Resilience for Survivability in IST
– ReSIST –

A European Network of Excellence
– Summary –

Abstract

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

It will integrate 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.

Partners

ReSIST’s partners are:

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

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, i.e., *ubiquitous systems*. 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. Coping with complexity and cost certainly demands significant progress in the rigorous design of the functionalities provided by the information infrastructures. However, the interplay between: a) rigorous design on one hand, and b) complexity and cost on the other, will inevitably lead to residual development defects, vulnerabilities, and room for interaction mistakes. This has been true throughout the history of computing, and will be all the more true in the future. We thus deliberately focus on complementary approaches aimed at tolerating the various classes of threats that can lead to system failures. The desired outcome is to provide pervasive information infrastructures with *scalable resilience* for survivability in direct support of the emerging pervasiveness of computing systems.

Complexity growth under cost pressure results from (drastic) changes that can be functional, environmental and technological. Examples of such changes are: a) growth of systems as demand increases, b) merging of systems in company acquisitions or coupling of systems in military coalitions, c) interactions between systems of differing natures (e.g., large-scale information infrastructure on the one hand and networks of sensors on the other), d) dynamically changing systems (e.g., spontaneous, or 'ad-hoc', networks of mobile nodes and sensors), e) the ever-evolving and growing problem of attacks both by amateur hackers and by professional criminals. Accommodating such functional, environmental and technological changes at a satisfactory level of dependability and security induces the need for scalability, which in turn drives the requirement for resilience policies, algorithms and mechanisms to be *extensible*, *composable*, *adaptive*, mutually *compatible,* and *complete* with respect to the assumed threats. The satisfaction of these scalability properties clearly requires that the resilience policies, algorithms and mechanisms be *evolvable*. However, evolvability has to be accompanied, and ideally, guided by a) *assessment* of the effectiveness of resilience, b) assurance of its *usability* (from the viewpoints both of users and of administrators). Finally, such complex systems are naturally heterogeneous and diverse; this can be exploited to prevent vulnerabilities from becoming single points of failure. From the preceding reasoning, we can conclude that dependability and security scalability needs the emergence of what can be termed as *resilience scaling technologies* that should guide both system design and operation: *evolvability, assessability, usability, diversity*. These resilience-scaling technologies naturally draw upon the more classical resilience-building technologies: *resilience design, resilience evaluation and resilience verification*. The preceding course of reasoning is illustrated by Figure 1.

All of the various classes of threats have to be considered in this pursuit of scalable resilience: development or physical accidental faults, malicious attacks, interaction mistakes. Indeed, those classes of threats are inter-related, e.g.: a) attacks are aimed directly at vulnerabilities, that are mostly of an accidental nature (either residual defects, including flaws in security enforcement, or physical malfunctions), and some vulnerabilities are unavoidable because of usability constraints, b) human-interaction mistakes can often be traced to

