Resilient Computing: a multi-disciplinary MSc Curriculum

Luca Simoncini
Professor of Computer Engineering
Faculty of Engineering,
University of Pisa, Italy

On the term Resilience

The term resilience has been used in many fields and, as a property, two threads can be identified: a) in social psychology, where it is about elasticity, spirit, resource and good mood, and b) and in material science, where it is about robustness and elasticity.

The notion of resilience has then been elaborated:

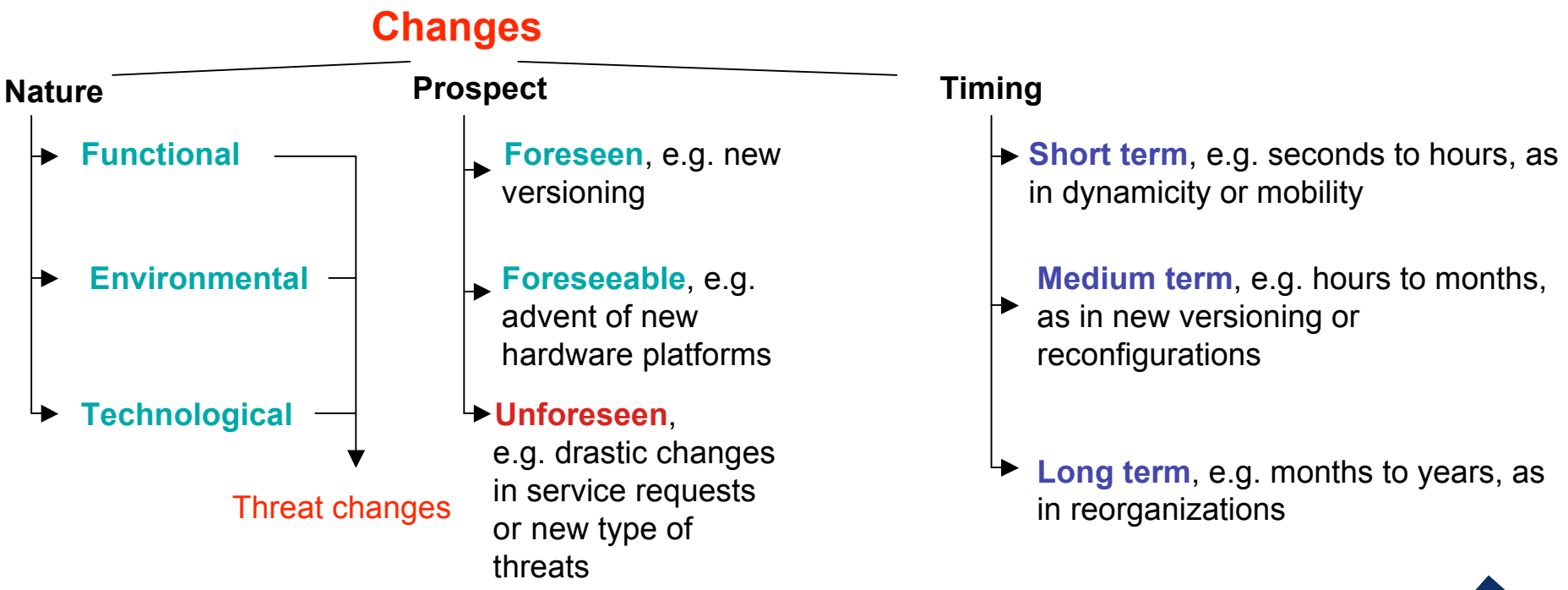
- In child psychology and psychiatry, referring to living and developing successfully when facing adversity;
- In ecology, referring to moving from a stability domain to another one under the influence of disturbances;
- In business, referring to the capacity to reinvent a business model before circumstances force to;
- In industrial safety, referring to anticipating risk changes before damage occurrence.

A common point to the above senses of the notion of resilience is the ability to successfully accommodate unforeseen environmental perturbations or disturbances.

