Contribution ID: **34** Type: **not specified**

Access Security of RHIC Control System

Sunday 8 October 2017 14:00 (30 minutes)

RHIC Control System is based on the Accelerator Device Object (ADO) model, and it uses RPC protocol over TCP/IP transport level. The access to any device is managed by corresponding ADO Manager, a C++ or Python program, running on a workstation or a front-end controller. All wired networking equipment is isolated from the rest of the lab behind the strictly maintained department firewall. Each new device, before being wired to the network, passes rigorous certification process. The device access policy is based mainly on access monitoring rather than on the access control. Most of the released client applications provided with a 'Set History' feature, which logs the setting of each ADO parameter into a central database, the user logins are also tracked. The 'Set History' monitoring is attached to the central alarm monitor. In addition, some of the equipment is protected with software locks, based on a file access properties. The 'Set History' monitoring was very useful in investigation of very complex machine failures.
To further improve the access security we began to implement additional features like password protection and lockout-tagout.

Summary

Primary author: SUKHANOV, Andrei (BNL)

Co-authors: BROWN, Kevin (BNL); NEMSURE, Seth (BNL); D' OTTAVIO, Ted (BNL)

Presenter: SUKHANOV, Andrei (BNL)