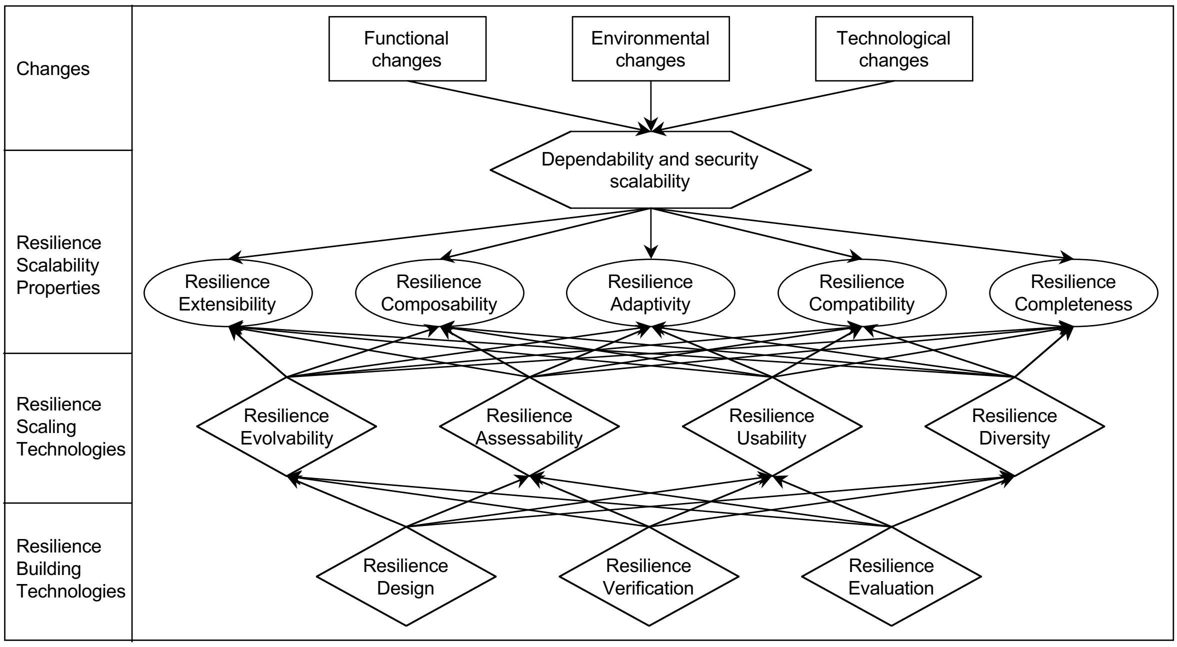


Figure 1 - Scalable resilience

development defects. However, interest in physical malfunctions in ReSIST will be focused on problems that go beyond the current state-of-the-art, e.g., new modalities of malfunctioning in emerging technologies (such as sensor networks), or the role of physical malfunctions in creating vulnerability. It has to be stressed that the classes of threats are more than inputs for scalability issues, as the environmental and technological changes induce *changing threats*, e.g., accrued importance of a) malicious attacks that go along with openness, or of b) configuration mistakes that emerge as a major source of failures as system complexity increases.

The future large, networked, evolving systems constituting complex information infrastructures —perhaps involving everything from super-computers and huge server "farms" to myriads of small mobile computers and tiny embedded devices— are the types of system at which ReSIST is particularly targeted. Such systems are in fact the dawning of the ubiquitous systems that will support Ambient Intelligence. We will use this term **ubiquitous systems** as a shorthand for portraying the ReSIST target systems and services, for which we aim to provide *scalably resilient policies, algorithms and mechanisms*.

Joint Programme of Activities

The components of the Joint Programme of Activities (JPA) are given by Figure 2.

In addition to the four *resilience scaling technologies* (evolvability, assessability, usability, diversity) and the three basic *resilience building technologies* (design, verification and evaluation), the JPR comprises three *resilience integration technologies*: a resilience knowledge base, a resilience-explicit computing approach, and a resilience ontology. These resilience integration technologies orchestrate orderly progress and integration, and constitute a unique feature of ReSIST: research supporting and favouring integration. Exploitation of the results obtained in order to promote a resilience culture is achieved via *training* and *dissemination*. The multi-dimensional synergies necessary for carrying out the above-identified activities are supported by *integration operations*. Leadership and steering of the network will be delivered at the *operational* and *strategic* levels.

