ReSIST: Resilience for Survivability in IST

A European Network of Excellence

Contract Number: 026764

Deliverable D18: Second Open Workshop report

Report Preparation Date: October 2007
Classification: Public
Contract Start Date: 1st January 2006
Contract Duration: 36 months
Project Co-ordinator: LAAS-CNRS
Partners: Budapest University of Technology and Economics
City University, London
Technische Universität Darmstadt
Deep Blue Srl
Institut Eurécom
France Telecom Recherche et Développement
IBM Research GmbH
Université de Rennes 1 – IRISA
Université de Toulouse III – IRIT
Vytautas Magnus University, Kaunas
Fundação da Faculdade de Ciencias da Universidade de Lisboa
University of Newcastle upon Tyne
Università di Pisa
QinetiQ Limited
Università degli studi di Roma "La Sapienza"
Universität Ulm
University of Southampton

Information Society Technologies

SIXTH FRAMEWORK PROGRAMME

Contents

1- Summary 5

2- Programme 7

3- Attendance List 13

4- Slides 17

From Resilience to ReSIST, Jean-Claude Laprie (LAAS-CNRS, Toulouse, France) 19

From Resilience-Building to Resilience-Scaling Technologies, Michel Banâtre (University of Rennes - IRISA, France) 27

Evolvability: Research Directions, Andras Pataricza (Budapest University of Technology and Economics, Hungary) 41

Software Evolvability: An industry’s view, Giuseppe Martufi (Elsag-Datamat, Italy) 57

Assessability: Research Directions, Aad Van Moorsel (University of Newcastle upon Tyne, UK) 65

Assessability: Industry's View, Jean-Paul Blanquart (EADS-Astrium, France) 71

Usability: Research Directions, Philippe Palanque (University of Toulouse - IRIT, France) 75

Usability: Industry's View, Colin Corbridge (Defence Science & Technology Laboratory, UK) 91

Diversity: Research Directions, Lorenzo Strigini (City University, London, UK) 95

Diversity: Industry's View, Michele Morganti (Nokia-Siemens, Italy) 103

Resilient Systems: Current Research and Future Directions, Yves Paindaveine (European Commission) 109

5- ReSIST Brochure 121

1- Summary

The workshop was held at Università degli studi di Roma *La Sapienza*, on 18 October 2007. Local organisation was jointly carried out by the University and by Deep Blue.

The workshop was aimed at presenting the findings of ReSIST concerning research that needs to be pursued or undertaken on the resilience of computing systems and information infrastructures. Recommended research directions have been structured according to the four identified resilience-scaling technologies: evolvability, assessability, usability and diversity. For these technologies the ReSIST partners produced over forty texts addressing gaps and challenges, which were then synthesised:

- Evolvability: resilient ubiquitous systems, adaptation and self-organisation, models, resources and infrastructures for ubiquitous systems.
- Assessability: assessing evolvable systems, methods and techniques for assessability, assessability as an engineering discipline.
- Usability: development processes, contextual usability, going beyond standard usability.
- Diversity: large-scale vs. small-scale diversity, designed diversity vs. spontaneous diversity.

The ReSIST deliverable D13 (*From Resilience-Building to Resilience-Scaling Technologies: Directions*) provides the texts on research gaps and challenges, together with the syntheses. This report was distributed at the workshop as a CD, which included also deliverable D12 (*Resilience-Building Technologies: State of Knowledge).*

After a welcome address by Roberto Baldoni (Università degli studi di Roma *La Sapienza*), an overview of ReSIST and the NoE’s views on resilience were presented by Jean-Claude Laprie (LAAS-CNRS), and Michel Banâtre (IRISA) presented an overview of the research agenda.

Sessions devoted to each of the resilience-scaling technologies followed, each with a presenter and responder. The presenters were members of ReSIST who summarised the proposed research directions; a leading practitioner external to ReSIST then responded with an independent reaction from an industrial perspective. The corresponding sessions were as follows:

- Evolvability
  - *Research Directions:* Andras Pataricza (Budapest University of Technology and Economics, Hungary*)*
  - *Industry's View:* Giuseppe Martufi (Elsag-Datamat, Italy)
- Assessability
  - *Research Directions:* Aad Van Moorsel (University of Newcastle upon Tyne, UK)
  - *Industry's View:* Jean-Paul Blanquart (EADS-Astrium, France)
- Usability
  - *Research Directions:* Philippe Palanque (University of Toulouse - IRIT, France)
  - *Industry's View:* Colin Corbridge (Defence Science & Technology Laboratory, UK)
- Diversity
  - *Research Directions:* Lorenzo Strigini (City University, London, UK)
  - *Industry's View:* Michele Morganti (Nokia-Siemens, Italy)

During the concluding session, the views of the European Commission were presented by Yves Paindaveine.

Each session was including a discussion time for interaction with the audience.

The workshop was attended by 100 persons, out of which 43 were external to ReSIST.

The remainder of this report gives:

1) The workshop programme.
2) The attendance list.
3) The copies of the slides presented during the workshop.
4) The ReSIST brochure that was distributed to the attendees.

