ID de Contribution: **14** Type: **Non spécifié**

Control Systems Under Attack ‼?

mercredi 20 septembre 2006 08:30 (1 heure)

The enormous growth of the worldwide interconnectivity of computing devices (the "Internet") during the last
decade offers computer users new means to share and distribute information and data. In industry, this results in an adoption of modern Information Technologies (IT) to their plants and, subsequently, in an increasing integration of the production facilities, i.e. their process control and automation systems, and the data warehouses. For the European Organization for Nuclear Research (CERN), the Internet opens the possibility to control (parts of) the LHC particle collider and its four LHC experiments remotely from any where
in the world.
Unfortunately, the adoption of standard modern IT in distributed process control and automation systems also
exposes their inherent vulnerabilities to the world.
Furthermore, this world is by far more hostile than a local private controls network as the number and power of worms and viruses increase and hackers start to become interested in control systems.
This presentation will address security problems in common-of-the-shelf control systems and present results of CERN's test stand for control systems security (TOCSSiC). From that, basic security requirements concerning
the cyber-security of automation devices with regard to network-based attacks can be deduced. However, protection solely on the device-level will not be sufficient. A general "defense-in-depth"approach will be described, which requires protective measures at every layer: the security of the device itself, the firmware, network connections and protocols, the software applications, third party software, and the cooperation of the developers, manufacturers and users.

Auteur principal: LUEDERS, Stefan (CERN)

Orateur: LUEDERS, Stefan (CERN)

Classification de Session: Session plénière