THESEUS
PROFESSIONAL SERVICES
1829 Reisterstown Rd., Ste. 350, Baltimore, MD 21208
410.857.0023 | theseuspro.com

Cyber Security in the Nuclear Industry

Brief Course Description:

The course describes Cyber Security principles, and the application of Cyber Security for the nuclear industry. The course includes a roadmap to the applicable guidance for those designing and building software or buying software for nuclear applications. Cyber Security for procuring firmware-based digital devices as well as upgrading and maintaining existing firmware-based devices is discussed. Also included is guidance for procuring and evaluating digital devices that are replacing older, analog based electronic components for use in nuclear facilities. Beginning with the Cyber Security Rule at 10 CFR 73.54, the course introduces the learner to the documentation from EPRI, NRC, ASME, NIST and NEI. Use of the Cyber Security Domains (Asset Security, Communications and Network Security, Security Engineering, etc) in the context of the regulatory environment will be discussed. Topics covered include the Secure Development Environment, the Secure Operating Environment, Critical Digital Assets (CDA), and Secure Software/System Development Lifecycles. The course includes a discussion of ICS environments regarding industrial Cyber Security as well as more traditional IT based Cyber Security in IT environments. The course briefly introduces Cyber Security requirements for developing and using nuclear codes and software development methods.

Who Should Attend:

I&C engineers, design engineers, software engineers, risk managers, QA specialists, V&V specialists, procurement engineers, technicians, vendor auditors, receipt inspectors, NSSS suppliers, and vendors who wish to sell into nuclear environments.