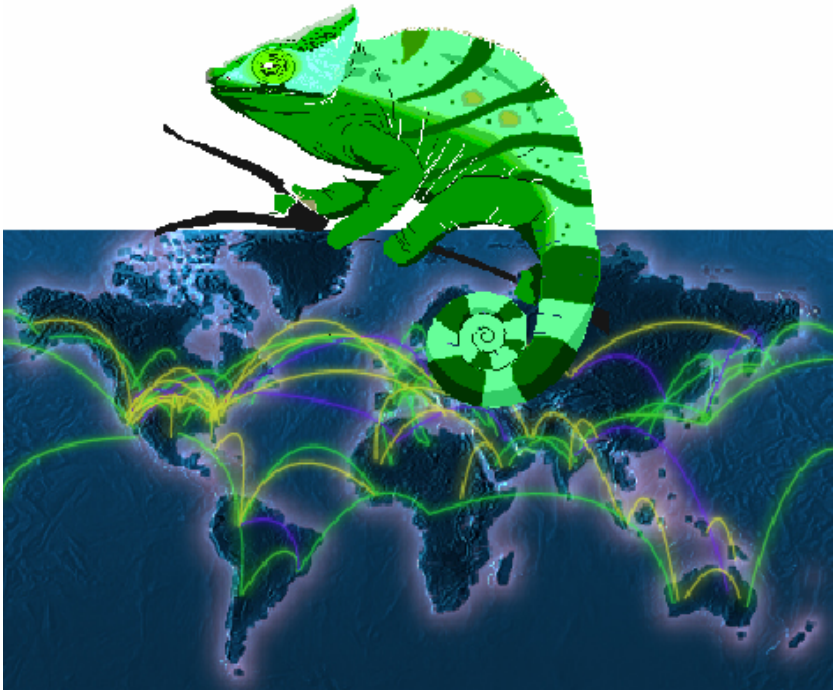
Volume 1, October 2006

# DESEREC NEWSLETTER

## DEPENDABILITY AND SECURITY BY ENHANCED RECONFIGURABILITY




***>About the DESEREC Newsletter***
*DESEREC Newsletter is published by DESEREC,*
*a research project partially funded by the*
*European Commission under the 6th Framework Programme,*
*http://www.deserec.eu*

***>Registration to this newsletter is available at***
http://www.deserec.eu/newsletter.html

***>Questions on the project should be sent to the coordinator:***
http://www.deserec.eu/partners/partner_thc.html



***>Editor***
*Gwendal Le Grand, ENST, gwendal.legrand@enst.fr*

DESEREC Dependability and Security by Enhanced Reconfigurability

# Table of contents



# Selected links

DESEREC (Dependability and Security by Enhanced Reconfigurability)
http://www.deserec.eu

**Related projects:**
CI2RCO (Critical Information Infrastructure Research Co-ordination Project)
http://www.ci2rco.org

IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems)
http://www.irriis.org

SEINIT (Security Expert Initiative)
http://www.seinit.org

POSITIF (Policy-based Security Tools and Framework)
http://www.positif.org

WS-Diamond (Web Services - DIAgnosability, Monitoring and Diagnosis)
http://wsdiamond.di.unito.it/

**Other links**
ENISA(European Network and Information Security Agency)
http://www.enisa.eu

INFSO D-Network & Communication Technologies
http://cordis.europa.eu/ist/trust-security/events.htm

6th European Dependable Computing Conference:
http://edcc.dependability.org

IFIP Working Group 11.10 on Critical Infrastructure Protection:
http://www.cis.utulsa.edu/ifip1110/Conferences/WG11-10CallForPapers.asp

International Journal of Information and Computer Security (IJICS):
http://www.inderscience.com/ijics/



Information Society Technologies

# Goals of the Newsletter

by Gwendal Le Grand,
Ecole Nationale Supérieure des Télécommunications (ENST)

Numerous projects and initiatives in the field of dependability and security have been launched or are still on-going worldwide; but the exchange of information between these projects and initiatives is complex. This newsletter focuses on the achievements of DESEREC in order to assist the readability and visibility of the project's results. It has the following objectives:
- Inform on past and future DESEREC activities and events,
- Summarise ongoing activities,
- Provide links to detailed material on specific subjects,
- Foster liaison with other related projects,
- Disseminate and advertise the project's results,
- Announce significant events (e.g. conferences) in the field of dependability and security.