Resilient Computing

Resilience (for computing systems and information infrastructures):

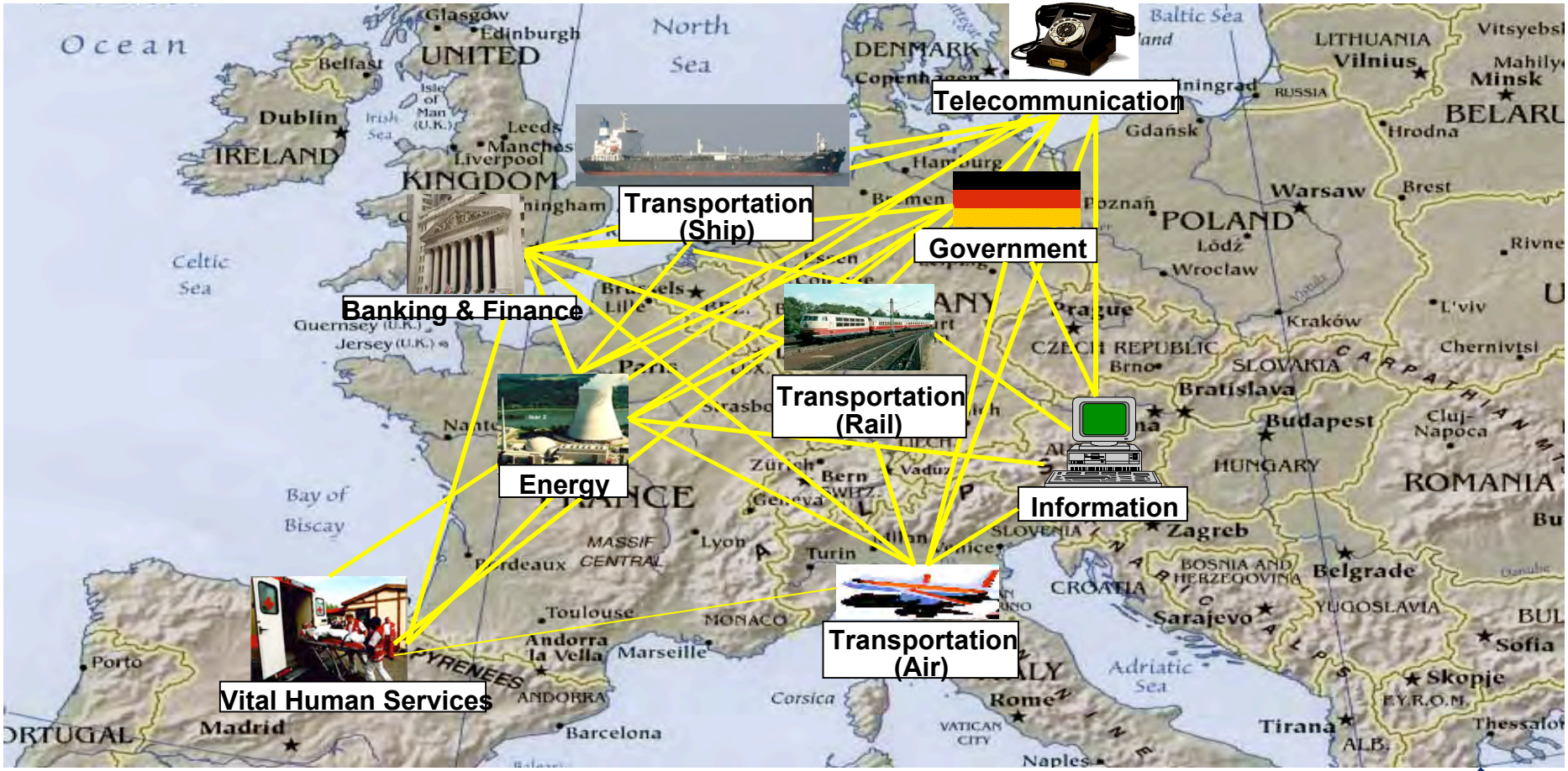
the persistence of service delivery that can justifiably be trusted, when facing changes



