

Preface

The conference DepCoS - RELCOMEX '06 is organized by the Institute of Computer Engineering, Control and Robotics (previously the Institute of Engineering Cybernetics), Wrocław University of Technology.

The conference is building upon tradition of two series of scientific events which had been organized by the Institute of Engineering Cybernetics:

- Reliability and Exploitation of Computer Systems RELCOMEX - the first conference was organized in 1977 and the last one in 1989; all these conferences took place in the beautiful Książ Castle, not far from Szklarska Poręba,
- Microcomputer School - seven events organized in the Sudety Mountains (beautiful too) since 1985 till 1995 (more details on the back cover of the Proceedings).

Since the first conference (1977) everything in the theory of system reliability, the theory of systems (and networks), and especially in the informatics (computer science, computer engineering, computer application, computer tools) has unimaginably changed and needs new scientific and engineering approach.

It may be interesting to realize the premises which form the basis of the new approach to reliability and maintenance of computers and networks:

- **An object of research has changed** - instead of separate devices (or even only elements) now a network of computer systems is under consideration and the computer system itself is understood as a unity of functionalities, software and, in the extreme end, hardware.
- **System events** - majority of malicious system events are consequences of software faults and human error. It is easy to notice that hardware failures are indeed more and more rare now but the number of various attacks (addressed or broadcast) on the system is growing rapidly. It is a new important problem.
- **System renewal** - the fundamental problems of maintenance of contemporary computer networks and systems are focused on renewal of system functionality and information resources after each system fault or attack on the system. Methodologies are searched for to design optimal policies of system reconfiguration and recovery. Another important problem is reconfiguration and rerouting in computer networks.
- **Mathematical computer tools** - a lot of new possibilities are available for building more suitable mathematical models of systems and networks under consideration and then to solve these models with new computer tools. Please note how many mathematical restrictions may be released when simulation models and tools are used!

Because of the above remarks the scientific term **reliability** has gradually turned into the more comprehensive term **dependability**.

The new title of our conference is Dependability of Computer Systems and the conference heritage is emphasized in the abbreviation DepCoS – RELCOMEX.

The main topics of the conference are:

- Modeling
- Methodology and tools
- Dependability of computer networks
- Software security and reliability
- Multi – agent systems
- Fault tolerance in digital systems
- Applications

The term “dependability” is receiving increasing attention in contemporary information society. With unprecedented proliferation of information systems in all aspects of everyday life, new challenges that must be met require novel, multi-disciplinary thinking. EU Integrated Program DESEREC, presented briefly on the following pages, is an example of such standpoint. It seems certain that this approach will shape the future of what originated under the term “reliability” many years ago.

Prof. Wojciech Zamojski
Conference Chairman



Dependable security by enhanced reconfigurability DESEREC

DESEREC aims to increase the dependability of critical open and interconnected information systems by a multi-disciplinary, coordinated effort. Project partners propose a **joint step forward** for today techniques to dramatically improve the information and communication systems supporting the critical services to European citizens.

- **Modelling and simulation (“incident prevention”)**: DESEREC devises and develops innovative approaches and tools to design, model, simulate, and plan critical infrastructures to dramatically improve their resilience.
- **Distributed detection (“incident detection”)**: DESEREC integrates various detection mechanisms to ensure fast detection of severe incidents but also to detect complex ones, based on a combination of seemingly unrelated events, or on an abnormal behaviour.
- **Response (“operate through incidents”)**: DESEREC provides a framework for computer-aided counter-measures initiatives to respond in a quick and appropriate way to a large range of incidents to mitigate the threats to the dependability and rapidly thwart the problem. **Re-configuration** is the utmost mechanism for system survivability.

A three-tiered response to exceptions and incidents: planning of nominal and degraded operating modes, detection of incident and quick local response, reconfiguration to a planned or emergency mode with a high level of automation in response and a human-driven improvement of rules for detection, decision and response. By achieving that inter-disciplinary framework, DESEREC also provides a far higher resilience to internal attacks, the most unpredictable by nature.

DESEREC will respond efficiently to the three families of incidents which can occur in a critical system: Attacks from the outside, Intrinsic failures and Misbehaviour or malicious internal use.