In general the DESEREC Newsletter aims at promoting the project's results. The DESEREC consortium supported the following guidelines:
- Newsletter contributions should be short summaries on DESEREC related activities,
- Long articles should not be included directly in the newsletter but the newsletter may include hyperlinks to long articles or slide presentations.

The present issue of the newsletter is mainly focused on the training event which was held in Wroclaw (Poland) in September 2006. We present an introduction to the Deserec project, followed by summaries of the presentations given during the workshop.

Registration to the newsletter can be done online at: http://www.deserec.eu/newsletter.html. Each newsletter volume will then be announced by email to the registered email list. The DESEREC Newsletter is also published on the following web site: http://www.deserec.eu/.

# Introduction to DESEREC

by Benoit Bruyère,
Thalès Communications (THC)

DESEREC is an Integrated Project of the Sixth Framework Programme of the European Union in the thematic area "Information Society Technologies", under the Strategic Objective "Towards a global dependability and security framework".

The fast growth of highly interconnected Communications and Information Systems (CIS), and their use to carry out critical activities, has open an important issue regarding the resilience, reliability and security of these CISs. DESEREC aims at managing the mission-critical Information Systems in order to optimise the use of CIS resources for the provision of its business services. The strong interdependence of CIS increases the consequences of accidents, failures, and attacks and implies high vulnerabilities. Only a multi-disciplinary approach is able to leverage dependability of CISs by an alliance of the following three approaches, currently scattered into separated scientific fields:
- **Modelling and simulation**: DESEREC devises and develops innovative approaches and tools to design, model, simulate, and plan critical infrastructures to dramatically improve their resilience.
- **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**: 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 thwarts the problem. CIS Re-configuration is the utmost mechanism for their survivability.

This multi-disciplinary approach allows DESEREC to respond efficiently to the three families of incidents which can occur on a critical system: **Attacks from the outside**, **Intrinsic failures** and **Misbehaviour or malicious internal use**. The DESEREC framework will gather information from multiple sources in order to analyse and decide appropriate reaction, as illustrated below (the figure below introduces the main functions of DESEREC).

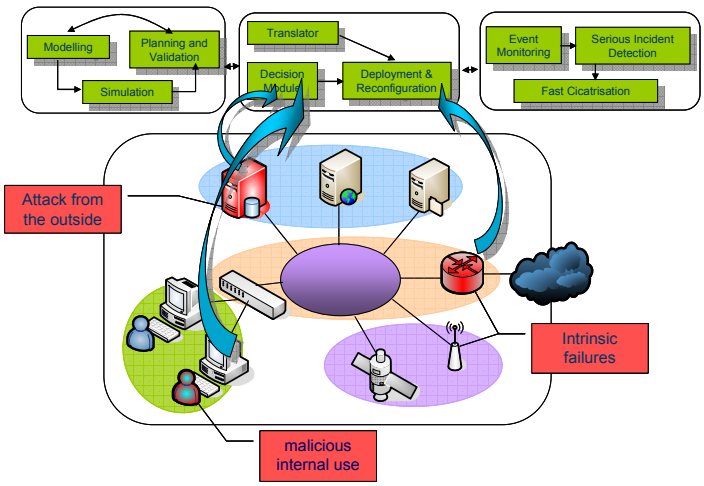



**Figure 1. CIS under DESEREC monitoring and control**

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:

- **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 overall system (i.e. through computer aided reactions) in order to maintain the critical business services. The prime objective of DESEREC is to increase the availability of the services provided to end-users of the CIS giving the priority to the critical ones (from the stand point of the service provider).
- **Some hours** to build a new configuration optimised to resist to a new situation and validated through modelling and simulation.

