

**CALL for Contributions:  
DECOS/ERCIM Workshop 2007 on Dependable Embedded Systems**

“Dependable Embedded Systems – Challenges, Impact, Solutions, Examples, Professional and Academic Education and Training”

Chairs Erwin Schoitsch (Austrian Research Centers – ARC), Amund Skavhaug (NTNU Trondheim),

at SAFECOMP 2007, Nuremberg, Germany, Sept.18, 2007 ([www.safecomp.org](http://www.safecomp.org))

**Deadline for contributions (papers): Aug. 6, 2007**

Size of Papers : about 6-10 pages in SAFECOMP Format

“Smart Systems” (including all types of embedded control systems with “intelligence”) are nowadays omnipresent in our daily life. Applications range from non-safety critical applications (entertainment, infotainment, edutainment, non-critical communications, certain home appliances from the “ambient intelligence” area) to safety related or safety critical ones. These systems include industrial control systems, embedded systems in cars, railways, aircrafts and other vehicles, wireless sensor surveillance and monitoring networks, building automation systems, critical infrastructures and many others. Nowadays a large amount of research is done on these topics separately – domain independent as well as domain dependent. But in the foreseeable future this way of research may not be sufficient to satisfy all needs of automation systems. Starting with EU-FP 6, where the Embedded Systems Unit within the IST directorate was created, these problems were addressed by (integrated) projects like DECOS (Dependable Embedded Components and Systems) and organizations like ERCIM (European Research Consortium on Informatics and Mathematics) and EWICS (European Workshop on Industrial Computer Systems), and various standardization and industrial organizations.

In the near future, the trend to connect embedded control systems and subsystems, including public networks and automation networks, vehicles and critical infrastructure systems, via public communication systems will highly increase (catch phrases are: “industrial control via internet”, “car on the internet”, “Power grids control via internet” etc.). Then, for example car2car communication for platooning cars needs not only to be safe, but also secure. Security breaches will impact safety and vice versa: a holistic system view is required, covering all life cycle phases – from concept, risk/hazard analysis, development to maintenance and disposal, and all system aspects (control system, system under control, environment, human interaction and usage). Dependable systems are systems that can justifiably be relied on throughout the complete life cycle and under all possible conditions of use. Depending on the application the dependability attributes safety, reliability, maintainability, survivability, availability and security are emphasized to a greater or lesser extent, i.e. a complex dependable control system will never be totally available, safe and secure. The optimal combination of desirable dependability attributes has to be found and implemented, based on system risk/hazard assessment and evaluation.

Additionally, these emerging issues have to be addressed by education and training too – contributions to topics related to education, training and “life-long learning” in the dependable smart systems area are very welcome!

Topics:

- Design concepts and architectures for dependable networked embedded systems
- Methods, means and techniques to tolerate, remove, to prevent and forecast faults in dependable networked embedded systems
- Functional Safety and Security Standards, validation and certification of dependable networked embedded systems
- Tools and tool chains to facilitate design, development, operation and maintenance effectively and efficiently of dependable networked embedded systems in industrial context
- Education and Training issues, means and methods to cope with the growing demand for people being aware and professionals in a holistic way of thinking

The presentations will be grouped and discussions on (hopefully) even controversial issues are encouraged and moderated by the chairpersons. Papers will be peer reviewed and proceedings be published by ERCIM after the workshop, including results of discussions as well.

Information/Contributions to: [erwin.schoitsch@arcs.ac.at](mailto:erwin.schoitsch@arcs.ac.at) , [amund.skavhaug@ntnu.no](mailto:amund.skavhaug@ntnu.no)