As incidents act with different time scales and impact levels, DESEREC includes three response loops working on 3 different answering times to provide a suited answer (Figure 1):

- A few seconds to locally respond to a severe and well-characterized incident and to launch emergency curative procedure to avoid escalation process or dramatic damage.
- Some minutes to detect very complex problem and to readjust the system (i.e. through computer aided reactions).
- Some hours to build a new configuration optimized to resist to a new situation and validated through modelling and simulation.

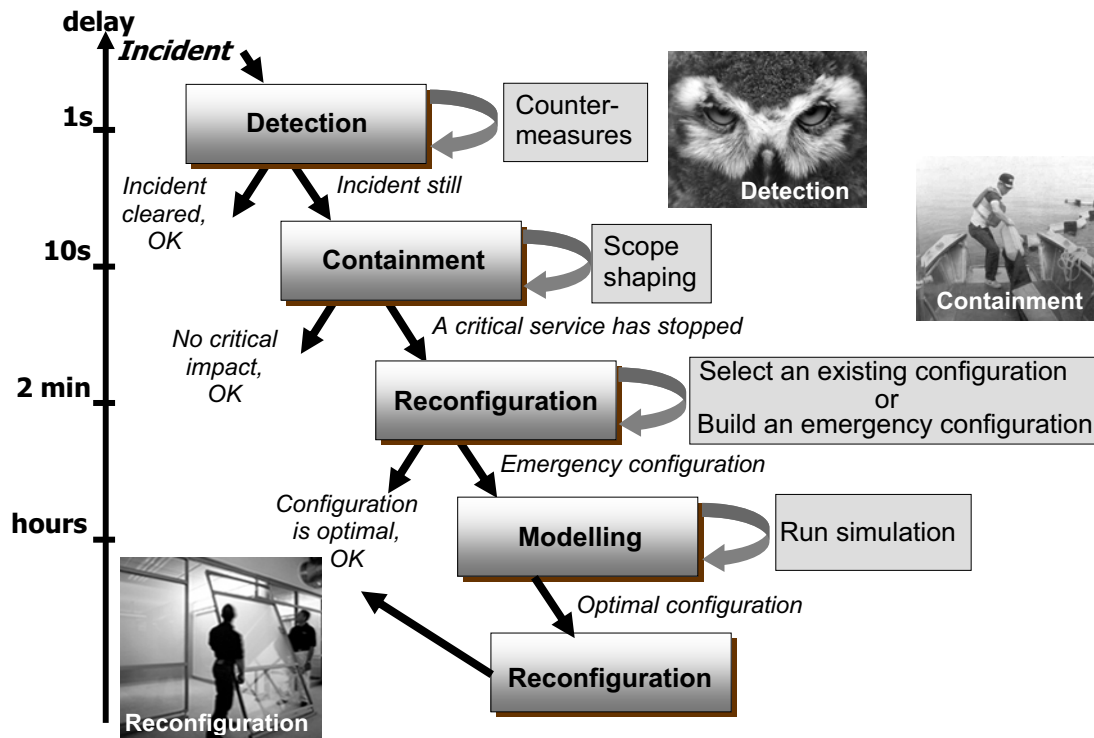


Figure 1. DESEREC expected outcome: a multi-tiered response infrastructure

Applicable to every structured Information System, the DESEREC approach, framework, and tools improve their resilience and their ability to provide dependable services. In this context, DESEREC aims at:

- Designing, developing and validating tools for incident detection and decision support. The tools span different time scales and provide solutions for survivability that range from immediate reaction to global and smooth reconfiguration through policy based management for an improved resilience.
- Enhancing the self-healing properties of critical infrastructures by planning, designing and simulating optimised architectures tested against several realistic scenarios.
- Improving risk management, crisis management in critical infrastructures with the design of new models, countermeasures, and incident management tools as well as a thorough analysis of several situations (infrastructures and scenarios). Devises, characterizes, models and designs mechanisms to mitigate the cascading and escalating effects induced by inter and intra dependencies.
- Developing decision support tools for critical infrastructures, validated by scenarios for several case studies on infrastructures.
- Providing stakeholders, the industry and services architects and ICT students with appropriate training courses and disseminating innovative findings and tools.

Project coordinator

Mr André Cotton
<http://www.deserec.org>
Thales Communications S.A.
160 Boulevard de Valmy
92700 Colombes, France

More information

Andre.COTTON@fr.thalesgroup.com

Project partners:

