Contribution ID: **6** Type: **not specified**

Update on the CERN Computing and Network Infrastructure for Controls (CNIC)

Sunday 14 October 2007 11:15 (30 minutes)

Over the last few years, modern accelerator and experiment control systems are based more and more on commoncommercial-off-the-shelf products (VME crates, PLCs, SCADA systems, etc.), on Windows or Linux PCs, and on communication infrastructures using Ethernet and TCP/IP. Despite the benefits coming with this (r)evolution, new vulnerabilities are inherited, too: Worms and viruses spread within seconds via the Ethernet cable, and attackers are becoming interested in control systems. Unfortunately, control PCs cannot be patched as fast as office PCs. Even worse, vulnerability scans at CERN using standard IT tools have shown that commercial automation systems lack fundamental security precautions: Some systems crashed during the scan, others could easily be stopped or their process data be altered. During the two years following the presentation of the CNIC security policy at ICALEPCS2005, a "defense-in depth"approach has been applied to protect CERN's control systems. This presentation will give a review of its thorough implementation and its deployment. Particularly, measures to secure the controls network and tools for user-driven management of Windows and Linux control PCs will be discussed.

Author: Dr LUEDERS, Stefan (CERN)

Presenter: Dr LUEDERS, Stefan (CERN)