Contribution ID: **615** Type: **Paper**

Cyber Security Risk Analysis and Technical Defense Architecture Research of ICS in Nuclear Power Plant Construction Stage

Monday 10 February 2020 12:15 (15 minutes)

Abstract: The stable operation of the ICS (ICS) directly affect the safety of nuclear power plants and cyber security has become an important factor affecting nuclear safety. With the continuous development of the digitalization and networking of modern industry, the cyber security of ICS in nuclear power plants is facing unprecedented challenges. Therefore, it is necessary to take cyber security into consideration from the construction stage in nuclear power plants. From the perspective of the business owner, we analyze the cyber security risks faced by ICS during the construction phase and propose the technical defense architecture for newly built and being built nuclear power plants respectively combining the related international standards and guidelines. Further, we propose to build ICS cyber security test platform to verify the feasibility of the defense architecture.

1. Introduction

It was considered in the past that the ICS of nuclear power plants was relatively safe because it was isolated with outsider world and used specialized hardware and software to run proprietary protocols. However, with the higher degree of industrial digitalization and networking, the Windows platform and industrial Ethernet based on IEEE802.3 have been widely used in ICS. The ICS become open and face unprecedented security threats. From the " Stuxnet" incident in Iran to the recent power blackout in Venezuela, the cyber security of ICS in power plants is facing more and more challenges. Cyber security has become an essential part of production safety and the key ICS of a nuclear power plant will directly cause reactor shutdown events, which will lead to nuclear safety issues. Therefore, it is necessary to take cybersecurity into consideration from the construction stage, analyze the cyber security risks during the construction phase, and build targeted technical protection solutions for under construction and new nuclear power plants.

2. Related standards

2.1 RG 5.71

2.2 IAEA NSS

2.3 IEC 62443

2.4 IEC 62645

2.5 IEC 63096

3. Cyber security risk analysis of ICS in the construction stage of nuclear power plant

3.1 requirements for cyber security in nuclear power project management

This chapter introduces the main works of construction stage in nuclear power plants and analyzes the cyber security requirements in "information and document management" which is one of the seven fields of nuclear power project management.

3.2 Critical Digital Assets Identification

According to the requirements of RG 5.71, this chapter addresses how to identify the critical digital assets of ICS in nuclear power plant.

3.3 external threats analysis of critical ICS

This chapter analyzes the external threats to the critical digital assets identified in 3.2(critical ICS,) in the construction phase of nuclear power plants.

3.4 vulnerability analysis of critical ICS

This chapter analyzes the possible vulnerability of critical digital assets identified in 3.2 during the nuclear power plant construction phase.

4. Technical defense architecture research

Because of the long construction cycle of nuclear power plant, it will take huge cost to change the defense architecture after it was confirmed in the design phase. Therefore, this chapter studies the cyber security defense architecture of ICS in newly built and being built nuclear power plants respectively.

4.1 Technical defense architecture for critical ICS in newly built nuclear power plants

In this chapter, we propose the technical defense architecture based on trusted computing for critical ICS in newly built plants. We analyze the difference between trusted computing and traditional defense method, and explore how to use trusted computing technology to construct a defense architecture with active immune

function.
4.2 Technical defense architecture for critical ICS in nuclear power plants being built
Because of the insufficient design of cyber security, we must take the cost and schedule into consideration as for the defense architecture for plants being built. We propose a semi-active defense architecture based on network isolation, protocol analysis for ICS and intrusion detection technology, which can detect and block threats in time.
4.3 Cyber security test platform for ICS in nuclear power plants
ICS have high requirement for high availability and some ICS with real-time control function, such as the protection system, will directly cause reactor shutdown events. Therefore, the cyber security technical defense architecture of critical ICS must be fully tested and verified. In this chapter we introduce the digital twin technology, and discuss the feasibility and advantages of constructing the cyber security test platform for ICS based on digital twin technology.
5. Conclusion
6. References

Gender

Female

State

China

Author: Mrs GUO, Yun

Co-authors: Mrs LOU, Xinxin; Mrs BAJRAMOVIC, Edita; Mr WAEDT, Karl

Presenter: Mrs GUO, Yun

Session Classification: Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

Track Classification: CC: Information and computer security considerations for nuclear security