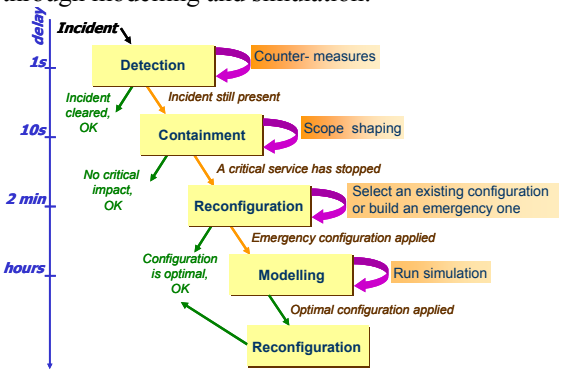



**Figure 2. DESEREC Reaction loops**

## Objective

DESEREC aims at providing methods and tools to monitor, analyse, design, model, simulate, and plan the optimised configurations of CIS supporting mission-critical business services. DESEREC improves risk management as well as business services dependability and survivability with reconfiguration methods and automated support tools for incident detection and reaction on different time scales.

The DESEREC framework may be deployed over *existing* and *new* mission-critical Communications and Information Systems with minimum CIS adaptations. The DESEREC framework will increase the dependability of *CIS* by means of an architecture based on the following tiers:

- **Planning**: Modelling, simulation, and utility tools with a suitable approach to plan optimal operational configurations, detection and reactions scenarios through modelling and simulation of critical system and their potential threats. They allow to define coherent and homogeneous operational mode and define the efficient response to anticipated incident, the process to face unexpected ones and the method to restore an optimal usage of the system after a switch to a degraded configuration.
- **Detection and Prevention**: Distributed, multi-technology sensors and a set of detection mechanisms to detect all kind of incident that can occur in the system. They ensure fast detection of elementary incidents and in addition, elaborate the detection of distributed incident from a combination of apparently unrelated events or from an abnormal behaviour in the system.
- **Reaction**: a framework for computer-aided and automated counter-measures initiatives in order to respond in a quick and appropriate way to a large range of incidents. These responses include the identification of the scope of a given incident, the best approach to isolate the "suspected" devices to avoid propagation of threats or a cascading effect.

# Training workshop, "architecture, modelling, and tools"

by *Tomasz Walkowiak* and Dariusz Caban, Wroclaw University of Technology (PWR)

The DESEREC Consortium held its first training workshop "Architecture, Modelling and Tools for increasing dependability and security of Information Systems" at Wroclaw University of Technology in Poland on 25-26 September, 2006. It was a very successful event with 50 participations: representatives of the partner institutions, prospective end-users and academia.

The workshop was organized in 3 sessions. Session 1 focused on the project aims, analyzed testbeds and foreseen architectures. It reflected the current state of work done in the project, especially on the reconfigurable architecture. Session 2 was dedicated to the methodologies proposed for managing dependability: modelling of systems and policies. Their integration within the system is a major project challenge. Session 3 presented some existing tools for modelling, simulating and monitoring, as currently used by the project partners.

*Session 1. User scenarios, architecture*
The objectives of DESEREC project (Benoit Bruyere), User scenarios, requirements, questionnaire (Francisco Hernández Gómez), Currently foreseen architecture (Maximilian List).

*Session 2. System modelling*
Modelling for security and dependability (Marco Aime), Introduction to modelling languages (Antonio F. Gómez Skarmeta), System modelling (Marco Aime), Policy modelling (Gregorio Martínez Pérez).

*Optional session 3. Tools presentation*
VIATRA2 model transformation framework (Imre Kocsis), SIMICS (Karl Mayer), NERD (Sander Degen).

The presentations were recorded to produce computer based training courseware, for distribution among the partners and prospective DESEREC end-users.

Further details of the workshop are available at the DESEREC Web pages http://www.deserec.eu.

# User scenarios

by Pedro Lopez,
GMV Soluciones Globales Internet (SGI)

The aim of the user scenarios is to analyse real world business cases obtain useful information in order to design / build DESEREC. This information is used to identify functional, performance, security and other requirements. A user scenario consists of:
- A set of business services and detailed descriptions of them,
- Service maps: ICT infrastructure (HW & SW) supporting the services,
- Business, applications and system dependencies, constraints and requirements,
- Monitoring systems (sources of events),
- A set of hypothetical hazards on ITC elements (HW/SW failures, attacks, …),
- A list of possible reactions to the hazards.