2- Programme

ReSIST: Resilience for Survivability in IST

A European Network of Excellence

http://www.resist-noe.eu

Second Open Workshop

Resilience in Computing Systems and Information Infrastructures: A Research Agenda

18 October 2007

Università degli studi di Roma *La Sapienza*, Italy

SAPIENZA
UNIVERSITÀ DI ROMA

The challenges raised for achieving satisfactorily dependability and security of the emerging ubiquitous systems are sharpened by the statistical evidence that those systems suffer from a gap in the achieved capabilities with respect to the expectations of the stakeholders.

A central characteristic of those ubiquitous systems being the continuous evolutionary changes they are facing, scaling up their dependability and security requests a *resilience* view in order to cope with and to adapt to these evolutionary changes. The changes can be functional, technological, environmental, and include threat evolutions. Such changes drastically increase uncertainty about system and infrastructure behaviour.

The workshop is aimed at presenting the findings of the European Network of Excellence ReSIST on the research directions for *resilience* of computing systems and information infrastructures to enable their dependability and security to scale-up.

Information Society
Technologies

SIXTH FRAMEWORK PROGRAMME

Workshop Programme

This workshop presents the findings of the ReSIST European Network of Excellence concerning research that needs to be pursued or undertaken on the resilience of computing systems and information infrastructures. Recommended research directions have been structured according to the four identified resilience-scaling technologies: evolvability, assessability, usability and diversity. For these technologies the ReSIST partners produced over forty texts addressing gaps and challenges, which were then synthesised:

- Evolvability: adaptation and self-organisation, models and resources for ubiquitous systems.
- Assessability: assessing evolvable systems, methods and techniques for assessability, assessability as an engineering discipline.
- Usability: operators' and designers' viewpoints; usability metrics.
- Diversity: large-scale vs. small-scale diversity, designed vs. spontaneous diversity.

A ReSIST report provides details on research gaps and challenges, together with the syntheses; this report will be distributed at the workshop as a CD.

An opening session will present the ReSIST view on resilience, and an overview of the ReSIST research agenda. A session devoted to each of the resilience-scaling technologies has been arranged, each with a presenter and responder. The presenters are members of ReSIST who will summarise the proposed research directions; a leading practitioner external to ReSIST will then respond with an independent reaction from an industrial perspective. A concluding session will provide the opportunity to hear the views of the European Commission.

Workshop Schedule

8h - 8h30 Registration

8h30 - 9h30 ***Opening Session***

Session Chair and welcome address: Roberto Baldoni (University of Roma "La Sapienza", Italy)

From Resilience to ReSIST, Jean-Claude Laprie (LAAS-CNRS, Toulouse, France)

From Resilience-Building to Resilience-Scaling Technologies, Michel Banâtre (University of Rennes - IRISA, France)

9h30 - 10h30 ***Evolvability***

Session Chair: Miguel Correia (University of Lisbon, Portugal)

Research Directions: Andras Pataricza (Budapest University of Technology and Economics, Hungary*)*

Industry's View: Enrico Angori (Elsag-Datamat, Italy)

Discussion

10h30 - 11h Coffee Break

11h - 12h ***Assessability***

Session Chair: Karama Kanoun (LAAS-CNRS, Toulouse, France)

Research Directions: Aad Van Moorsel (University of Newcastle upon Tyne, UK)

Industry's View: Jean-Paul Blanquart (EADS-Astrium, France)

Discussion

12h - 13h ***Usability***

Session Chair: Alberto Pasquini (Deep Blue, Italy)

Research Directions: Philippe Palanque (University of Toulouse - IRIT, France)

Industry's View: Colin Corbridge (Defence Science & Technology Laboratory, UK)

Discussion

13h - 14h Lunch

14h-15h ***Diversity***

Session Chair: Marc Dacier (Eurecom, Sophia-Antipolis, France)

Research Directions: Lorenzo Strigini (City University, London, UK)

Industry's View: Michele Morganti (Nokia-Siemens, Italy)

Discussion

15h - 16h ***Concluding Session***

Session Chair: Tom Anderson (University of Newcastle upon Tyne, UK)

Invited talk: *Resilient Systems: Current research and Future directions*, Jacques Bus (European Commission)