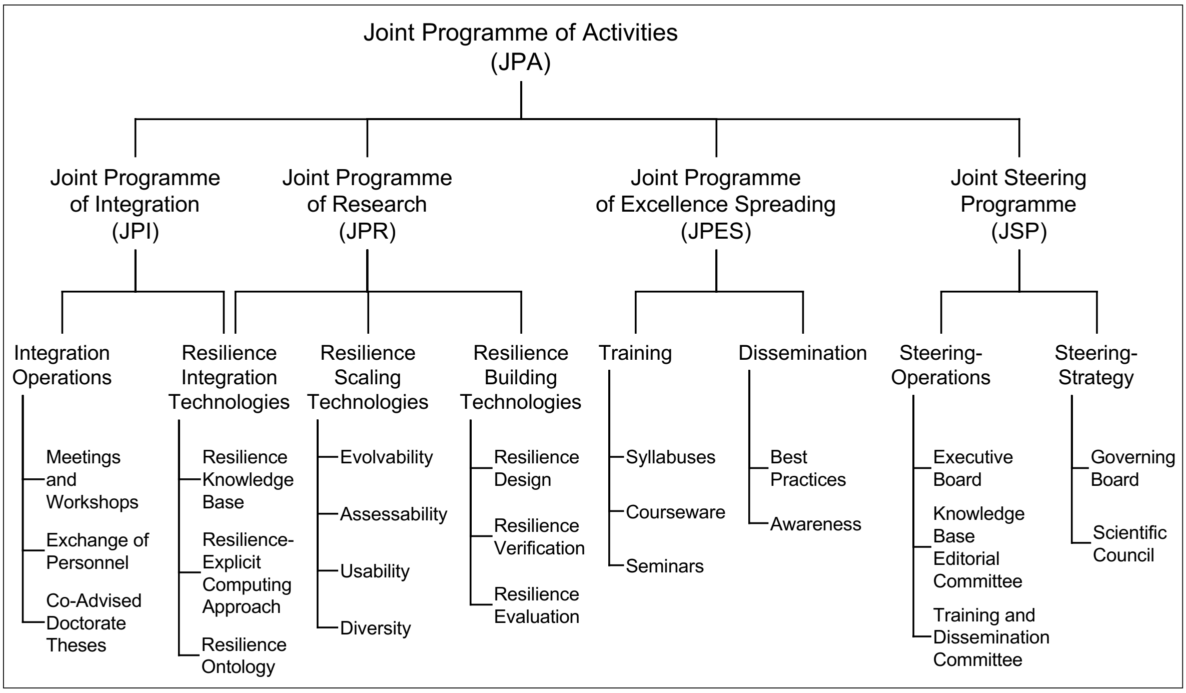

Joint Programme of Activities (JPA)
Joint Programme of Integration (JPI)
Joint Programme of Research (JPR)
Joint Programme of Excellence Spreading (JPES)
Joint Steering Programme (JSP)
Integration Operations
Resilience Integration Technologies
Resilience Scaling Technologies
Resilience Building Technologies
Training
Dissemination
Steering-Operations
Steering-Strategy
Meetings and Workshops
Exchange of Personnel
Co-Advised Doctorate Theses
Resilience Knowledge Base
Resilience-Explicit Computing Approach
Resilience Ontology
Evolvability
Assessability
Usability
Diversity
Resilience Design
Resilience Verification
Resilience Evaluation
Syllabuses
Courseware
Seminars
Best Practices
Awareness
Executive Board
Knowledge Base Editorial Committee
Training and Dissemination Committee
Governing Board
Scientific Council

Figure 2 - JPA components

The logic of the JPR integration is schematically summarised by Figure 3.

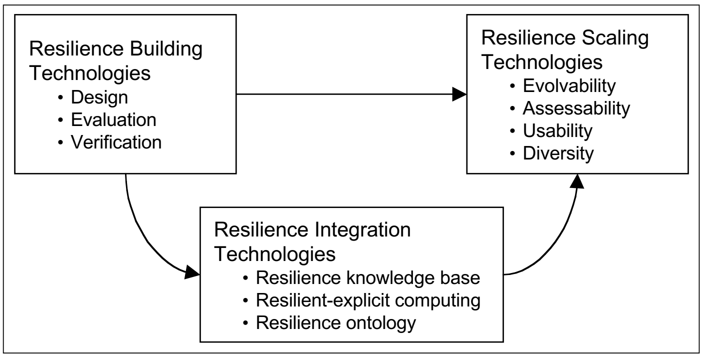

Resilience Building Technologies
• Design
• Evaluation
• Verification
Resilience Scaling Technologies
• Evolvability
• Assessability
• Usability
• Diversity
Resilience Integration Technologies
• Resilience knowledge base
• Resilient-explicit computing
• Resilience ontology

Figure 3 - JPR integration logic

ReSIST activity falls into four workpackages:

- WP0: Integration Management;
- WP1: Resilience Integration Technologies;
- WP2: Resilience building and scaling technologies;
- WP3: Training and Dissemination.

The relationship between the components of the JPA and the workpackages is given by Figure 4.

