

# **A holistic view at Dependable Embedded Software-Intensive Systems**

Erwin Schoitsch, Austrian Research Centers – ARC (Vienna, Seibersdorf)

[erwin.schoitsch@arcs.ac.at](mailto:erwin.schoitsch@arcs.ac.at)

## *Abstract:*

Embedded software-intensive systems are already almost “omnipresent” – and key to most of the innovations today and in the future in almost all domains of our life. Reliance on their services became a critical issue, although humans are very well able to adapt to unsatisfactory performance and reliability to a certain extend – today’s Windows-PCs, SPAM-emails and Internet are very good examples.

Dependability as a complex “umbrella”-property is key to massive, ubiquitous deployment and use of embedded smart systems, including sub-properties such as safety, reliability, availability, security, maintainability, survivability. These properties are, depending on the application, not independent: they can be complimentary or even contradictory. Embedded systems are completely integrated in their environment (“hidden” computing), and in many cases integrated in networks of different connectivity, interacting with each other, with humans and environment via various means. They consist of control units, sensors, actuators, “intelligence” (“smart systems”) – to serve our needs and fulfil their tasks in a safe and reliable manner. Applications include critical systems such as sea, ground and air transport, medical devices, industrial and power plant control, surveillance and monitoring, emergency systems, other working environments, and less critical ones for communication, info-/edutainment and entertainment.

Dependability therefore is not a simple single issue – it has to take into account hardware, software, communication, networking, interfaces, environment and humans (behaviour and different mind models, human mistakes), all in different roles. Systems are not always critical by definition, often the actual criticality and dependability levels rise based on our desire for enhanced reliance on them!! Examples are: safer cars imply more aggressive driving behaviour after some time; or: (almost) perfect driver assistance systems may lead to too much reliance on them thus becoming safety critical. On the other hand, by their originally not implied usage or unforeseen combination of incidents not taken into account by risk and hazard analysis, systems become (more) dangerous: examples are the Kaprun cable car fire catastrophe, or the London Ambulance System Disaster: The ambulance car emergency management system was not considered safety critical – but because of ambulances not arriving in time or at all at the required location several people died! The same would be the case if security breaches, e.g. malicious insertion of wrong data or commands in a control loop, could cause dangerous situations (chemical reactor explosion, traffic jam, air traffic control, ...), and nobody has thought it likely that someone could have interest in such an incident. Not only after 9-11, we have to take into account malicious actions. Additionally, public acceptance (or non-acceptance), legal or environmental issues, liability, and social aspects influence system usage and dependability as well.

The presentation will demonstrate that mass deployment of networked, dependable systems implies a new, holistic system view on critical systems, and how the challenges should be addressed by proper system assessment and evaluation, architecture, design, development, validation and maintenance.

## About the speaker:

Erwin Schoitsch, born 1944 (Vienna), received his Master Degree in Technical Physics and a Bachelor degree in Computer Science (1962-1969) at the University of Technology in Vienna. He works at Austrian Research Centres - ARC for more than 35 years, focusing on industrial and research projects dealing with systems of high dependability or with software process improvement, including many European projects (ESPITI, OLOS, SPIRE, ENCRESS, ACRuDA, ECUA, ISA-EuNet, AMSD, COOPERS, DECOS). He is active in international working groups (EWICS TC7, ERCIM) and standardization of functional safety (IEC 61508, ISO WD 26262). His main interest is the holistic approach to system dependability.