Contribution ID: **203** Type: **Poster**

Software Updating Effect on Safety and Security of Research Reactors

Computer-based systems have gradually replaced many of the mechanical and pneumatic control systems in research reactors and nuclear power plants. These systems have hardware and software components. Software updates are necessary due to the fact that at the point of software commissioning they may contain a number of undetected faults and cybersecurity bugs. These faults and bugs can lead to critical failures and cybersecurity vulnerabilities. Consequently, software update is crucial to resolve and mitigate these issues. Research reactors digital systems are subjected to changes, modification, and upgrading due to their extended usage and multi activities. But, gained experience from software updating highlighted the fact that sometimes software updating processes jeopardize the safety and vulnerable the cybersecurity of nuclear facility to cybersecurity attacks. There are some issues that should be addressed in more details when updating these digital systems. One important issue is the software updating planning where there are many factors that should be analyzed before starting the updating process. Another issue is the security of the updating process lifecycle to avoid the existence of new vulnerabilities which could be discovered and re-exploited by attackers. So, cybersecurity measures is an requirement to ensure that software update will improve system functionality which may be safety function or cybersecurity function or fix cybersecurity bugs which could be exploited by attackers. This paper discusses and analyzes the effect of software updating on safety and cybersecurity of research reactors from different point of views. Also, this paper proposes requirements and guidelines to avoid such drawbacks on safety and cybersecurity.

Software updates are necessary due to the fact that at the point of software commissioning they may contain a number of undetected faults, which can lead to critical failures of the fault tolerate critical systems. Assuring Safety and security are primarily based on keeping software updated for the critical system and are the first safeguard against cybersecurity incidents and events. Generally, a software update is a software file that contains fixes for problems. The updated process could be proposed by the software's users or developers based on detected bugs, or cybersecurity risks. In nuclear field updated process could be required by regulatory body in response to learned lessons from events and accidents happened in similar systems of nuclear plants. Also, it could be new capabilities added to the original software. Installing an update fixes the code and prevents the bugs from affecting the plant computers. Software update is needed for many reasons, such as:

- Updates protect against new-detected security risks.
- They introduce new features in safety critical software.
- Software updates can improve combability between system equipment and between updated system and other systems.
- They extend the useable life of your equipment by allowing the maximum productivity from your equipment.
- Updates fix bugs in the software and improve functionality.

Although, there is an air-gap between the public internet and nuclear plant digital systems, these systems are still subjected to cyber-attacks. Air-gap is very easy to be breached with nothing more than a flash drive. It noted that the destructive Stuxnet computer virus infected Iran's nuclear facilities via this route. Also, human factor cannot be neglected in such cybersecurity incidents. Both human and flash derive represent the bridge for malwares and viruses to cross the air-gap and attack digital systems in research reactors and nuclear power plants. This could be happened during software update and maintenance whatever unintentionally or intentionally by disgruntled employees, cyber criminals, state-sponsored hackers and terrorists. Two incidents related to software updated will discussed, one is concerned with safety and the other is concerned with cyber security attacks.

This paper proposes a framework for the software updating planning process of digital critical system (see Fig. 1) to avoid re-appearing cyber security vulnerabilities and errors and faults.

As cybersecurity regulations is still new topic to many regulatory bodies, this paper proposes a set of requirements to regulate the software updating process for safety and safety related digital systems:

1- Cybersecurity measures shall be in place through the lifecycle of software updating process.

2- Software updating shall be formally documented and approved in consistent with the software configuration management plan.

3- Software updating for safety and safety related systems shall be approved by regulatory body.

4- The software updating on safety and cybersecurity shall be implemented on simulator before its implementation on real systems.

5- The documentation shall include the reason for the change, identification of the affected software, and the

impact of the change on the system including the hazards and risks analysis.
6- Additionally, the documentation shall include an updating plan for implementing the change in the system along with updating documentation including the hazards and risk analyses and additional software life cycle activities such as V&V.

State

Egypt

Gender

Male

Primary author: SALLAM, Hany (Computer Engineering)

Presenter: SALLAM, Hany (Computer Engineering)

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