

Cyber Security of Structure, System and Components Important to Safety

Cyber-attacks on industrial installations including nuclear power plants (NPPs) are a significant issue/ Digital control systems are now at the core of industrial installations, playing a critical role in safety in many sectors, including Structures, systems, and components (SSCs) important to safety in the nuclear sector. The function of SSCs important to safety is to bring into a safe state when a fault occurs in the nuclear installations. Moreover, in the event of SSCs important to safety failure, the SSCs important to safety is expected to force the state of nuclear installation into its fail-safe condition. The architecture of SSCs important to safety need to be selected properly to enable safety function as designed.

Along with the various gains in flexibility and efficiency of digital systems, this evolution comes with new risks of digital attacks, exploiting a growing connectivity and reflecting recent changes in the threat landscape. Intrusion by an external or internal malicious attacker could violate the confidentiality, integrity, or availability of data. Even if the computers were not connected to the internet or air-gapped from the internet, attackers can devise scheme to infiltrate companies to get inside the system. The SSCs important to safety of the nuclear installations are potentially vulnerable to cyber attacks. After the appearance of Stuxnet, the safety assurance against cyber-attacks has been a serious problem for nuclear installations. With this vulnerability, it is proposed that SSC security risk assessment. Safety analysis procedure usually doesn't include cyber security aspects. Safety and security are highly related concepts. They share the same goal—protecting the SSCs important to safety from failing. Both deal with the protection of public and environment from radiological consequences, and both do this by avoiding, detecting, and responding to incidents that can cause such consequences.

Cybersecurity has become more critical these days and to address such concern, risk assessment for the security of the SSCs important to safety is proposed to be included in the design and evaluation, as part of the enhancement process. An important step to proactively include and align cybersecurity risk assessment against hacking, malware or any cyber threats in the design and evaluation of the SSCs important to safety is proposed. Hazards and threats that can cause or enable such incidents to occur are identified and the associated risks are analyzed in order to ensure that these risks are mitigated to acceptable levels. In this case hardware architecture of SSCs important to safety should fulfill new requirements.

Gender

Male

State

Indonesia

Author: Mr JUSUF, Farid Noor (BAPETEN)

Presenter: Mr JUSUF, Farid Noor (BAPETEN)

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