Some examples of recent resilience problems

- **The French Insurer's Association estimates the yearly cost of computer failures to be 2 B Euros, of which slightly more than half is due to malicious faults (e.g. by hackers and corrupt insiders)**
  https://www.clusif.asso.fr/fr/production/sinistralite/index.asp
- **"Nearly 10 million people in the US suffered from some kind of on-line fraud last year … the total cost was $1.2bn"**
  Stated by Gartner at RSA Conference, February 2005 - http://www.vnunet.com/news/1161375
- **"Law enforcement agencies in the United States and overseas recently disrupted an on-line organised crime ring that spanned eight U.S. states and six countries … 7 million credit card numbers had been stolen by the crime ring, costing consumers and credit card companies around $4.3 million"**
  Ralph Basham, Director of the U.S. Secret Service - http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=7667789
- **"Mobile devices such as PDAs and cell phones are the new frontier for viruses, spam and other security threats … 70 percent of all email traffic on the Internet is spam … The number of known viruses grew by 28,327 in 2004 (for a running total of 112,438 known viruses) an increase of 25 percent from 2003"**
  IBM 2004 Global Business Security Index Report - http://www.ibm.com/news/be/en/2005/02/09.html

Complex systems need to be correct and resilient



- Pervasive and ubiquitous computing - always on-line
- Open dynamic heterogeneous interconnected system
- Sensitive personal information
- Untrained users - often risks unaware

- "Panic inducing" malicious faults
- "Huge multiplicity common mode" accidental faults

Catastrophic failure

Focus and priorities

- **Understanding new risks and threats** arising from the dynamic and evolutionary nature of the systems and their environments.
- **Understand the boundary-less nature of systems** and their failure behaviour with a need for modelling, data collection, experimentation, assessing systemic risks, and the possibility of emergent behaviour and surprise.
- Developing existing resilience technologies to **deal with increased scale and complexity and criticality** (telecoms, embedded, smart cards) – **emphasis on critical components.**
- Developing theories, methods, tools for the design, development and evaluation of AmI systems and existing systems in the changed threat environment – **emphasis on composability.**
- Understanding and assessing trust, risk and responsibility, predicting trust relationships and developing methods for **users – oriented dependability risk assessments.**
- Dependability of **meta-data.**
- **Developing a multi-disciplinary resilience community** by empirical studies, joint program of work, addressing fundamental concepts. Does not exist at the moment.

Information Society Technologies

ReSIST NoE

Resilience for Survivability in IST

SIXTH FRAMEWORK PROGRAMME

Rationale

(Reasonably) known:
High dependability and security
for safety-critical or availability-critical systems

- Avionics, railway signalling, nuclear control, etc.
- Transaction processing, back-end servers, etc.

Continuous complexity growth
Large, networked, evolving, applications
running on open systems, fixed or mobile

