# ReSIST: Resilience for Survivability in IST

## A European Network of Excellence




## Partners

| | |
|---|---|
| LAAS-CNRS (coordinator) | France |
| Budapest University of Technology and Economics | Hungary |
| City University | UK |
| Technische Universität Darmstadt | Germany |
| Deep Blue Srl | Italy |
| Institut Eurécom | France |
| France Telecom Recherche et Développement | France |
| IBM Research GmbH | Switzerland |
| Université de Rennes 1 | France |
| Université de Toulouse III | France |
| Vytautas Magnus University | Lithuania |
| Fundação da Faculdade de Ciencas da Universidade de Lisboa | Portugal |
| University of Newcastle upon Tyne | UK |
| Universita di Pisa | Italy |
| QinetiQ Limited | UK |
| Università degli studi di Roma "La Sapienza" | Italy |
| Universität Ulm | Germany |
| University of Southampton | UK |

## Summary

ReSIST is an NoE that addresses the strategic objective "Towards a global dependability and security framework" of the European Union Work Programme, and responds to the stated "need for resilience, self-healing, dynamic content and volatile environments".

It integrates leading researchers active in the multidisciplinary domains of Dependability, Security, and Human Factors, in order that Europe will have a well-focused coherent set of research activities aimed at ensuring that future "ubiquitous computing systems", the immense systems of ever-evolving networks of computers and mobile devices which are needed to support and provide Ambient Intelligence (AmI), have the necessary resilience and survivability, despite any residual development and physical faults, interaction mistakes, or malicious attacks and disruptions.

The objectives of the Network are:

1) *Integration* of teams of researchers so that the fundamental topics concerning scalably resilient ubiquitous systems are addressed by *a critical mass* of co-operative, multi-disciplinary research.
2) Identification, in an international context, of the key *research directions (both technical and socio-technical)* induced on the supporting ubiquitous systems by the requirement for trust and confidence in AmI.
3) Production of significant *research results (concepts, models, policies, algorithms, mechanisms)* that pave the way for scalably resilient ubiquitous systems.
4) Promotion and propagation of a *resilience culture* in university curricula and in engineering best practices.

## Contract information

Contract Number: 026764

Funding for three years: MEuro 4.5

Coordinator

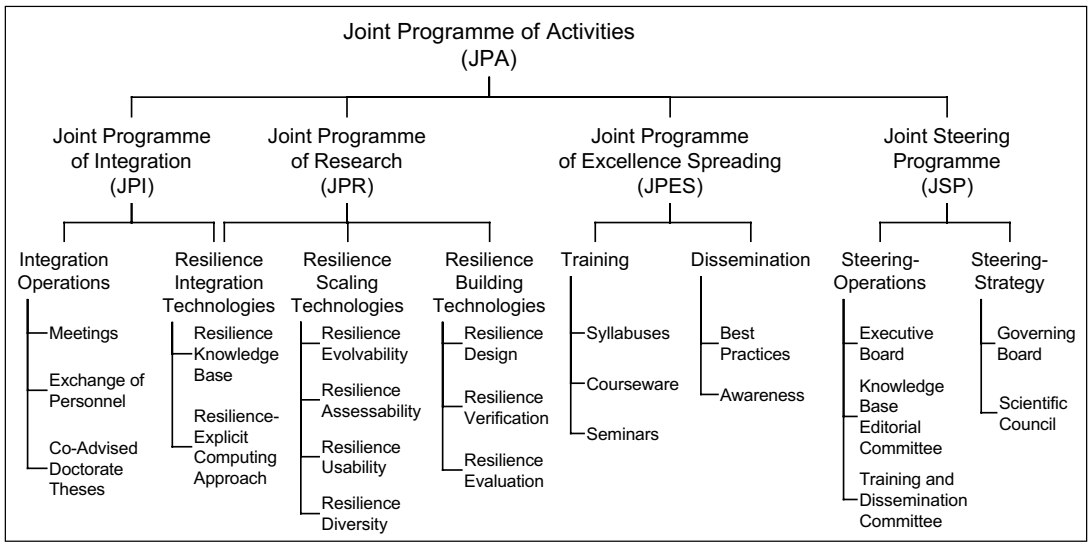
Dr Jean-Claude Laprie
LAAS-CNRS
7 Avenue Colonel Roche, 31077 Toulouse, France
e-mail: laprie@laas.fr - Phone: +33 5 61 33 78 85 - Fax: +33 5 61 33 64 11

## Rationale

The current state-of-knowledge and state-of-the-art reasonably enable the construction and operation of critical systems, be they safety-critical (e.g., avionics, railway signalling, nuclear control) or availability-critical (e.g., back-end servers for transaction processing). The situation drastically worsens when considering large, networked, evolving, systems either fixed or mobile, with demanding requirements driven by their domain of application. There is statistical evidence that these emerging systems suffer from a significant drop in dependability and security in comparison with the former systems. There is thus a *dependability and security gap* opening in front of us that, if not filled, will endanger the very basis and advent of Ambient Intelligence (AmI).

Filling the gap clearly needs dependability and security technologies to *scale up*, in order to counteract the two main drivers of the creation and widening of the gap: complexity and cost pressure.

## Joint Programme of Activities




At the heart of the JPA is the JPR. Two main steps will take place: first according to the basic resilience building technologies, then according to the resilience scaling technologies.

The first step will already be integrative, in bringing together researchers who are mostly active in separate domains according to the types of threats that are considered: accidental failures, malicious attacks, human-system interaction mistakes. To facilitate this first level of integration, a) resilience design activities will emphasise run-time surveillance and service continuity, including in-depth defences, b) resilience verification will focus on the defence mechanisms, and c) resilience evaluation will aim at unified measures with respect to accidental and malicious threats.

In the second step, research activities will be re-structured and re-shaped according to the resilience scaling technologies. Examples of challenges that such re-structuring and re-shaping will take up are:

- for evolvability, to be able to adapt to changing environments and threats,
- for assessability, to move from off-line, pre-deployment assessment to continuous automated and operational assessment,
- for usability, to reconcile the conflicting roles of humans as contributors to resilience and threats that resilience must tolerate,
- for diversity, to take advantage of diversity in order to prevent some vulnerabilities from becoming single points of failure.

This move from resilience building technologies towards resilience scaling technologies will be accompanied and facilitated by the resilience integration technologies:

- The knowledge-base will incorporate a representation of the relationships amongst the various dependability and security terms, i.e. a dependability and security ontology
- The resilience-explicit computing approach will involve creating and manipulating dependability and security meta-data.

The logic of the JPR integration is schematically summarised below.