



Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures



SCADA Cybersecurity Workshop Stavanger, 3rd December 2014

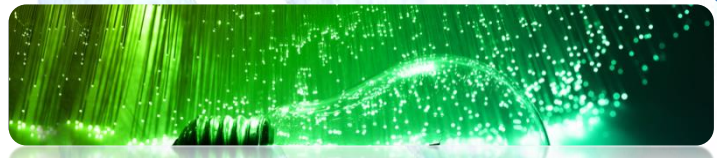
Lyse has the pleasure to invite you to the
5th CockpitCI Workshop.

Critical Infrastructure is increasingly threatened by cyber-attacks following their transition from a proprietary and closed architecture to an open, standard-based solutions aimed to enforce interoperability and the deployment of smart systems. For the last two years, the partners of the European CockpitCI project have developed a framework to allow the community of CI owners to detect, analyse and exchange real-time information about attacks in order to assess risk and avoid disastrous cascading effects.

The present workshop aims to describe the projects results. Furthermore, security issues for operators will be addressed and business impacts will be discussed.

AGENDA

- 8:30 Registration
- 9:00 Welcome : Lyse
- 9:15 Pr. Paulo Simoes (University of Coïmbra, Portugal): *“Improving cyber-security awareness on Industrial Control Systems: the CockpitCI approach”*
- 9:45 Mr. Michele Minichino, (ENEA Casaccia Research Center, Italy): *“An electrical grid and its SCADA under cyber attacks: modelling versus a Hybrid Test Bed”*
- 10:30 Dr. Sergei Iassinovski, (Multitel, Belgium): *“Quality of service indicators simulation under cyber attacks using Intelligent RAO Simulator”*
- 11:00 Coffee break
- 11:30 Mrs. Chiara Foglietta, (University Roma TRE, Italy): *“Integrated Risk Prediction: think globally and act locally”*
- 12:00 Dr. Leonid LEV (Israel Electrical Corporation, Israel): *The validation methodology for the multinational research projects. CockpitCI project example”*
- 12:30 Question & Interactive discussion



Where: Lyse Energi AS
Breiflåtveien 18
4017 Stavanger

Registration required
Send an email to alan.howarth@lyse.no
by the 28th November .

For more information about the workshop or organizational issues, please contact alan.howarth@lyse.no