9th Control System Cyber-Security Workshop (CS)2/HEP

Sunday 21 September 2025 - Sunday 21 September 2025

Book of Abstracts

Contents

1

Intro into the 9th CS2/HEP

2

Discussions

- What are your general policies for controls? Have you been audited? What are lessons learnt and best practises?
- How do you allow remote monitoring / control?
- How did you design your control network and interact with your data centre(s) and campus networks?
- How to you address cloud usage like OracleDB, Git, but also ML/AI/LLM?
- What about remote software development and CI/CD pipelines? Do you run SBOM? Some other verifications?
- How to secure IoT and SoC ("system on a chip") components?
- What about "zero-trust" in an OT environment?

/have input on/wonder

security subject HERE

3

A Wish or Hope for better OT cybersecurity

Authors: Chandler Lawrence[1]; Timothy Zingelman[None]

[1] *Fermilab*

We have implemented a commercial security appliance which processes a full network feed from our control system to passively identify threats and anomalies. We will discuss the successes and failures so far using this tool

4

(Too?) Many of ways into CERN

Author: Stefan Lueders[1]

[1] *CERN*

Remote access to labs for users and experts, in particular, control systems, is essential for the efficient running of control systems of accelerators and experiments. However, such an Internet-connectivity exposes sensitive and poorly protection systems to the risks of direct attacks. This presentation shall discuss the remote access model into the CERN Campus network as well as into its technical infrastructure.

5

18 months into the CERN cyber-security audit

Author: Stefan Lueders[1]

[1] *CERN*

With thorough 2023 cyber-security audit at CERN, the IT department and the CERN Computer Security Office as well as the Organization as a whole has been tasked with 95 different work packages to improve their computer security posture. This presentation will go to their implementation and deployment, the successes and the areas creating additional problems

6

Lessons Learned from the HZB security incident

Authors: Roland Müller[None]; Thomas Birke[None]

A ransomware attack disrupted HZB and BESSY II operations, prompting a complete network infrastructure rebuild. The recovery task force utilized standardized Ansible playbooks for rapid deployment, resulting in a modernized science data acquisition network with improved configurations managed through version-controlled GitLab repositories for enhanced tracking and maintenance.

7

The Extremely Large Telescope (ELT) Primary Mirror Control System

Author: Luigi Andolfato[None]

The Control System of the Extremely Large Telescope (ELT) Primary Mirror will be presented in terms of network layout, control system stack, possibility for remote access and data transfer, SW development and maintainability processes, interaction with other systems and the Internet.

8

Control Systems, Cyber Security and Conflicting Priorities

Author: Karen White[1]

[1] *Oak Ridge National Laboratory*

Control systems for scientific user facilities and cybersecurity initiatives share important goals but do not always share common paths and priorities. This talk will explore priority drivers, conflicts and compromises.

9

Cyber Secure Experimental Physics and Industrial Control System

Author: George McIntyre[1]

[1] *SLAC National Accelerator Laboratory*

Secure PVAccess (SPVA) brings production-grade cybersecurity to the Experimental Physics and Industrial Control System (EPICS) framework by encapsulating the PVAccess protocol within Transport Layer Security (TLS). It integrates X.509 certificate-based authentication with common laboratory-wide services such as Kerberos and LDAP, and delivers a full certificate authority, management, and distribution solution. Leveraging this robust authentication layer, Secure PVAccess extends the existing EPICS Security model to enforce true Process Variable (PV) access control based on verified peer identities, attributes, and connection modes. We describe the overall architecture, key design decisions, software components, current status, envisioned future capabilities, and the collaborative effort driving this initiative.