Contribution ID: **5** Type: **not specified**

Standards Based Measurable Security for Embedded Devices

Sunday 11 October 2009 09:15 (30 minutes)

Control systems are now routinely connected with enterprise networks and even wide area networks, opening their components to a large array of cyber security threats. Facing threats on such a large scale can now longer solely be done through ad-hoc incident response and post-mortem activities. Defense in depth strategies are being widely adopted and advocated through emerging control systems specific cyber security standards [1]. With these strategies comes the need to accurately prioritise risks and manage system assets, in order to implement measured, tailored security restrictions and automatically assess damages to provide efficient and precise incident response. Eventually, an organization must be able to measure incidents trends and evaluate business impact to feed constant security policy reviews. CERN has implemented a control device cyber security test bench, entitled TOCSSiC [2], updated to provide standards-compliant measurements. Such measurements can be employed to automatically evaluate device vulnerabilities and security policy compliance.

[1] F. Tilaro, “Control system cybersecurity standards, convergence and tools”, CERN technical report, April 2009

[2] S. Lueders, “Control systems under attack !?”, ICALEPCS, October 2005

Author: Mr COPY, Brice (CERN)

Presenter: Mr COPY, Brice (CERN)