Contribution ID: **13**   Type: **not specified**

Discussions

Sunday, 18 October 2015 15:30 (1 hour)

Potential discussion topics:

- Implementing Multi Factor Authentication
- Reduction of "privileged users" on controls devices
- How to have a QA process for software development and a secure software development life-cycle
- The fallout of Windows XP's death
- Virus scanning on control PCs and other cyber Security tools which can benefit (e.g. Firewall, IDS/IPS, white listing software, patch management, system hardening)
- Maintaining private networks with consumer-grade equipment
- The buying and selling of 0-day vulnerabilities, with the participation of governments.
- Governments sabotaging good standards (e.g. encryption)
- Specific Policy & Standards and Governance on Control System Cyber Security –Are there any organisation that has them, at the control system level?, or the IT ones are used instead?
- Cyber security audits/ KPI/metrics. Is it common to have specific audits on Control System Cyber security? What do organisations audit/report on?
- Are security incidents being logged or tracked, are we experiencing an increase over the last few years?
- Would people in the workshop be interested in creating a Survey around Control system Cyber Security? Organisations could opt to participate in completing the survey and then we could get a good picture where our community is heading to and what are the main areas of interest/concern.

Presenter: Dr LUEDERS, Stefan (CERN)