Discussion

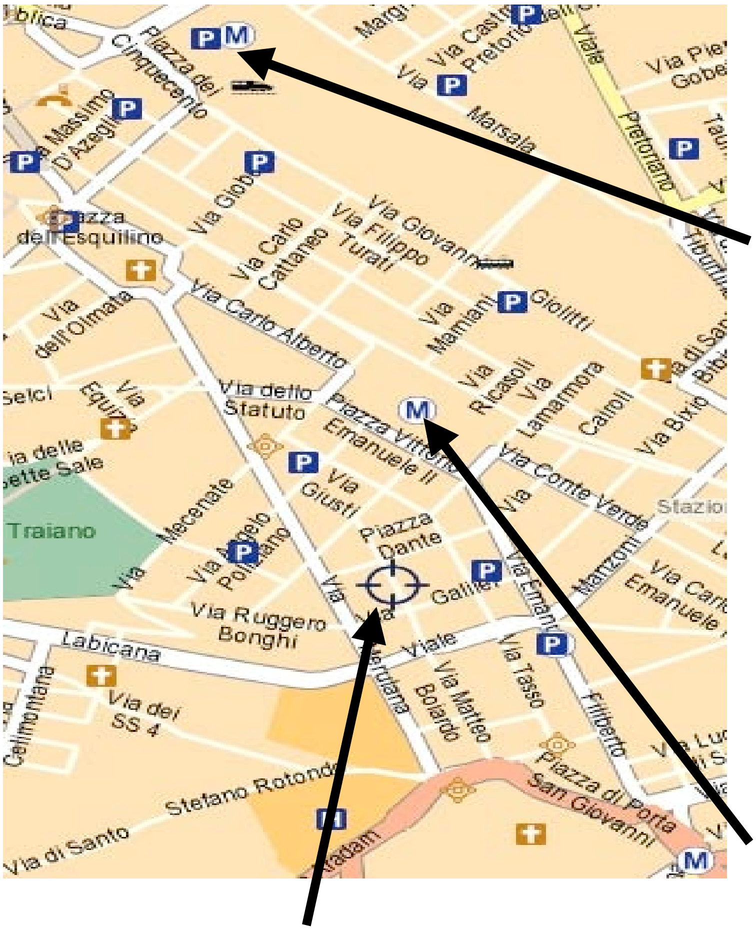
Workshop registration

Registration to the workshop is free of charge. Advance registration using the registration form at the end of the programme is requested for logistics purposes, **by 1st October**.

Workshop attendance includes a CD with the report *From Resilience-Building to Resilience-Scaling Technologies: Directions*, as well as two companion reports: *Resilience-Building Technologies: State of Knowledge,* and *Support for Resilience-Explicit Computing*. Coffee breaks and the lunch are also included in workshop attendance.

Workshop Location and how to reach it

Aula Magna
Dip. di Informatica e Sistemistica dell'Univ. di Roma La Sapienza
Via Ariosto 25, Roma, Italy



Workshop location

From Leonardo da Vinci (Fiumicino) Airport.
Option 1) take a taxi (from 40 Euros to 50 Euros) to Via Ariosto 25
Option 2) take the train “Leonardo Express”to **Termini station** (there is a train every 30’)

From Ciampino Airport.
Option 1) take a taxi (from 30 Euros to 40 Euros) to Via Ariosto 25
Option 2) take a bus to **Termini station** for timetable please follow the following URL
http://www.adr.it/content.asp?Subc=2398&L=1&idMen=204

From Termini Station
Option 1) walk for 15 minutes.
Option 2) take the metro A (direction Anagnina), DIS is in the middle between **Vittorio** metro stop and Manzoni metro stop.

Hotels

Mercure Roma Delta Colosseo, 4 stars
Via Labicana 144, 00184 Roma
Phone: (+39)06/770021
Fax : (+39)06/77250198
http://www.accorhotels.com/accorhotels/fichehotel/gb/mer/2909/fiche_hotel.shtml

A block of rooms has been reserved:
- Single room: 129 Euros including breakfast
- Double room, single usage: 158 Euros including breakfast
- Double room, double usage: 195 Euros including breakfast

Reservation deadline: 15th September
Reservation e-mail: carla.fresia@dblue.it

Hotel Mecenate Palace, 4 stars
Via Carlo Alberto 3, 00185 Roma,
Tel. +39 06 44702024,
160 Euros including breakfast
booking online at:
http://www.hotelmecenatepalace.com/hotel-reservations/index.php

Hotel Milton Roma, 4 stars
Via Emanuele Filiberto 155, 00185 Roma
Tel. +39 06 4523161
130 Euros including breakfast if booked with venere.com (nice and close but it could be noisy; ask for a room in the back)

Hotel Edera, 3 stars
Via Poliziano 75, 00184 Roma
Tel. +39 06 70453888
140 Euros including breakfast if booked with booking.com (very close)

Hotel Novecento 3 stars
Via Carlo Emanuele I 12, 00185 Roma
Tel. +39 06 7096247
90 Euros including breakfast if booked with travellero.com

Palatino Grand Hotel, 4 stars
Via Cavour 213, 00184 Roma
Tel. +39 06 4814927
140 Euros not including breakfast
booking online at:
http://www.hotelpalatino.com/index_ita.html
(a bit more far from the workshop location)

About ReSIST

ReSIST is an Network of Excellence 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 physical and residual development faults, interaction mistakes, or malicious attacks and disruptions.