User scenarios also provide a test environment where DESEREC prototype will be demonstrated. Such environments are based on a test-bed or framework containing an isolated ICT infrastructure that emulates a production environment. At the same time, the business cases defined within user scenarios will be used as a part of the verification of the DESEREC prototype at the end of the project.

The services provided by the RENFE user scenario are the following:
- Web Information,
- Internet Ticket Selling,
- Timetable querying.

From OTE (Hellenic Telecommunications Organization) services described by the user scenarios are:
- Fast Internet Access,
- IPTV Services: Video on Demand and Video Broadcasting.

# Modelling requirements and system modelling

by Antonio Lioy,
Politecnico di Torino (Polito)

Evaluation of security and dependability requires the ability to model the target system according to several different views, as well as to model the attacks, faults and the behaviour of the basic components, both in normal and abnormal conditions.
First of all, business service requirements should be given, describing the expected functionality, protection and performance level (e.g. web-based booking service with privacy and integrity protection, capable of 100 bookings/minute). This is needed to check if a given system configuration partly or fully matches the requirements.
Each business service must then be decomposed into its basic ICT services (e.g. web front-end, database back-end, and authentication server); the dependencies between these services must be given.
As ICT services are implemented by computational nodes, network appliances and communication links, these elements must be described as well, along with the mapping of the ICT services onto them. To avoid duplication of efforts, a library of well-known elements should be available (for example for standard hardware and software) along with some constraints, such as the fact that an ASP application requires the IIS web server.
In order to evaluate the functionality of the system and its performance, proper behavioural models of the basic elements must be supplied, closely tied to the tools used for the analysis (e.g. network-level or system-level simulators). Additionally, prediction of abnormal system behaviour is possible only with proper models for attacks, faults and their propagation.
Finally, risk analysis requires knowledge of the known vulnerabilities (that could be provided by different public database) and of the system configuration, including not only the ICT aspects but also other important information such as physical location and electric power distribution.
It is also important that the requirements set forth at the business level be automatically transformed into requirements at the other levels, so that the evaluation results can be compared with the expect behaviour.
DESEREC has analysed several proposals for system and service modelling, including plain UML, CIM, MS SDM, SysML, BPEL, WS-CDL, and WSMO. As a result, DESEREC has drawn a system modelling framework spanning three views:
- the "service view" describes business services, including orchestration of service components, along with the global requirements and policies affecting the services

- the "resource view" describes system elements providing computational, storage and communication resources, along with their interconnection (topology), possibly at different levels of granularity (e.g. sub-networks) to cope with the complexity of large ICT systems

- the "allocation view" describes how resources are use to support business service delivery, including the transformation of global requirements and policies into sub-system and element configuration directives

# Modelling Languages

by Daniel Martinez,
University of Murcia (UMU)

DESEREC has analyzed a number of state-of-the-art alternatives for its modelling needs, which include system and rules models. This analysis has covered many different languages and notations, including the Unified Model of Dependability (UMD), the Unified Modelling Language (UML) and the Common Information Model (CIM), among others. The advantages and drawbacks of each of them have been reviewed, in order to find the most appropriate candidate.
The analysis has found that the Common Information Model (CIM) is the most suitable choice for the overall modelling tasks in DESEREC. CIM, developed by the Distributed Management Task Force (DMTF, http://www.dmtf.org), is a hierarchical, object-oriented data model with powerful expression and extension capabilities.
The extensibility of CIM has allowed to build over it two especially remarkable modelling languages: SDL (System Description Language) and SPL (Security Policy Language). They offer XML-based notations for representing managed system elements and policy rules, respectively. These languages provide DESEREC with a powerful framework for allowing system administrators to model their information systems, along with the rules that must govern its operation and reaction to failures. The configuration of system components, their monitoring and their resilient reconfiguration can be then automatically performed by the intelligent DESEREC engine.