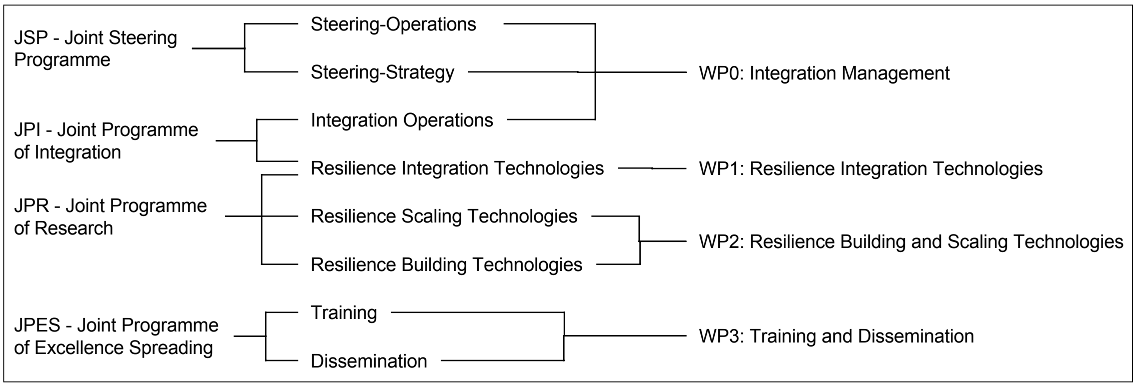

JSP - Joint Steering Programme
Steering-Operations
Steering-Strategy
WP0: Integration Management
JPI - Joint Programme of Integration
Integration Operations
Resilience Integration Technologies
WP1: Resilience Integration Technologies
JPR - Joint Programme of Research
Resilience Scaling Technologies
Resilience Building Technologies
WP2: Resilience Building and Scaling Technologies
JPES - Joint Programme of Excellence Spreading
Training
Dissemination
WP3: Training and Dissemination

Figure 4 - Relationship between the components of the JPA and the workpackages

Figure 5 illustrates the relationship between the workpackages and the organisational entities of the Network.

