**Technical Scope**

Integrating cyber security and functional safety has been an integral part of any company’s overall risk management strategy. **Cyber Security for Industrial Control Systems** will feature an exclusive track on ‘Systems Safety’ designed to bring experts from both fields under one roof to discuss, debate and find solutions to the challenges facing critical systems.

Contributions to this track can range from theoretical research concepts and ideas to more applied engineering and industrial applications, and are encouraged from, but not limited to, the themes and topics in the following areas:

**Tops**

1. Safety assessment and Hazard identification
2. Competency and competency schemes
3. Complex programmable electronic devices (e.g. ASICs, FPGAs)
4. Corporate governance
5. Securing systems, management involvement and governance
6. Defining measurable safety requirements
7. Scoping the safety contract for suppliers
8. Independent safety and cybersecurity auditing
9. Safety and systems engineering
10. Safety standards and Industry best practices
11. Defining measurable safety requirements
12. Holistic risk assessment; safety and security together
13. Maintaining levels of safety and security with fewer funds and staff
14. Vulnerabilities, threats and solutions to cyber security in safety-critical systems
15. The human factors of cyber security and safety
16. The challenge of converging paradigms: Confidentiality, Integrity, Availability (CIA) and Safety, Reliability, Availability (SRA)

We will also consider presentations and workshops covering cyber security topics in the context of system safety.