements for maintaining the software applications which are introduced in this work can lead to safer operation of digital safety systems and in any case it cannot be omitted due to the current licensing requirements of regulatory bodies. Compared with previous software development methods, it enhances the safety of system by maintaining the system integrity more safely against various cyber threats. For example, the defense-in-depth architecture can make it hard to directly attack the safety system and the security controls of the security boundaries and safety systems can prevent the attacks, and the security monitoring and assessment can minimize vulnerabilities introduced into the plant environment.

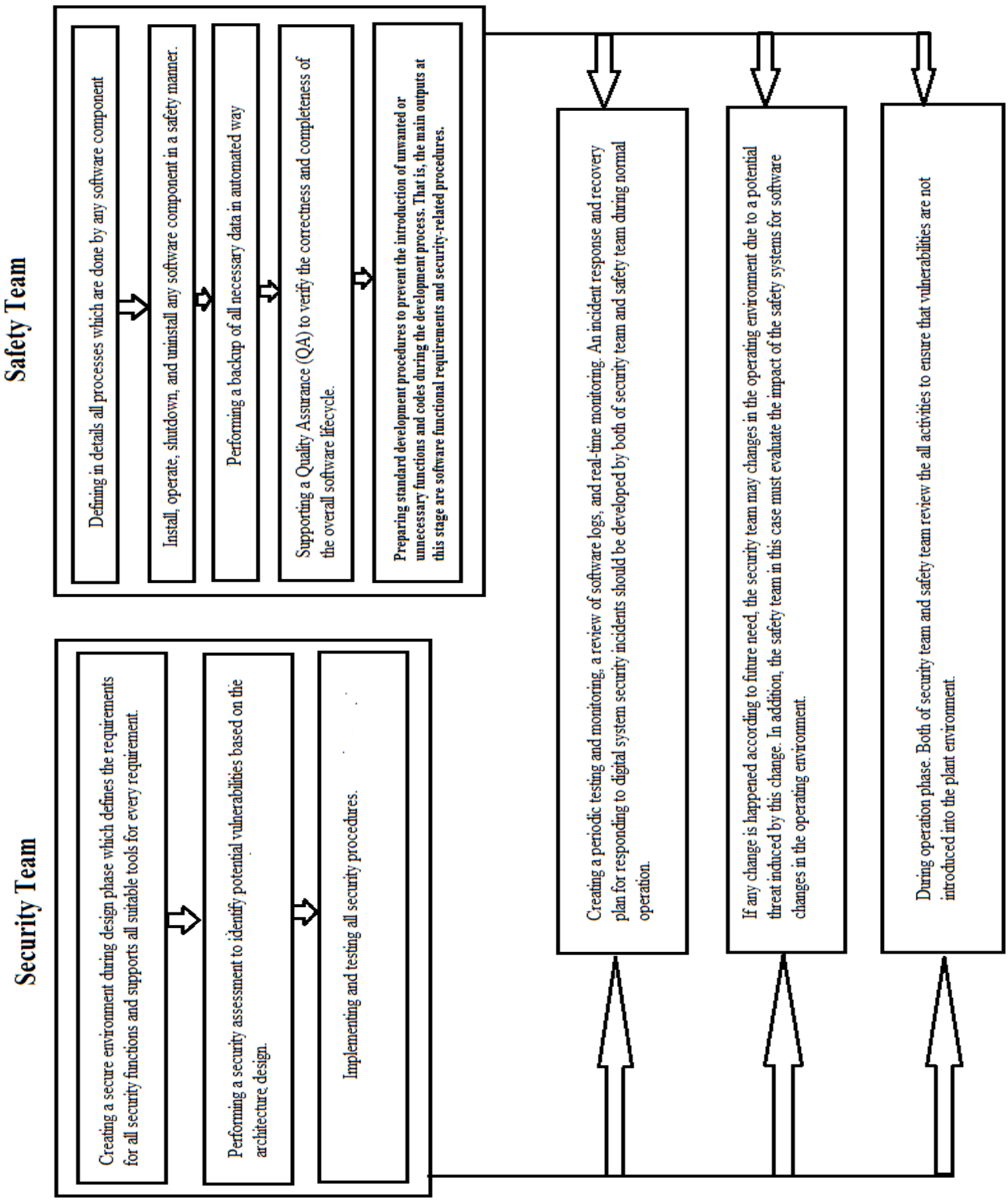

Figure 1. Summarizes all activates for maintaining the software applications used in nuclear facilities

References

[1] NUCLEAR REGULATORY COMMISSION. Criteria for Use of Computers in Safety Systems of Nuclear Power Plants. Regulatory Guide 1.152 Revision 3.US, 2011.

[2] NUCLEAR REGULATORY COMMISSION. Cyber Security Programs for Nuclear Facilities. Regulatory Guide 5.71.US , 2010.

[3] B. Ghahramani, Software reliability analysis: a systems development model, Computers & Industrial Engineering ., 45, 295-305, 2003.

[4] W. Weber, H. Tondok and M. Bachmayer, ,Enhancing software safety by fault trees: experiences from an application to flight critical software, Reliability Engineering & System Safety ., 89, 57-70, 2005.

[5] A. Ramadan and M. Hefnawi, An Approach to a New Network Security Architecture of Nuclear and Research Facilities ,Software Engineering., 7(1),10-15, 2019, doi: 10.11648/j.se.20190701.12.

[6] IH. Chou, Secure Software Configuration Management Processes for nuclear safety software development environment, Annals of Nuclear Energy., 38, 2174-2179, 2011.

[7] J. Lahtinen, J. Valkonen, K. Björkman, J. Frits, I. Niemelä and K. Heljanko, Model checking of safety-critical softwarei n the nuclear engineering domain, Reliability Engineering& System Safety., 105,104-113, 2012.

[8] W. Salem, M. Hefnawi, Management of the Processes for Evaluating External Human Induced Events Using Operating Systems Concept, Journal of Operating Systems Development & Trends.,5(2),24-29, 2018.

[9] IH. Chou and C-F. Fan, Regulatory-based development processes for software security in nuclear safety systems, Progress in Nuclear Energy., 52, 395-402, 2010.

[10] NUCLEAR REGULATORY COMMISSION. Criteria for Use of Computers in Safety Systems of Nuclear Power Plants. Regulatory Guide 1.152 Revision 2.US, 2006.

[11] B.Kesler, The vulnerability of nuclear facilities to cyber attack, Strategic Insights., 10(1),15-25,2011.

[12] I. Zakaria and H. Refai, A. Mashhour, Proposed Framework for Security Risk Assessment, Journal of Information Security., 2, 85-90, 2011.

[13] I. Fovino, L. Guidi, M Masera, A. Stefanini, Cyber security assessment of a power plant, Electric Power Systems Research., 81, 518-526, 2011.

[14] J. Song , J. Lee, C. Lee, K. Kwon, and D. Lee, A cyber security risk assessment for the design of I&C systems in nuclear power plants, Nuclear Engineering and Technology,, 44(8), 919-928,2012.

[15] D.Mark, MD. John and S. Justin, The art of software security assessment, Addison-Wesley, USA, 179-209, 2007.