W17 Emerging Cyber Threats to Industrial Control Systems

Industrial control systems (ICS) and other operational technology continue to face growing and evolving cyber threats. Advancements in digital technology have broadened its appeal and applicability throughout the nuclear industry, from digital instrumentation and control to advanced reactors. These applications combined with an evolving cyber threat have the potential to increase a facility's attack surface and expose it to increased cyber risk. This panel will discuss emerging ICS cyber threats and highlight potential mitigative measures to defend nuclear facilities from cyber attacks.

SESSION CHAIR(S):

- James Beardsley, Chief, Cyber Security Branch, Division of Physical and Cyber Security Policy, NSIR/NRC e-mail: James.Beardsley@nrc.gov

SPEAKER(S):

- Introductory Remarks

  James Beardsley, Chief, Cyber Security Branch, Division of Physical and Cyber Security Policy, NSIR/NRC

- Mark Bristow, Chief, Cyber Defense Coordination Branch, Threat Hunting Division, Cybersecurity and Infrastructure Security Agency
- Dragos Perspective on Emerging Threats to ICS

  Jacob Benjamin, Director of Professional Services, Dragos, Inc.

- Joel Max, Industrial Control Systems Lead, Federal Bureau of Investigation
- INL Perspective on Emerging Threats to ICS

  Robert Anderson, Nuclear Cybersecurity Consultant, Idaho National Laboratory

SESSION COORDINATOR(S):

- Tammie Rivera, Cyber Security Specialist, Division of Physical and Cyber Security Policy, NSIR/NRC e-mail: Tammie.Rivera@nrc.gov