



Contribution ID: 129

Type: **20-minute talk**

## Improving security in RTEMS and EPICS IOC applications

*Thursday, 27 April 2023 09:50 (20 minutes)*

Cybersecurity is a rising concern in real-time and industrial control systems due to increased security threats toward these systems. In this talk, we discuss our ongoing efforts in security testing through modularization and fuzzing of the software stacks to detect vulnerabilities in different components. We have previously worked on modularizing the network stack of RTEMS into linkable static libraries. Our current efforts revolve around fuzzing using techniques such as model inference and machine learning to learn the state machine model of ICS protocol implementations to fuzz deeper states for stateful ICS protocol implementations (channel access, EPICS pvxs, etc.). We also discuss some ideas for our future work on improving the security posture of RTEMS-EPICS integration.

### **Please select if talk will be in person or on zoom**

In person

**Primary author:** BANERJEE, Vijay (University of Colorado Colorado Springs)

**Co-author:** EZEObI, Uchenna (University of Colorado Colorado Springs)

**Presenters:** BANERJEE, Vijay (University of Colorado Colorado Springs); EZEObI, Uchenna (University of Colorado Colorado Springs)

**Session Classification:** Plenary Session

**Track Classification:** Cybersecurity