Network Partners

- LAAS-CNRS, Toulouse, France (Coordinator)
- Budapest University of Technology and Economics, Hungary
- City University, London, UK
- Technische Universität Darmstadt, Germany
- Deep Blue Srl, Roma, Italy
- IBM Research, Zurich, Switzerland
- Institut Eurécom, Sophia Antipolis, France
- France Telecom Recherche et Développement, Lannion and Caen, France
- 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 Ltd, Malvern, UK
- Università degli studi di Roma "La Sapienza", Italy
- Universität Ulm, Germany
- University of Southampton, UK

ReSIST 2nd Open Workshop

Dip. di Informatica e Sistemistica
dell'Univ. di Roma *La Sapienza*, Italy

SAPIENZA
UNIVERSITÀ DI ROMA

Registration Form

Fax to +33 (0)5 61 33 64 11 or e-mail the requested information to resistmeeting@laas.fr, **by 1st October**

Name (First Last) ______________________________

Email ______________________________

Company/Institution ______________________________

Address ______________________________

____

____

Phone ______________________________

Special Dietary Needs ______________________________

3- Attendance List

ReSIST: Resilience for Survivability in IST

A European Network of Excellence

http://www.resist-noe.eu

Second Open Workshop

Resilience in Computing Systems and Information Infrastructures: A Research Agenda

18 October 2007

Università degli studi di Roma *La Sapienza*, Italy

Attendance List

Abi Haidar, Diala, *France Telecom Recherche et Développement, France*
Ahrendt, Wolfgang, *Chalmers University of Technology, Sweden*
Almgren, Magnus, *University of Chalmers, Sweeden*
Anderson, Tom, *University of Newcastle upon Tyne, UK*
Andrews, Zoe, *University of Newcastle upon Tyne, UK*
Angori, Enrico, *Elsag-Datamat, Italy*
Antonino, Virgillito, *ISTAT, Italian's National Institute of Statistics, Italy*
Avizienis, Algirdas, *Vytautas Magnus University, Kaunas, Lithuania*
Bacivarov, Angelica, *University Politehnica Bucharest, Romania*
Bacivarov, Ioan, *University Politehnica Bucharest, Romania*
Baldoni, Roberto, *Università degli studi di Roma "La Sapienza", Italy*
Banâtre, Michel, *IRISA, France*
Battaglia, Luigi, *Consorzio SESM c/o SELEX-SI, Italy*
Beraldi, Roberto, *Università degli studi di Roma "La Sapienza", Italy*
Bernardeschi, Cinzia, *Università di Pisa, Italy*
Bézard, Christine, *Airbus, France*
Blanquart, Jean-Paul, *Astrium Satellites, France*
Bohli, Jens-Matthias, *Nec, Germany*
Bologna, Sandro, *ENEA - CR Casaccia, Italy*
Bonomi, Silva, *Università degli studi di Roma "La Sapienza", Italy*
Buchegger, Sonja, *Deutsche Telecom, Germany*
Carvalho, Pedro, *Universidade de Lisboa, Portugal*
Catalano, Cecilia, *ISTAT, Italian's National Institute of Statistics, Italy*
Chialastri, Antonio, *Italy*
Cimmino, Stefano, *Selex-Sima, Italy*
Claraz, Denis, *Siemens-VDO, France*
Coppola, Paolo, *INTECS, Italy*
Corbridge, Colin, *Defence Science & Technology Laboratory, UK*
Correia, Miguel, *Universidade de Lisboa, Portugal*
Dacier, Marc, *Institut Eurécom, France*
Dambra, Carlo, *Università di Pisa, Italy*
De Looy-Hyde, Jessica, *Defence Science & Technology Laboratory, UK*
Dini, Gianluca, *Università di Pisa, Italy*
Dyhouse, Tony, *Cyber Security KTN, UK*
Fabre, Jean-Charles, *LAAS-CNRS, France*
Faconti, Giorgio, *Università di Pisa, Italy*
Glaser, Hugh, *University of Southampton, UK*
Harrison, Michael, *University of Newcastle upon Tyne, UK*

