ICALEPCS 2025 - The 20th International Conference on Accelerator and Large Experimental Physics Control Systems

Contribution ID: **282** Contribution code: **WEBG004** Type: **Contributed Oral Presentation**

TIPPSS for navigating a changing cybersecurity landscape at the Electron-Ion Collider and other scientific research facilities

Wednesday 24 September 2025 11:45 (15 minutes)

The Electron-Ion Collider (EIC) aims to unlock the secrets of the strong nuclear force and revolutionize our understanding of the fundamental structure of visible matter. It is being built at Brookhaven National Laboratory (BNL) and could possibly be the only large collider built in the world in the next 20-30 years, during the "Age of AI". This creates the very unique opportunity for a complete AI/ML lifecycle of a large-scale state-of-the-art scientific research facility, but also many challenges, as this lifecycle overlaps with a rapidly changing cybersecurity landscape. Standards, regulations, and guidance are likely to be released (and then possibly revised) at the same time that design, construction, and then finally operations of the EIC must proceed. We present the use of the new Trust, Identity, Privacy, Protection, Safety, and Security (TIPPSS) framework from the IEEE/UL 2933 TIPPSS standard as a framework for scientific research facilities. This will enable us to design and build a safe and secure infrastructure, and robust trust and identity architecture, to protect the scientific instrument ecosystem as we enable "AI readiness"and AI/ML deployment (especially at scale) in the face of increasing cybersecurity challenges, using the EIC as a case study.

Footnotes

Funding Agency

Work supported by Brookhaven Science Associates, LLC under Contract No. DE-SC0012704 with the U.S. Department of Energy.

Author: NGUYEN, Linh (Brookhaven National Laboratory)

Co-authors: HUDSON, Florence (Columbia University); JAMILKOWSKI, James (Brookhaven National Laboratory); KULMATYCSKI, Kyle (Brookhaven National Laboratory)

Presenters: HUDSON, Florence (Columbia University); NGUYEN, Linh (Brookhaven National Laboratory)

Session Classification: WEBG MC06 Infrastructure and Cyber Security

Track Classification: MC06: Control System Infrastructure and Cyber Security