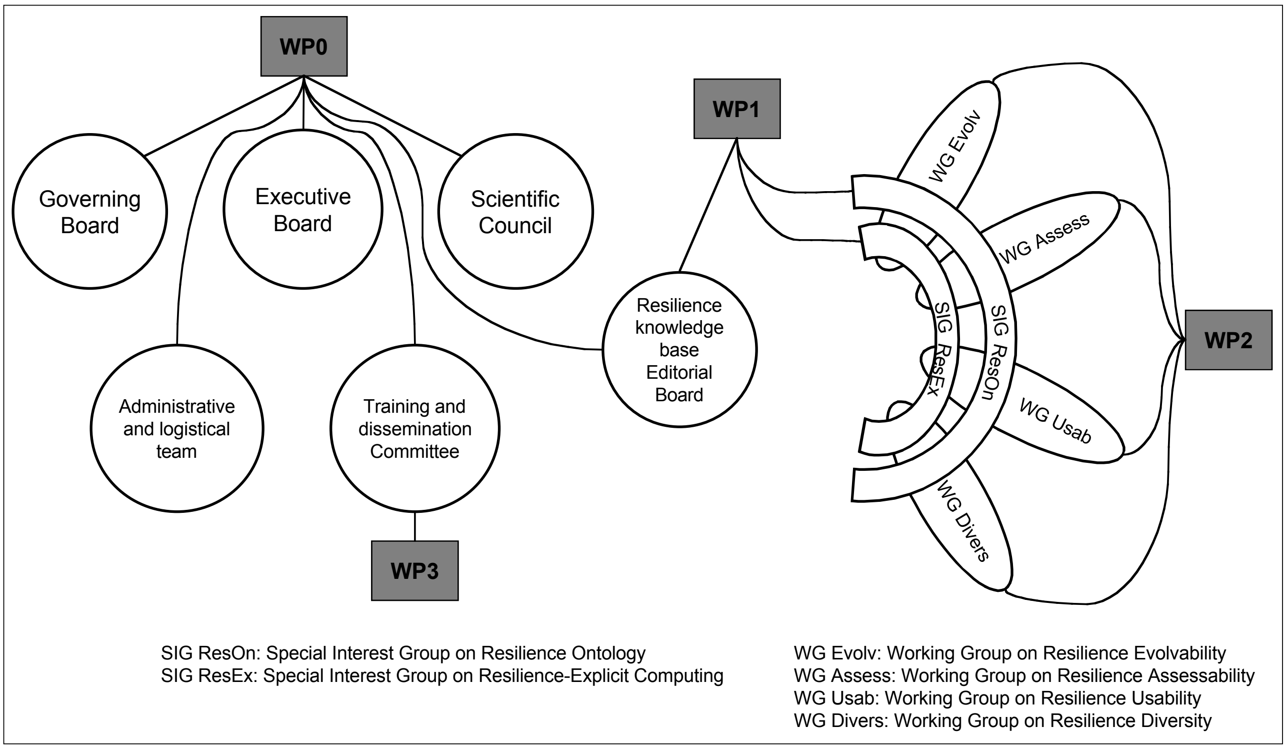

WP0
Governing Board
Executive Board
Scientific Council
Administrative and logistical team
Training and dissemination Committee
WP3
WP1
Resilience knowledge base Editorial Board
WG Evolv
WG Assess
SIG ResEx
SIG ResOn
WG Usab
WG Divers
WP2
SIG ResOn: Special Interest Group on Resilience Ontology
SIG ResEx: Special Interest Group on Resilience-Explicit Computing
WG Evolv: Working Group on Resilience Evolvability
WG Assess: Working Group on Resilience Assessability
WG Usab: Working Group on Resilience Usability
WG Divers: Working Group on Resilience Diversity

Figure 5 - Workpackages and organisational entities

First year achievements

The two major achievements of the first year of activity have been the production of a) the State of Knowledge in Resilience-Building Technologies, and of b) a prototype of the Resilience Knowledge Base.

The work for producing the State of Knowledge in Resilience-Building Technologies has been divided among five working groups (each with active participation from the ReSIST partners that work in the corresponding research area) dealing with different aspects of resilience building and the corresponding subdisciplinary areas. The document is therefore made up of five parts, each produced by one of the working groups:

- Resilience architecting and implementation paradigms
- Resilience algorithms and mechanisms
- Resilient socio-technical systems
- Resilience evaluation

- Resilience verification

This state of knowledge document is co-authored by 66 researchers and doctorate students. Its production has included an extensive review process, with an emphasis on the viewpoint of scientists who are not specialists of the sub-disciplines covered, so that the document can serve as an introduction to the problems relevant for ReSIST in the area covered, besides documenting the advanced results produced by ReSIST members. The document is to serve as a basis for the development of ReSIST's research roadmap and a stepping stone in the process of integration within the ReSIST network. In pursuing this internal goal, the five working groups have also produced substantial surveys that will be useful for the community at large.

The Resilience Knowledge Base (RKB) is intended to provide a semantic web environment for effective access to a body of knowledge on resilience concepts, methods and tools. The current prototype RKB contains contains 40 millions basic facts, from three classes of information:

- resilience data captured from each partner's information resources, including research interest details and courseware,
- external sources including CORDIS (EU research projects), NSF (US research projects), Citeseer, and the ACM (both on publications and the RISKS index of "Computer-related Risks to the Public"),
- two ontologies, on Dependability and Security, and on Systems concepts, together with associated glossary text.

