(CS)^2

HEP

Contribution ID: **18** Type: **not specified**

Technical, Legal, and Social Issues in Control Systems: Past, Present, Future

Sunday 6 October 2013 15:30 (25 minutes)

Control systems in physics, as well as non-scientific arenas, have been targeted for attack by governmental and non-governmental entities alike. The move toward use of a network bus architecture, concomitant with the opening of networks to commercial, private, and public access, increases security, safety, and privacy issues immensely. Protocols and systems developed for a sandbox environment frequently did not take into account the opening of networks to world-wide access. Private networks are no longer private; NAT can be easily bypassed; the need to transfer source code, configurations, firmware, opens up multiple attack vectors, at least some of which can not be eliminated. Risk analysis is frequently used to determine local policies. Legal and financial issues introduce additional factors into those policies. Even so, recent revelations about governmental and private coordination of network traffic monitoring and attacks introduce new factors not previously considered in this risk analysis. Quality management techniques such as RIPE (http://www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf) can be applied to suggest best practices. However, even those do not always allow for deep technical analysis. We discuss legal, technical, and social issues involved in dealing with the difficult situation of modern networked control systems, with examples from our clinical accelerator.

Primary author: BANERIN, Stefani (UW School of Medicine)

Presenter: BANERIN, Stefani (UW School of Medicine)