# Policy Modelling

by Daniel Martinez,
University of Murcia (UMU)

The implementation of dependability in DESEREC relies on the abstract representation of rules, which define how the managed system must react when incidents happen. Among existing languages for modelling such rules, the SPL notation (Security Policies Language) was found the best existing candidate. Based on the powerful XML language, SPL allows describing abstract policy rules as extensible pieces of information, each of which defines a link from a set of conditions to a set of actions. The main features of SPL are:
- It is vendor and device independent,
- It initially supports filtering, authentication, authorization, channel protection and operational policies, but can be extended to represent additional types,
- It provides an XML schema for each type of policy, allowing automatic validation.

In DESEREC two main types of policy rules are modelled with SPL:
- Configuration policies, which specify how the system should work. They are translated into full configurations.
- Reaction policies, which specify how to monitor the system for incidents, and what to do if they happen.

This overall policy framework provides DESEREC with a flexible and extensible solution for system management, enabling it to both configure itself and react automatically.

**The following articles present possible tools which may be used within the DESEREC solution.**

# VIATRA2

By Imre Kocsis,
Budapest University of Technology (BUTE)

Model transformation based tool and data integration rapidly gains popularity in architecting system development workflows and related verification and validation activities. Using high-level, declarative specification of the notions of the source and target domains and the transformation steps between them significantly reduces development and maintenance costs.

VIATRA2 - a general purpose, declarative graph transformation based model transformation framework developed at the Fault Tolerant System Research Group of BUTE - acts as a 'modelware' framework: it supports engineering model to engineering model and engineering model to mathematical domain transformations, code generation and format conversion. VIATRA2 is already used in numerous R&D efforts, including FP6 projects.

Besides being applicable for workflow integration, VIATRA2 offers a platform for the consistent, metamodel-level formulation of general incident and fault mechanisms and propagation properties. A new field of research, the automated enrichment of engineering models with domain specific knowledge promises a knowledge base assisted support of verification and validation and the enablement of the model driven supervisory architecture design of large-scale, general purpose IT systems.

VIATRA2 is an Eclipse-based framework; its extension facilities are based on those of this widely known platform, making domain-specific customization and embedding into other Eclipse-based solutions well supported tasks.

# SIMICS

by Wolfgang Fritsche
Industrieanlagen-Betriebsgesellschaft (IABG)

SIMICS represents a full system simulator, which allows simulating distributed, net-worked Information Systems. For this purpose SIMICS is able to model hardware components like processors, their registers, I/O chips or bus systems, as well as different networks links, like Ethernet, ATM, Fibre-Channel, or Packet-over-Sonet. It then uses these modelled hardware components to build for example host systems, routers or servers, and interconnect these with the modelled network links. As SIMICS models the underlying hardware as close as possible, it is possible to run complete operating systems, network stacks or even original binary application software, without any modifications compared to the real environment. This provides the basis for per-forming simulations, in which the experimental setup is closely modelled to the real world.

From its internal design, SIMICS is event-driven, but for the sake of performance, processors are treated specially to allow optimizations where possible. Peripheral devices and I/O are working in the simulation on a transaction style. For network packets this means that always the complete packet is transmitted in a single action, not byte by byte.

Within DESEREC, SIMICS is expected to be used for simulation of a subset of the whole CIS when needed.

# NERD

by Peter Albeda
Netherlands Organisation for Applied Scientific Research (TNO)

NERD stands for Network Emergency Responder and Detection system. Within the DESEREC project NERD is expected to be integrated in the fast detection module.

NERD is an open source security monitoring tool, that has the following functionality:
- The tool collects NetFlow data that is being sent to the NERD server by the routers in the network.
- NERD stores the collected NetFlow data in files. The most recent data is kept in memory to speed-up the real-time analysis of data by limiting disk processing.
- The data files (in memory) are used by NERD to process "real-time" analysis based on flexibly configurable rules (see paragraph on rules). This real-time analysis generates alarms on the user interface.
- The data files are also used by NERD to execute user-initiated post-analysis of the data. A user can directly start a "basic" analysis from an alarm. Each post analysis generates a graph that can be clicked to see the raw data.
- Both the real-time and post analysis are defined with clusters and filters. These clusters and filters can be predefined and stored.
- NERD provides a web based interface to its users.

NERD was developed to be used in large backbone networks. More information on NERD (and the software) can be found on http://www.nerdd.org.