Scalability of Dependability

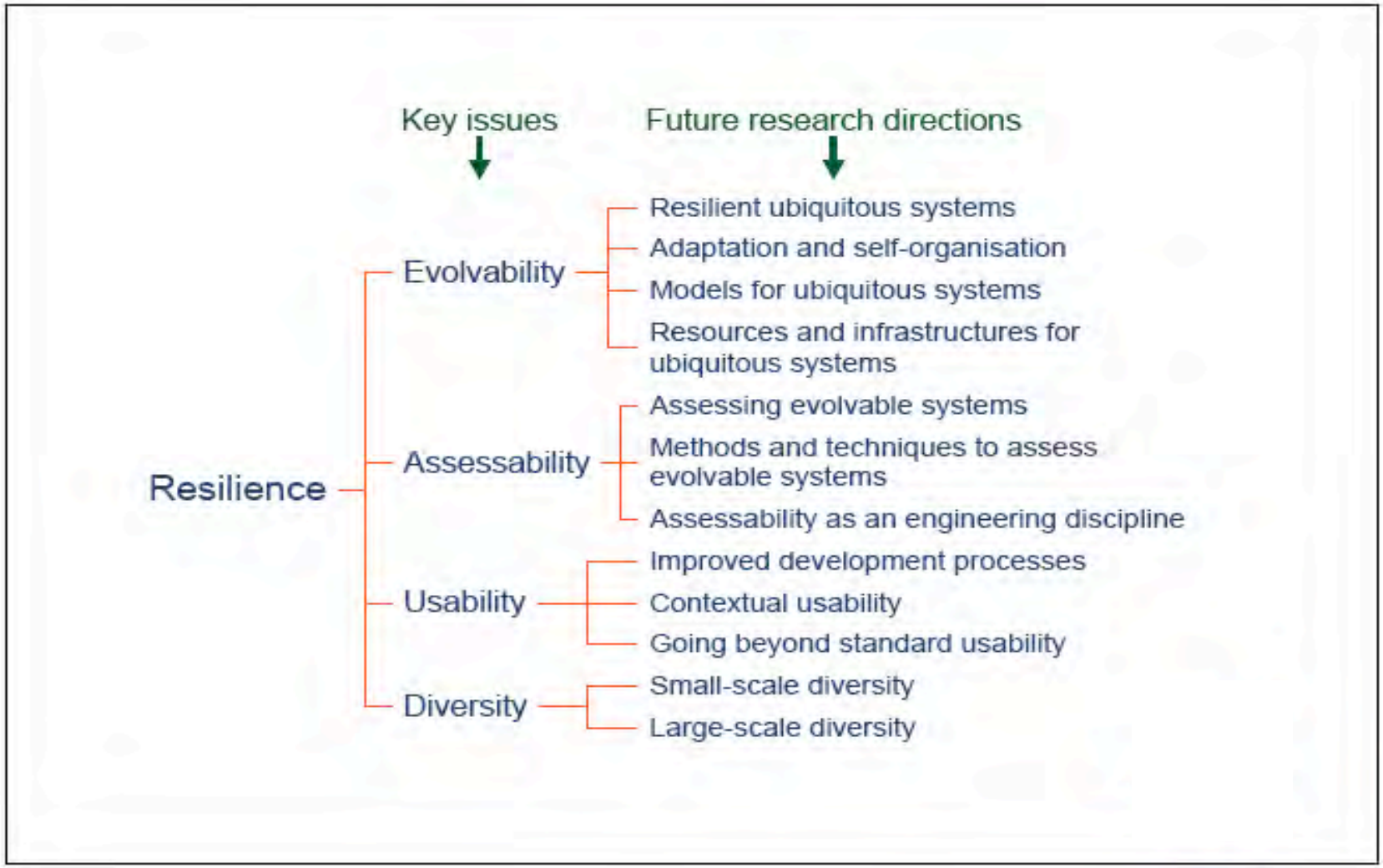
Beyond rigorous functional design, provision of

Resilience for Survivability,
wrt accidental and malicious threats

Logic

Partners

Budapest U
City U
Darmstadt U
DeepBlue
Eurecom
France Telecom R&D
IBM Zurich
IRISA
IRIT
LAAS-CNRS (Coord.)
Lisbon U
Newcastle U
Pisa U
QinetiQ
Roma-La Sapienza U
Southampton U
Ulm U
Vytautas Magnus U


Key issues
Future research directions
Resilience
Evolvability
Resilient ubiquitous systems
Adaptation and self-organisation
Models for ubiquitous systems
Resources and infrastructures for ubiquitous systems
Assessability
Assessing evolvable systems
Methods and techniques to assess evolvable systems
Assessability as an engineering discipline
Usability
Improved development processes
Contextual usability
Going beyond standard usability
Diversity
Small-scale diversity
Large-scale diversity

MSc curriculum rationale

To move from the usual application-driven MSc curricola (like MSc in embedded systems or web-based systems, etc.)