Humayoun, Shahrukh, *Università degli studi di Roma "La Sapienza", Italy*
Jacob, Grégoire, *France Telecom Recherche et Développement, France*
Kanoun, Karama, *LAAS-CNRS, France*
Kennedy, Catriona, *University of Birmingham, UK*
Kharchenko, Vyacheslav, *National Aerospace University, Ukraine*
Khelil, Abdelmajid, *Technische Universität Darmstadt, Germany*
Koopman, Philip, *Carnegie Mellon Uuniversity, USA*
Lac, Chidung, *France Telecom Recherche et Développement, France*
Laprie, Jean-Claude, *LAAS-CNRS, France*
Leita, Corrado, *Institut Eurécom, France*
Lotti, Giulia, *Deep Blue, Italy*
Mancini, *ENAV, Italy*
Marchetti, Carlo, *Senato della Repubblica Italian, Italy*
Martuffi, Giuseppe, *Elsag-Datamat, Italy*
Masci, Paolo, *Università di Pisa, Italy*
Meskauskiene, Irena, *Central Project Management Agency, Lithuania*
Mian, Adnan Nour, *Università degli studi di Roma "La Sapienza", Italy*
Milani, Alessia, *Università degli studi di Roma "La Sapienza", Italy*
Millard, Ian, *University of Southampton, UK*
Morganti, Michele, *Nokia-Siemens, Italy*
Mortimer, Derek, *University of Newcastle upon Tyne, UK*
Müller, Samuel, *IBM Research, Switzerland*
Nanni, Vincenzo, *ENEA - CR Casaccia, Italy*
Ohalloran, Colin, *QinetiQ Limited, UK*
Oualha, Nouha, *Institut Eurécom, France*
Paindaveine, Yves, *European Commission, Belgium*
Palanque, Philippe, *IRIT, France*
Palumbo, Massimiliano, *Selex-Sima, Italy*
Parkin, Simon, *University of Newcastle upon Tyne, UK*
Pasquini, Alberto, *Deep Blue, Italy*
Pataricza, András, *Budapest University of Technology and Economics, Hungary*
Pham, Van Hau, *Institut Eurécom, France*
Popov, Peter, *City University, London, UK*
Poppleton, Michael, *University of Southampton, UK (RODIN Project)*
Powell, David, *LAAS-CNRS, France*
Pozzi, Simone, *Deep Blue, Italy*
Presenza, Domenico, *Engineering SpA, Italy*
Querzoni, Leonardo, *Università degli studi di Roma "La Sapienza", Italy*
Riordan, James, *IBM Research, Switzerland*
Roy, Matthieu, *LAAS-CNRS, France*
Saglietti, Francesca, *University of Erlangen-Nuremberg, Germany*
Sanna, Alberto, *Ospedale San Raffaele, Italy*
Scipioni, Sirio, *Università degli studi di Roma "La Sapienza", Italy*
Sebastian, Maurice, *Technical University Braunschweig, Germany*
Seinauskas, Rimantas, *Kaunas Technological University, Lithuania*
Sidlauskas, Kestutis, *Vytautas Magnus University, Kaunas, Lithuania*
Simoncini, Luca, *Università di Pisa, Italy*
Snook, Colin, *University of Southampton, UK (RODIN Project)*
Stein, Steffen, *Technical University Braunschweig, Germany*
Strigini, Lorenzo, *City University, London, UK*
Sujan, Mark-Alexander, *University of Warwick, UK*
Suri, Neeraj, *Technische Universität Darmstadt, Germany*
Tedeschi, Alessandra, *Deep Blue, Italy*
Tucci Piergiovanni, Sara, *Università degli studi di Roma "La Sapienza", Italy*
Van Moorsel, Aad, *University of Newcastle upon Tyne, UK*
Voges, Udo, *Forschungszentrum Karlsruhe, Germany*
Von Henke, Friedrich, *Universität Ulm, Germany*
Warns, Timo, *University of Oldenburg, Germany*
Windsor, James, *ESA ESTEC, The Netherlands*
Wright, David, *City University, London, UK*
Zurutuza, Urko, *University of Mondragon, Spain*
Zutautaite-Seputiene, Inga, *Lithuanian Energetics Institute, Lithuania*

4- Slides

ReSIST

Resilience for Survivability in IST

A European Network of Excellence

Second Open Workshop

esist
Information Society
Technologies
SIXTH FRAMEWORK PROGRAMME
SAPIENZA
UNIVERSITÀ DI ROMA
DEEPBLUE consulting&research

