DESEREC
Dependability and Security by Enhanced Reconfigurability

An ICT for Trust and Security research project addressing the dependability of Information systems

Dependability concerns

- The everyday life of European citizens relies on critical activities supported by networked Information Systems (I.S.):
  - Communications (telephone, Internet)
  - Energy & fluids (electricity, gas, water)
  - Transportation (railways, airlines, road)
  - Health and emergency response
  - e-Government

- So far, limited taken actions let these I.S.:
  - not failure-proof enough to face:
    - Software & hardware faults
    - Malicious actions: intrusion, virus
  - with poor self-healing capability
  - and therefore sensitive to cascading effects
  - suffering long recovery time

- The DESEREC project aims to leverage those capabilities in new and existing Information Systems
**Why DESEREC?**

**The picture**
- Administrators are swamped by information of inappropriate level
- Most of the decision are taken short-term, with poor mid-term capability to arbitrate between business services with different criticality
- No synthetic view on dependability is provided

**The proposed approach**
- Provide information and interaction at service level instead of component level for day-to-day management
- Bring high-level management capabilities giving the ability to react appropriately upon errors/failures to maintain critical services
- Support mid-term strategy with planning and simulation tools enabling a proactive management of performance and dependability

---

**The 3-tiered approach proposed by DESEREC**

**First objective – Detect & Prevent**
- Detect proactively incident and potential fault
- Keep as much as possible every failure local
  - Contain the incident: isolate the compromised area

**Second objective - React**
- Sustain or quickly resume the critical applications
- Reallocate resources used by less critical ones

**Third objective – Plan**
- Reallocate optimally the resources to recover the full range of services
- Validate the configurations by simulation
**DESEREC - A multi-tiered response**

- Incident
- Detection
- Containment
- Reconfiguration
- Modelling
- Reconfiguration

**High level functional blocks**

Management of mission-critical CIS via a model-based solution organised around three-tier reaction loop

- Planning (central)
  - Modelling
  - Simulation
  - Operational Planning

- Reconfiguration (global)
  - Decision
  - Deployment
  - Reconfiguration
  - Translation

- Self-Healing (local, fast reaction)
  - Event Monitoring
  - Serious Incident Detection
  - Fast Reaction

**Mission-Critical Information System**
CIS seen as a cluster of molecules

- Introduce the molecule and multiple functional plans/views

---

DESEREC Approach to resilience

- Optimizing the resilience of the Information System at the business service level
- The improvement of the resilience is achieved by optimizing the use of the available resources through reconfiguration
- Resilience engineering is one of the objective of DESEREC providing a learning mechanism for improving proactive reaction to incidents