To identify a MSc curriculum where, in the first year, the focus is on advanced fundamental invariants (application independent) that can provide students with a solid updated theoretical knowledge for dealing with resilience

To specialize, in the second year, on applications of such knowledge on real projects in selected application tracks with strong connection with productive world

To remove the gap between what is *known* and what is *used*:

From Best Practices ⟶ to Methodical Scientific Approach

Curriculum aims

- To equip students with the skills and knowledge required to develop and assess secure and dependable computer-based systems
- To provide a qualification enhancing employment prospects in resilient computing
- To develop research skills
- To develop and improve key skills in written and oral communication and in teamwork
- To develop and improve skills in using the literature and information technology resources relevant to resilient computing
- To encourage the development of creativity skills
- To develop skills in critical assessment, analysis and storage of information
- To provide a curriculum which meets the requirements of appropriate professional bodies, thus providing a basis for further professional development and lifelong learning
- To address the relevant professional, legal and ethical issues relevant to the development, assessment and maintenance of resilient systems
- To provide an international perspective on developments in computer resilience.

Curriculum organization

1st Year

- **1st semester: Basics and Fundamentals (30 ECTS)**

Courses:

- **Advanced Probability and Statistics**(6 ECTS)
- **Cryptology and Information Security** (6 ECTS)
- **Logic in Computer Science** (6 ECTS)
- **Advanced Graph Theory** (3 ECTS)
- **Human Factors, Human and Organizational Behavior** (3 ECTS)
- **Fundamentals of Real-Time Systems** (3 ECTS)
- **Fundamentals of Dependability** (3 ECTS)

- **2nd semester: Methods, Techniques and Tools (30 ECTS)**

Courses:

- **Computer Networks Security** (6 ECTS)
- **Resilient Distributed Systems and Algorithms** (6 ECTS)
- **Dependability and Security Evaluation of Computer-based Systems** (6 ECTS)
- **Testing, Verification and Validation** (6 ECTS)
- **Usability and User Centered Design for Dependable and Usable Socio-technical Systems** (6 ECTS)

3rd semester: Projects (in cooperation with industry on specific appl. fields) (30 ECTS)

Courses (common to all application tracks)

- **Middleware Infrastructures for Application Integration** (3 ECTS)
- **Software Reliability Engineering** (3 ECTS)
- **Management of Projects** (3 ECTS)

Application track: **Resilience in Communication Networks**

Courses (specific for this track):

- **IP Networks and Service Resilience** (3 ECTS)
- **Resilience of Mobile Applications** (3 ECTS)

Application track: **Safety-critical Systems**

Courses (specific for this track):

- **Development Process and Standards for Safety-Critical Applications** (3 ECTS)
- **Architectural Issues and Examples of Systems** (3 ECTS)

Application track: **Resilience in e-Business**

Courses (specific for this track):

- **Enterprise Security** (3 ECTS)
- **Computer and Network Forensics** (3 ECTS)

Common to all Application tracks:

- **Project in cooperation with Industry** (9 ECTS)
- **Space for additional Courses** (6 ECTS)

4th semester: Master's Thesis and Dissertation (30 ECTS)

- **Specific Courses and Seminars** (3 ECTS)
- **Preparation and Presentation of the Thesis** (27 ECTS)

Teaching load

- 1 ECTS = 25 hours Lectures+Labs+individual study (average)
- For the 1st and 2nd semesters: Lecture hours: 350 hours; Exercise and labs: 270 hours and Individual study: 880 hours;
- For the 3rd and 4th semesters: Lecture hours: 160 hours; Exercise and labs: 215/235 hours and Individual study: 1125/1105 hours;
- In total: 3000 hours (consistent with 120 ECTS each 25 hours worth) of which:
  - -Total number of lectures + exercise and lab: 995/1015 hours and
  - -Total number of hours of individual study: 2005/1985 hours.