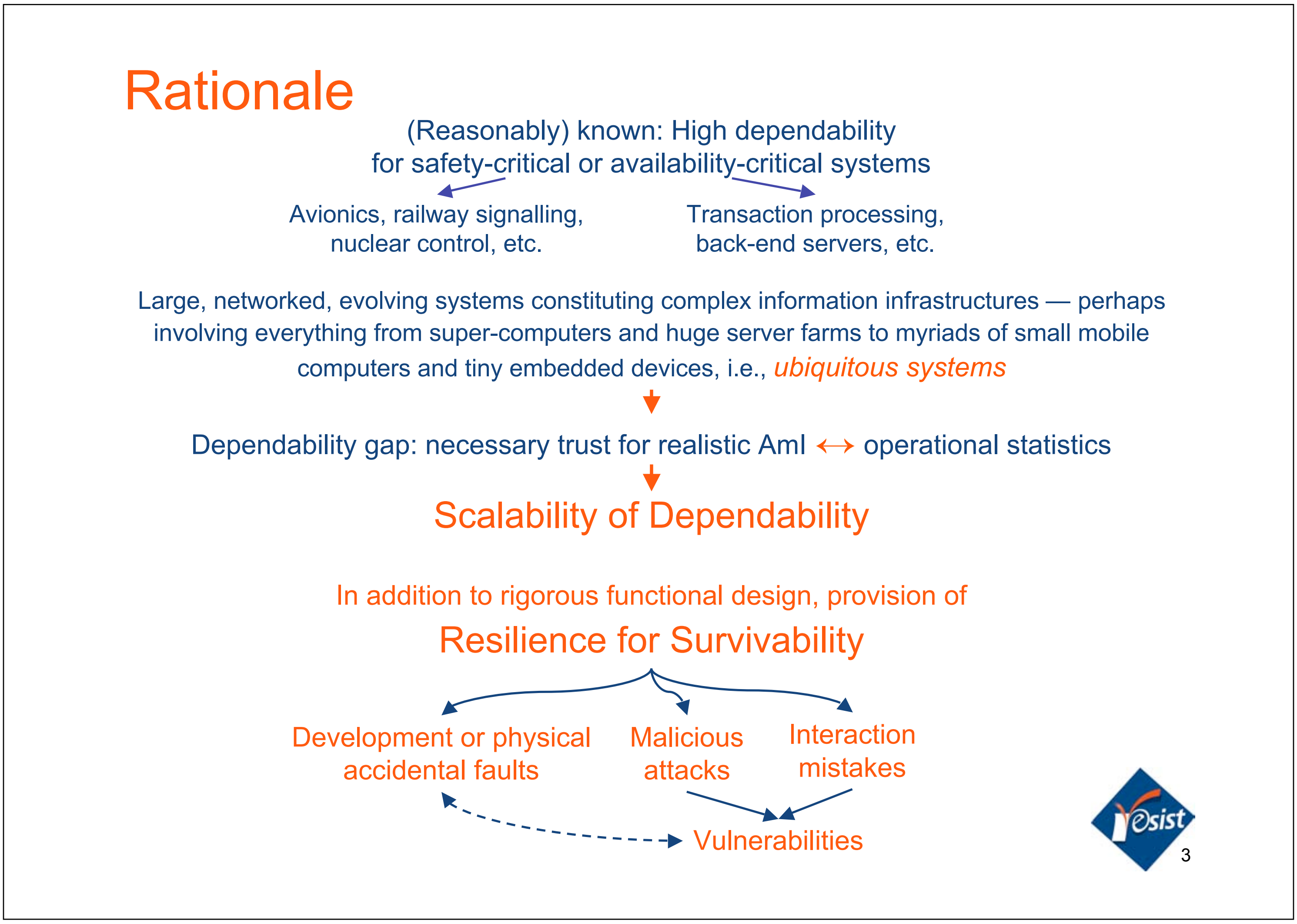
ReSIST

Resilience for Survivability in IST

A European Network of Excellence

- Rationale
- Resilience: definition and technologies
- Joint Programme of Activities, and Logic
- Partnership
- Organisation
- Results, and near future
- Workshop Programme

esist
Information Society
Technologies
SIXTH FRAMEWORK PROGRAMME



Rationale

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

Avionics, railway signalling,
nuclear control, etc.

Transaction processing,
back-end servers, etc.

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, i.e., *ubiquitous systems*

