Contribution ID: **146** Type: **Poster**

Strengthen Computer Security on Radiation Detection Equipment for Nuclear Security

Radiation detection equipment is very important as its purposes used for nuclear security need in the prevention intentional and unintentional unauthorized acts involving nuclear and radioactive material. And computer security is a particular aspect of information security that is concerned with computer based systems, networks and digital systems. Normally people focus attention on the specific conditions affecting computer security at nuclear facilities follow NSS-17. But IAEA documents about computer security on radiation detection equipment is little while technical and functional specification of equipment, which may directly relate to the detection results, is well-known as NSS-1.

Since each procedure of relative detection data is expected to be digital in current digital age, hidden dangers of juggled digital data will affect the accuracy of equipment performance and mislead monitoring results of nuclear radiation detection. All fields of security (including personnel, physical, information and computer) interact and complement each other to establish an equipment's security. A failure in any of the field could impact the other. Computer security on radiation detection equipment is a cross-cutting field that has interactions with all on-site practical security factors.

In this paper two aspects, where one is technical control and the other is management, are primary considered to be strengthened to effectively protect information security of control computer. The content includes extending performances related with computer security to technical and functional specification of equipment. This may protect digital data on computer (including embedded singlechip), communication system and connected cable from cyber-attack.

From the aspect of technical measures, the primary means of preventing and mitigating the consequences of security breaches is "defence in depth". Since a radiation detection equipment is an integrated system with detecting, transmitting, processing and storing functions, the digitization of data from detector is start of control flow. Then according the composition of the equipment, flow direction of digital data need to be controlled. Also access control ways such as encryption of files, identification of authorization, remote access restrictions and necessary authentication can be adopted. Communication protection can be enhanced from digital feature composition of hardware and protocols of software. It is better if a tamper-proof mechanism for data files can be established.

From the aspect of management control, a security policy of regular inspection should be established. Its context cover life cycle management of a radiation detection equipment, including data of continuous monitoring, records of software operating, adjusting, controlling and processing, logs of different operators. When there is exceptional case, it may means the equipment has the risk of out of control. If possible, assessment tool can be used to conduct vulnerability assessment tests such as vulnerability scanning and Trojan penetration on the system of equipment.

State

China

Gender

Male

Primary authors: Prof. LI, Yong; Prof. WANG, Guobao; Prof. WANG, Qiang

Presenter: Prof. LI, Yong

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