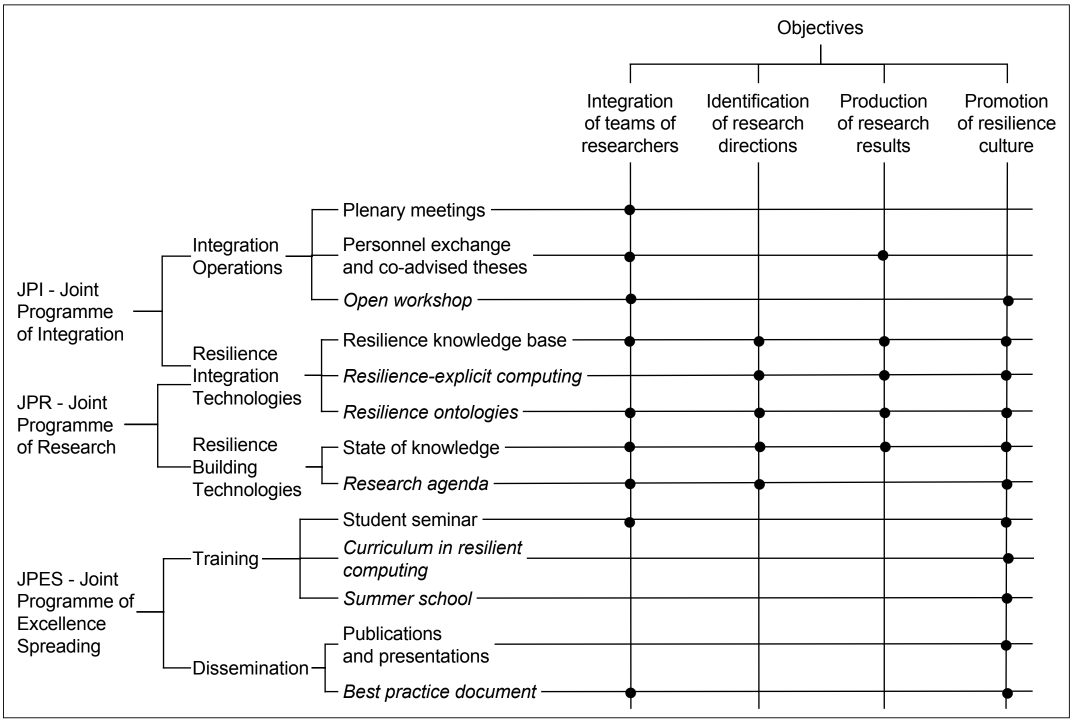
Accessing information in the RKB enables relationships between entities to be displayed in the form of Communities of Practice. The prototype RKB was reviewed by all ReSIST partners, and updated in response to feedback.

Besides the two achievements addressed so far, a number of significant events and advances have taken place during the first year of activity:

- Gathering of 101 ReSIST participants to the initial plenary meeting of the network (held at LAAS, on 21-23 March), that enabled: i) first direct contacts between all teams from the Network partners, ii) start of community building, iii) elaboration of the first deliverables.
- Holding of the Student Seminar (at Centro Studi "I Cappuccini", San Miniato, Italy, on 5-7 September). Attended by 32 Doctorate Students and 15 Senior Members, the seminar enabled fostering connection among young researchers, and in depth discussion of the topics that are object of research, through Doctorate activity, on resilient computing.
- Exchanging personnel for at least one month stays, by 5 ReSIST members, totalling 17 months of stay.
- Co-advising of 4 doctorate theses.
- Producing 6 articles in scientific journals, and presenting 55 communications whose texts appear in proceedings.
- Presenting ReSIST at 11 national, European and international events.

In addition to the above facts, ground work has been performed on the preparation of a) coming events, such as the Open Workshop (21-22 March 2007 in Budapest) and the Summer School (24-28 September 2007 in Porquerolles island) or b) deliverable production, such as the Research Agenda (that will constitute a deliverable due in June 2007, entitled: "From Resilience-Building to Resilience-Scaling Technologies: Directions"), the Resilience-Explicit Computing approach, the Resilience Ontology, the Best Practice Document, the Curriculum in Resilient Computing.

Figure 6 shows the contribution of the ReSIST activities, according to components of the Joint Programme of Activities, to the objectives. Activities in italics are those that have been under preparation during the first year, and that will produce significant achievements during the second year.



Objectives
JPI - Joint Programme of Integration
JPR - Joint Programme of Research
JPES - Joint Programme of Excellence Spreading
Integration Operations
Resilience Integration Technologies
Resilience Building Technologies
Training
Dissemination

	Integration of teams of researchers	Identification of research directions	Production of research results	Promotion of resilience culture
Plenary meetings	●			
Personnel exchange and co-advised theses	●		●	
Open workshop	●			●
Resilience knowledge base	●	●	●	●
Resilience-explicit computing		●	●	●
Resilience ontologies	●	●	●	●
State of knowledge	●	●	●	●
Research agenda	●	●		●
Student seminar	●			●
Curriculum in resilient computing				●
Summer school				●
Publications and presentations				●
Best practice document	●			●

Figure 6 - Contribution of the ReSIST activities to the objectives