Contribution ID: **249** Type: **Oral**

cybersecurity matter for remote access of SMR

Remote operation is a crucial aspect of the business model for some Small Modular Reactor (SMR) operators, encompassing Physical Protection Systems (PPS) and I&C systems. However, the reliance on digital technologies raises viability concerns related to the growing potential for cyber attacks.

This paper presents a study on cyber security issues of remote communication and identifies technical vulnerabilities related to potential unmanned teleoperated SMR plants. It proposes a new implementation that complies with the defense in depth principle highlighted in NSS 17 that relies on nested VPN tunnels for both PPS and I&C operation. This approach is compared with other possible implementations, addressing their advantages and drawbacks. The study also examines some of the implementable solutions in terms of encryption algorithms to consider the whole lifecycle of SMR operations. The document proposes generic recommendations for telecommunication hardware to take account of diversity and segmentation of usage principles.

This study also analyses the French regulatory framework in order to identify the potential adaptations required for the development of such systems.

Country OR International Organization

FRANCE

Email address

olivier.dhenin@sfr.fr

Confirm that the work is original and has not been published anywhere else

yes

Author: BOULLEY, Sylvain

Co-authors: BENOIT ROSARIO, Abel (Ministry in charge of nuclear security); DHENIN, Olivier (IRSN); FICHOT, olivier (IRSN)

Presenter: BOULLEY, Sylvain

Track Classification: Topical Group C: Safety, Security and Safeguards: Track 11: Security of SMR: Physical Protection and Computer Security