Dependability gap: necessary trust for realistic AmI ↔ operational statistics

Scalability of Dependability

In addition to rigorous functional design, provision of

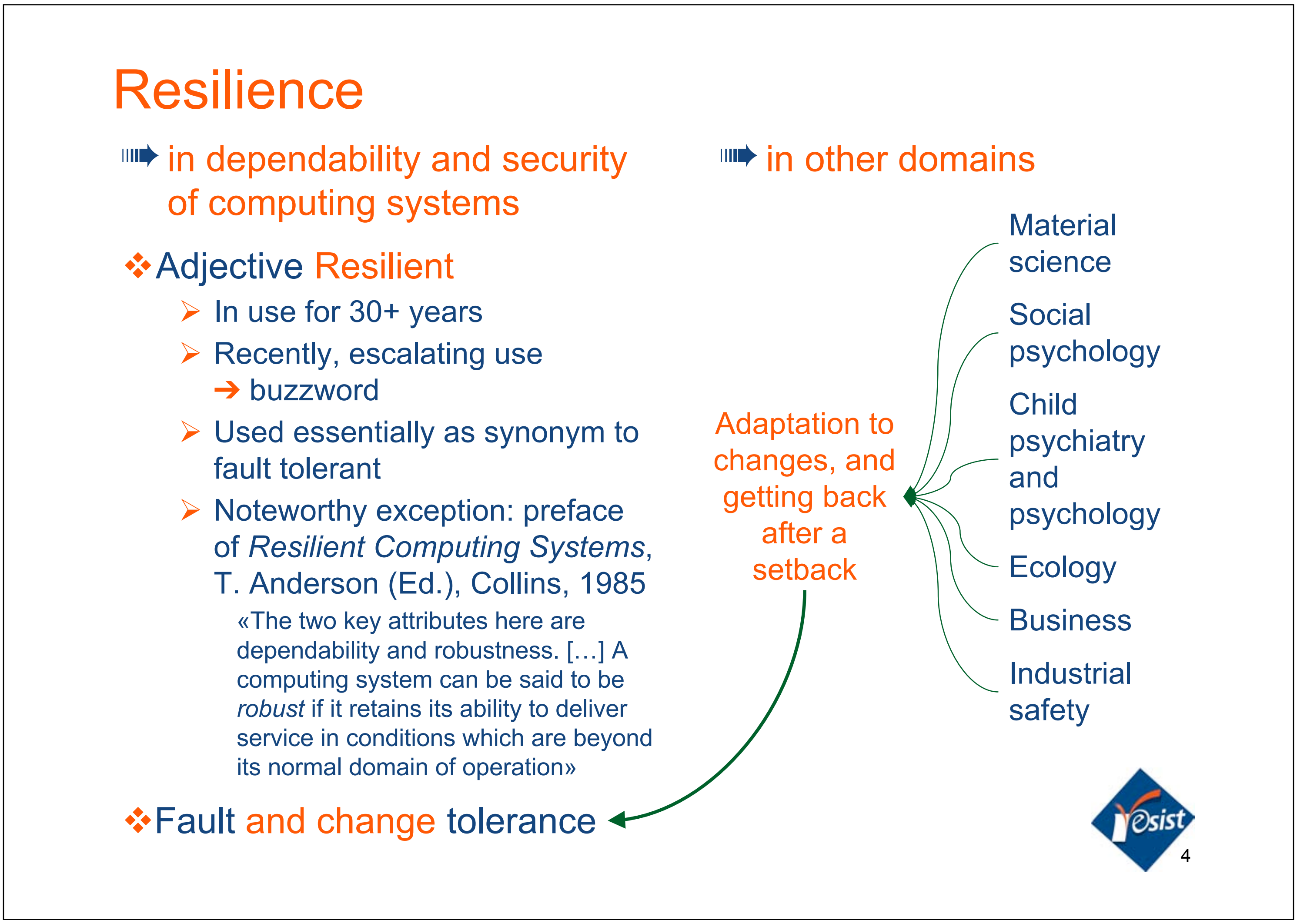
Resilience for Survivability

Development or physical accidental faults

Malicious attacks

Interaction mistakes

Vulnerabilities



Resilience

➠ in dependability and security of computing systems

❖ Adjective Resilient

- ➢ In use for 30+ years
- ➢ Recently, escalating use ➔ buzzword
- ➢ Used essentially as synonym to fault tolerant
- ➢ Noteworthy exception: preface of *Resilient Computing Systems*, T. Anderson (Ed.), Collins, 1985

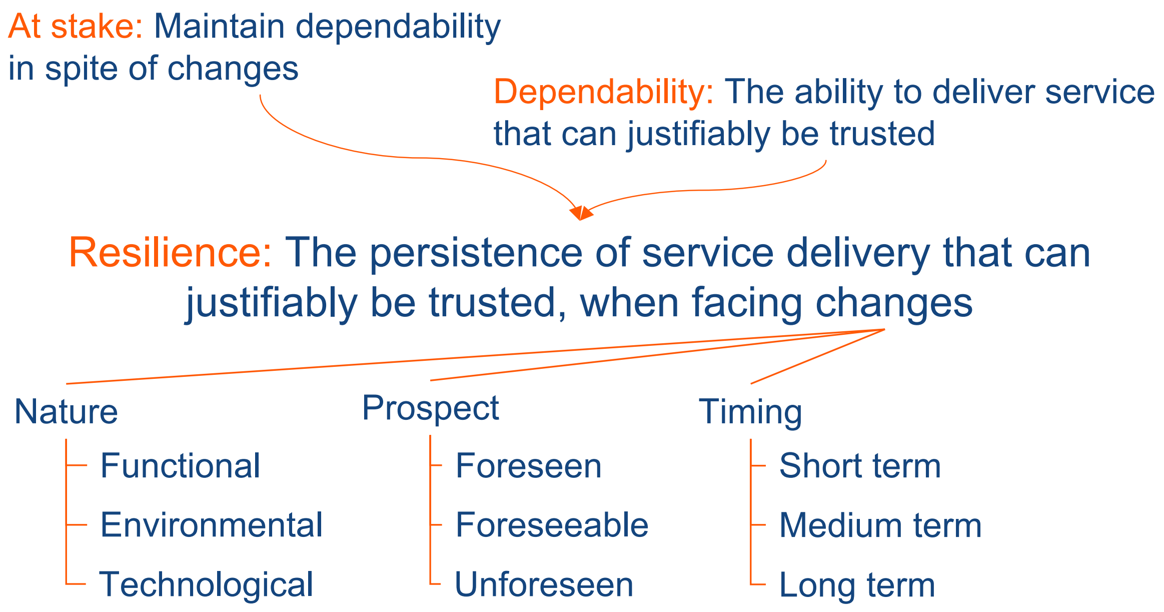
  «The two key attributes here are dependability and robustness. […] A computing system can be said to be *robust* if it retains its ability to deliver service in conditions which are beyond its normal domain of operation»

❖ Fault and change tolerance

➠ in other domains

Adaptation to changes, and getting back after a setback

- Material science
- Social psychology
- Child psychiatry and psychology
- Ecology
- Business
- Industrial safety



At stake: Maintain dependability in spite of changes

Dependability: The ability to deliver service that can justifiably be trusted

Resilience: The persistence of service delivery that can justifiably be trusted, when facing changes

