Contribution ID: **413** Type: **Poster**

# The considerations and the counter measures of different computer security systems that is used in a research reactor

Computers play a vital role in all aspects during the life time of the research reactor including management, and the safe and secure operation. As the technology advance, the use of computer-based systems at nuclear facilities continues to increase, including the use of many non-standard information technology systems in terms of architecture, configuration, or performance requirements. It is very important that all such systems are properly secured against malicious computer-based actions. At the same time, computer networks and computer-based systems have become a larger target for malicious acts. This includes not only desktop computers, mainframe systems, servers, network devices, but also lower level components such as embedded systems and PLCs (programmable logic controllers).

The requirements of Computer security in nuclear facilities may differ from requirements in other fields. In business applications, only a limited range of requirements is involved; but for nuclear facilities, an entirely different set of considerations need to be taken into account, for example, those affecting e-commerce, banking or even military applications.

According to the IAEA NSS 17, Computer security objectives are commonly defined as protecting the confidentiality, integrity and availability attributes of electronic data or computer systems and processes. By identifying and protecting these attributes in data or systems that can have an adverse impact on the safety and security functions in nuclear facilities, the security objectives can be met.

The security of computer systems [NSS 17] is based on a graded approach, where security measures are applied proportional to the potential consequences of an attack. Categorizing computer systems into zones, and levels is the practical implementation of the graded approach. In any nuclear facility, the plant equipments are classified into two main groups, systems that are important to safety and systems that are not important to safety.

This paper will define the different security levels for the nuclear facility, and list the different considerations for all the computer systems that are used within a research reactor during the reactor lifetime phases according to their security level. For example the reactor protection system (security level 1) needs protective measures that are different from that measures which is needed for office automation systems (security level 5). These protective measures are based on the potential impact on the facility, and to make sure that the different computer systems provide safe, reliable, and deterministic behavior. Also this paper will introduce a survey of existing risks, vulnerabilities, and Consequences of a cyber attack at nuclear facilities.

## State

Egypt

## Gender

Male

**Primary author:** Mr HABASH, Mohamed (Egypt Second Research Reactor - Egyptian Atomic Energy Authority)

**Presenter:** Mr HABASH, Mohamed (Egypt Second Research Reactor - Egyptian Atomic Energy Authority)

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