

Call for papers - Special session: “Cybersecurity of control and safety systems”

Co-chaired by

Dr. Vitaly Promyslov (V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia), contactv1925@mail.ru and vp@ipu.ru

Dr. Ludovic Pietre-Cambacedes (EDF, France), contactludovic.pietre-cambacedes@edf.fr

Scope

Modern digital control systems are now at the core of many industrial facilities, conditioning their performance and safety. They rely on complex and distributed architectures, implementing multiple functions, on numerous digital components throughout the facility. A more profound automation of industrial facilities has the potential to increase operation safety, to enhance production and to reduce development costs. Nevertheless, it also brings new cyber security threats for the facility. Logically, the technical evolutions of control and safety systems (including interconnectivity, use of COTS and of wide audience standards), and the rapid evolution of the threat landscape (marked recently by Stuxnet and Flame) has turned cybersecurity into a high-priority issue. To face this challenge, innovation and research are needed: this session aims at contributing to this effort. It is open to both industrial and academic contributions in the area of cybersecurity of control and safety systems. High-quality scientific papers are expected, but industrial use-cases and application reports are also most welcome.

Topics

The list of topics includes, but is not limited to:

- Secure development of control systems or safety systems
- Security metrics
- Intrusion-tolerant and resilient systems and architectures
- Coordination between safety and cybersecurity requirements or provisions
- Intrusion detection in control systems
- Threat and attack modeling
- Formal security models
- Assessment tools and methodologies
- Cybersecurity solutions matching SCADA specificities and constraints
- Cybersecurity maintenance over time in I&C environments
- Risk assessment approaches adapted to I&C context
- Cybersecurity exercises and contingency plans
- Incidence response
- Forensics for industrial control systems
- Policy, regulations, normative frameworks
- National and international coordination or research initiatives

Important dates and submission information

The deadlines are similar to those for the regular papers (Oct. 1, 2012: deadline for draft papers (6 pages max.); Feb. 1, 2013: notification of acceptance; Apr. 15, 2013: final papers submission and early registration). For submission, please select in the paper submission section “invited paper” and indicate the session code:

4pxfx

For more information, please see <http://mim2013.org/code/sessions.htm> or contact one of the session chairs.

Proposal submitted to 2013 IFAC Conference on Manufacturing Modelling, Management, and Control. Uploaded July 23, 2012.