Curriculum Pre-requisites

- Discrete Mathematics
- Calculus
- Basic Computer and Network Architectures
- Programming and Data Structures
- Basics of Operating Systems
- Basics of Software Engineering
- Basics of Probability and Statistics

The portal to MSc Curriculum and Courseware material

http://www.resist-noe.org/

This is the official ReSIST portal

- **Original ReSIST Courseware, as set of slides, for the following Courses:**
  - ✓ **Fundamentals of Dependability - J-C. Laprie**
  - ✓ **Computer Network Security - P. Verissimo, M. Correia**
  - ✓ **Resilient Distributed Systems and Algorithms - P. Verissimo, M. Correia**
  - ✓ **Dependability and Security Evaluation of Computer-based Systems - M. Kaâniche, K. Kanoun, J-C. Laprie**
  - ✓ **Testing Verification and Validation - F. von Henke, C. Bernardeschi, P. Masci, H. Pfeifer, H. Waeselynck**
  - ✓ **Usability and User Centred Design for Dependable and Usable Socio-technical Systems - P. Palanque, M. Harrison, M. Winckler**
  - ✓ **Management of Projects - G. Lami**
  - ✓ **Middleware Infrastructures for Application Integration - R. Baldoni, R. Beraldi, G. Lodi, L. Querzoni, S. Scipioni**
  - ✓ **Software Reliability Engineering - K. Kanoun**
- **A very extensive search for support material has been made on the web**

Support material from:

- ✓ LAAS-CNRS, France
- ✓ Budapest University of Technology and Economics, Hungary
- ✓ City University, London, UK
- ✓ Technische Universität Darmstadt, Germany
- ✓ Institut Eurécom, France
- ✓ France Telecom Recherche et Développement, France
- ✓ IBM Research GmbH, Switzerland
- ✓ Université de Rennes 1 – IRISA, France
- ✓ Université de Toulouse III – IRIT, France
- ✓ Fundação da Faculdade de Ciencias da Universidade de Lisboa, Portugal
- ✓ University of Newcastle upon Tyne, UK
- ✓ Universitá di Pisa, Italy
- ✓ Universitá degli studi di Roma "La Sapienza", Italy
- ✓ Universität Ulm, Germany
- ✓ Aalborg University, Denmark
- ✓ Adelard, UK
- ✓ Carleton University, Canada
- ✓ Carnegie Mellon University, USA
- ✓ Chalmers University, Sweden
- ✓ Chinese University of Hong Kong, China
- ✓ CSR, London, UK
- ✓ Duke University, USA
- ✓ EPFL, Switzerland
- ✓ ETH Zurich, Switzerland
- ✓ EWICS TC7
- ✓ George Mason University, USA
- ✓ Georgia Institute of Technology, USA
- ✓ Queen Mary University, London, UK
- ✓ Katholieke Universiteit Leuven, Belgium
- ✓ Imperial College, London, UK
- ✓ Lehigh University, USA
- ✓ MIT, USA
- ✓ Saarland University, Germany
- ✓ Scuola Superiore S. Anna, Pisa, Italy
- ✓ Technical University of Madrid, Spain
- ✓ University College London, UK
- ✓ University of Aachen, Germany
- ✓ University of Bielefeld, Germany
- ✓ University of Birmingham, UK
- ✓ University of Bristol, UK
- ✓ University of California at Berkeley, USA
- ✓ University of Cambridge, UK
- ✓ University of Copenhagen, Denmark
- ✓ University of Edinburgh, UK
- ✓ University of Glasgow, UK
- ✓ University of Konstanz, Germany
- ✓ University of Melbourne, Australia
- ✓ University of Pennsylvania, USA
- ✓ University of Southern California, USA
- ✓ University of Texas at San Antonio, USA
- ✓ University of Twente, Netherland
- ✓ University of Waterloo, Canada
- ✓ University of Yale, USA
- ✓ Weizmann Institute of Science, Israel
- ✓ Westminster College, USA

Contributions welcome !

- **Resilient Computing Curriculum - Deliverable D37 downloadable from http://www.resist-noe.org/**

- **Resilient Computing Courseware - Deliverable D38 downloadable from http://www.resist-noe.org/ includes a large database of support material**

Persons interested to contribute:
Mail to me: Luca Simoncini <luca.simoncini@isti.cnr.it>