

Preface

The conference DepCoS - RELCOMEX '07 is the second event in the new annual conference series organized by the Institute of Computer Engineering, Control and Robotics (previously the Institute of Engineering Cybernetics), Wrocław University of Technology.

The common title of the conference series is
Dependability of Computer Systems
with the abbreviation

DepCoS - RELCOMEX.

The conference abbreviation emphasizes a heritage 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 the 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). The conference is building upon this tradition.

This year all submitted papers have been divided into five sessions that are devoted to:

- Modeling
- Methodology and tools
- Dependability of computer networks
- Software security and reliability
- Applications

We believe that the DepCoS–RELCOMEX conferences will create a platform for discussion of dependability and maintenance problems of large systems, specially of computer systems and networks which, at present, often operate in “hostile” environment. Because computer systems play an increasingly important role in virtually all aspects of contemporary information society, new challenges require novel, multi-disciplinary thinking about the term “reliability”. EU Integrated Program DESEREC, presented briefly on the following pages, is an example of such approach.

Finally, as the Conference Chairman I would like to express my sincere thanks to members of Program Committee, to the reviewers and to all involved in preparation of this event. Also, it is my heartfelt desire that these few days spent in the beautiful neighborhood of Sudety Mountains will remain in warm memories of the participants. Let the 2007 edition of DepCoS-RELCOMEX be as successful as its reputable predecessors!

Prof. Wojciech Zamojski
Conference Chairman



Dependability and 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 interdisciplinary 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.

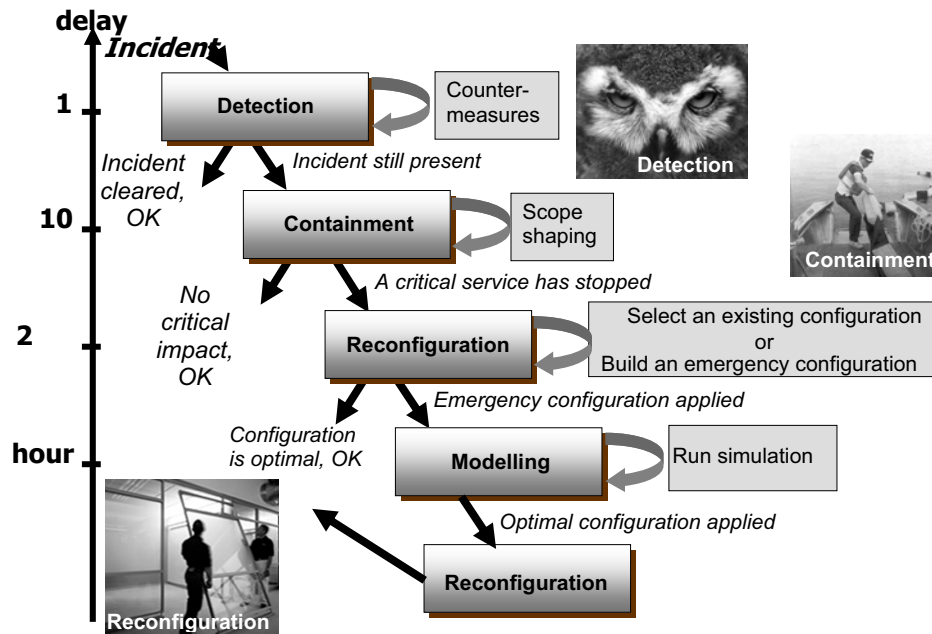


Figure 1. DESEREC expected outcome: a multi-tiered response infrastructure

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
Thales Communications S.A.
160 Boulevard de Valmy
92700 Colombes, France

More Information

<http://www.deserec.eu>

Project Partners



Thales Communications
(FR)

Budapest University of
Technology and
Economics (HU)

IEIIT/CNR (IT)

EADS Defence and
Security Systems SA (FR)

ENST (FR)

EPT (FR)

IABG mbH (DE)

Intracom (GR)

OTE (GR)

Politecnico di Torino (IT)

Wroclaw University of
Technology (PL)

Renfe-Operadora (ES)

Security Evaluation
Analysis and Research
Laboratory Ltd (HU)

Soluciones Globales
Internet (ES)

Trusted Logic (FR)

TNO (NL)

University of Murcia (ES)

Thales Services (FR)