

# Functional Safety and IT Security – an Engineering Yin and Yang relationship?

---

Workshop @ SAFECOMP 2015, September 22<sup>nd</sup>, 2015, Delft, NL

(<http://safecomp2015.tudelft.nl/>)

Workshop organizers: Chris Johnson (University of Glasgow), Jens Braband (Siemens AG)

Full day workshop. In order to encourage contributions from industry or regulators, full papers are welcome, but the minimum requirement is an extended abstract (2 pages).

Information security for safety related systems has become a real issue, in any case since attacks on industrial control systems have been reported. However, most of the attacks are denial-of-service attacks leading to service interruptions, but so far rarely to safety-critical incidents. But also other services supporting safety-related systems, such as satellite positioning or communication systems, have been shown to be susceptible to IT security attacks.

Also the increasing integration of Commercial Off the Shelf components, e. g. computing platforms or communication systems, into safety-critical systems has increased concern that mass market malware may be transferred into safety-related applications. This would have been less likely when previous systems relied on bespoke components; fewer attackers had the technical knowledge to compromise safety related systems. Also the growing demand for remote services and the continuing trend towards standardization is increasing the exposure of safety systems to cyber attacks. These concerns have been compounded by the increasing diversification of the supply chain and a growing reliance on sub-contractors who may not understand safety and security concerns. At the same time, a growing range of advanced persistent threats have begun to target safety-related infrastructures.

Like in Chinese philosophy IT security and functional safety seem to be in a kind of Yin and Yang relationship: both concepts are at first sight opposite or contrary, but are actually complementary, interconnected and interdependent in the cyberphysical world. Take the control of the cockpit cabin door as an example: from a safety point of view it should open in case of emergencies, while from a security point of view it should be locked.

In this workshop, we want to address a broad range of issues that arise at the interface between safety and security – including but not limited to:

- Taxonomy of Safety and Security systems
- Integrated Tools and techniques that support both safety and security concerns – such as risk assessments;

- Conflicts between safety and security, e. g. patch management
- synergies and differences in risk/threat assessment for security and safety critical systems;
- synergies and differences in incident reporting and analysis for security and safety critical systems;
- Human and organizational issues in the coordination of safety and security across the business lifecycle;
- Exchanging good practice – for example extending incident analysis techniques from safety related mishaps to identify the root causes and contributory factors in security incidents.
- the role of regulation and certification
- system architectures which satisfy both safety and security needs, e. g. allowing SW patching while maintaining safety approval
- experience with standards

For paper submission the same rules as for SAFECOMP regular papers apply (see <http://safecom2015.tudelft.nl/paper-submission-details>).

Deadlines:

- 1st paper or full presentation submission: 22 May 2015
- Notification of acceptance: 15 June 2015
- Camera-ready paper submission: 28 June

Publication of accepted reviewed papers usually by Springer LNCS. Selected papers may also be published in a Special Edition of Elsevier's Safety Science.