# CeMoSS - Certification and Model-Driven Development of Safe and Secure Software

Software is a key factor driving the innovation of many technical products and infrastructures for everyday use. Dependable software requires rigorous quality assurance in particular to achieve an adequate level of safety and information security. In many domains like avionics, power generation and distribution, industrial automation, railway and automotive, as well as medical devices and health information systems, dependable systems and the software therein have to be formally approved with respect to safety and security and certified according to international standards, before being put in operation. In spite of all domain-specific singularities, the following issues challenging the development of safe and secure software shall be addressed in the workshop and discussed by a cross-domain audience:

- Model-driven software development with extensive tool support becomes more and more accepted in industry. Although safety standards recommend the formal foundations and systematics a model-driven approach relies on, advanced features of model driven development frameworks like automated code generation, model transformation and model checking are not yet addressed in detail in the standards. Thus using new methods and tools brings new risks into the certification of a product since it requires additional arguments in the assurance case just because the development deviates from the best-practice procedure, even if there is strong evidence that the new approach outperforms the older one with respect to error avoidance or error disclosure.

- Critical infrastructures and dependable systems are no longer operated in isolation, but connected to other company networks or accessed by mobile devices using the public telecommunication infrastructure like in smart home environments or car to car communication. Connectivity is an enabling factor for enhanced services, but also raises new threats from the newly introduced dependency between functional safety and IT security. New modeling approaches shall integrate safety and IT security issues in risk and safety analysis and design. Open issues are in particular the integration of safety and security processes, risk acceptance criteria that take both, safety and security into account, even for architectures of commercial systems with a life-cycle of a few decades and a holistic view on safety and security in the assurance case. A particular challenge arises in safety critical industrial infrastructures where life cycles are much longer than 10 years. Then security updates may be required without impact on functional safety and the resp. safety cases and certifcates.

- Open source software has been introduced in the realm of dependable systems as tools in supporting processes, but first usages of open source components as part of

the dependable system itself are under development (See the European project OpenETCS). In case open source software is used exactly as versioned and documented, it may be certified according to IEC 61508 or other relevant standards. However, the development or adaption of dependable software in an open source project raises new questions about adequacy of processes, tools and the competences of personnel as well as liability issues. Finally, the balance between the developing and operating staff and bodies, and the users of dependable systems has to be newly discussed.

Topics of interest include but are not limited to: risk analysis, integration of safety and security, seamless tracing and decomposition of safety and security constraints, safety and assurance cases, modular certification, qualification of methods and tools, external proof checking of formal validation & verification results. The CeMoSS-workshop shall foster the cross-domain discussion of challenges and possible solutions in the development ofhigh assurance systems and infrastructure between academia and industry. Thus contributions reporting onoriginal research ideas as well as experience reports raising open questions from industrial practice are most welcome.

December 2013

Michaela Huhn (TU Clausthal)
Stefan Gerken (Siemens AG)
Carsten Rudolph (Fraunhofer SIT)
PC chairs CeMoSS'14