Contribution ID: **381** Type: **Oral**

Insider Threat Security Considerations for Advanced and Small Modular Reactors

The wide range of nuclear power plant technologies currently in design globally have a range of unique characteristics that create novel security considerations compared to large conventional nuclear power plants. Some of these characteristics create insider threat considerations for nuclear security, where insiders are defined as individuals with legitimate access to nuclear facilities and materials who use this access to carry out sabotage or theft of nuclear material. These include a lack of mature security culture in developer organisations, serial plant manufacturing in a production line environment, plant siting in remote and isolated areas, minimised staff numbers, teleoperation of plants by offsite staff, the increased reliance on digital instrumentation and control systems, and the potential for greater involvement of foreign experts and third-party suppliers, especially on short-term bases for, e.g, refuelling and maintenance. The paper takes a technology agnostic approach to examine what these factors may mean for insider threat risks and suggests that plant designers should be identifying and minimising the opportunities of insiders to act throughout the engineering design process. Doing so is anticipated to lead to much more effective insider threat mitigation in deployed small and advanced reactors.

Country OR International Organization

United Kingdom of Great Britain and Northern Ireland

Email address

ross.peel@kcl.ac.uk

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

YES

Authors: Dr PEEL, Ross (King's College London); HOMAN, Zenobia (King's College London)

Presenter: Dr PEEL, Ross (King's College London)

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