Nature
- Functional
- Environmental
- Technological

Prospect
- Foreseen
- Foreseeable
- Unforeseen

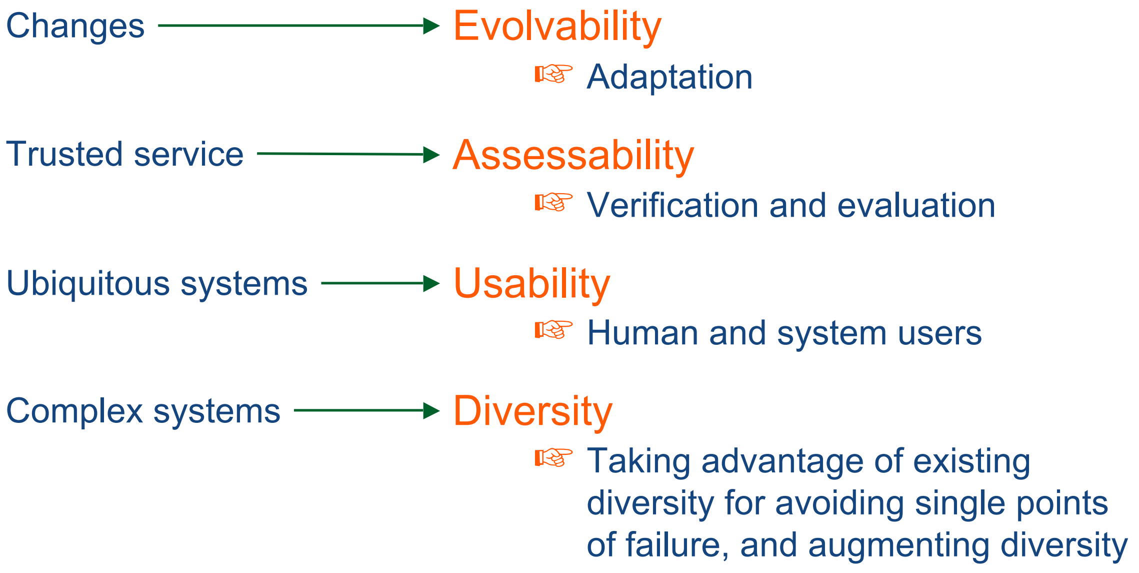
Timing
- Short term
- Medium term
- Long term

☞ The definition does not exclude the possibility of failure

Alternate definition of dependability

Ability to avoid service failures that are unacceptably frequent or severe

Technologies for resilience



Changes → Evolvability

☞ Adaptation

Trusted service → Assessability

☞ Verification and evaluation

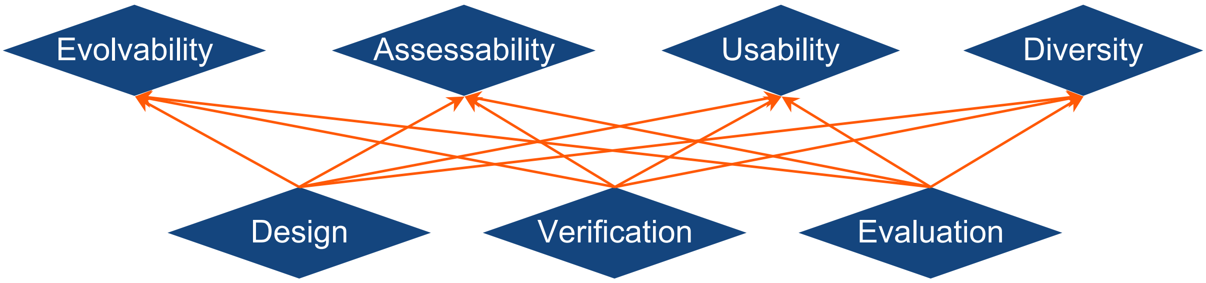
Ubiquitous systems → Usability

☞ Human and system users

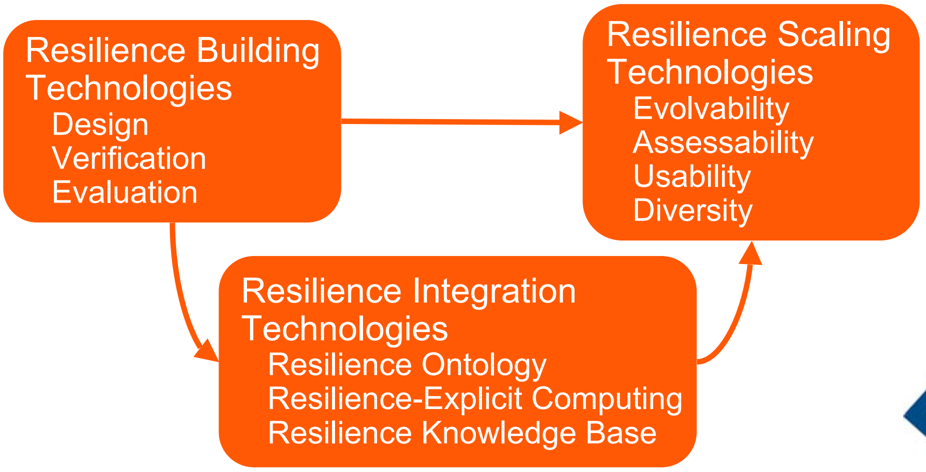
Complex systems → Diversity

☞ Taking advantage of existing diversity for avoiding single points of failure, and augmenting diversity

Joint Programme of Activities



Logic of Joint Programme of Research

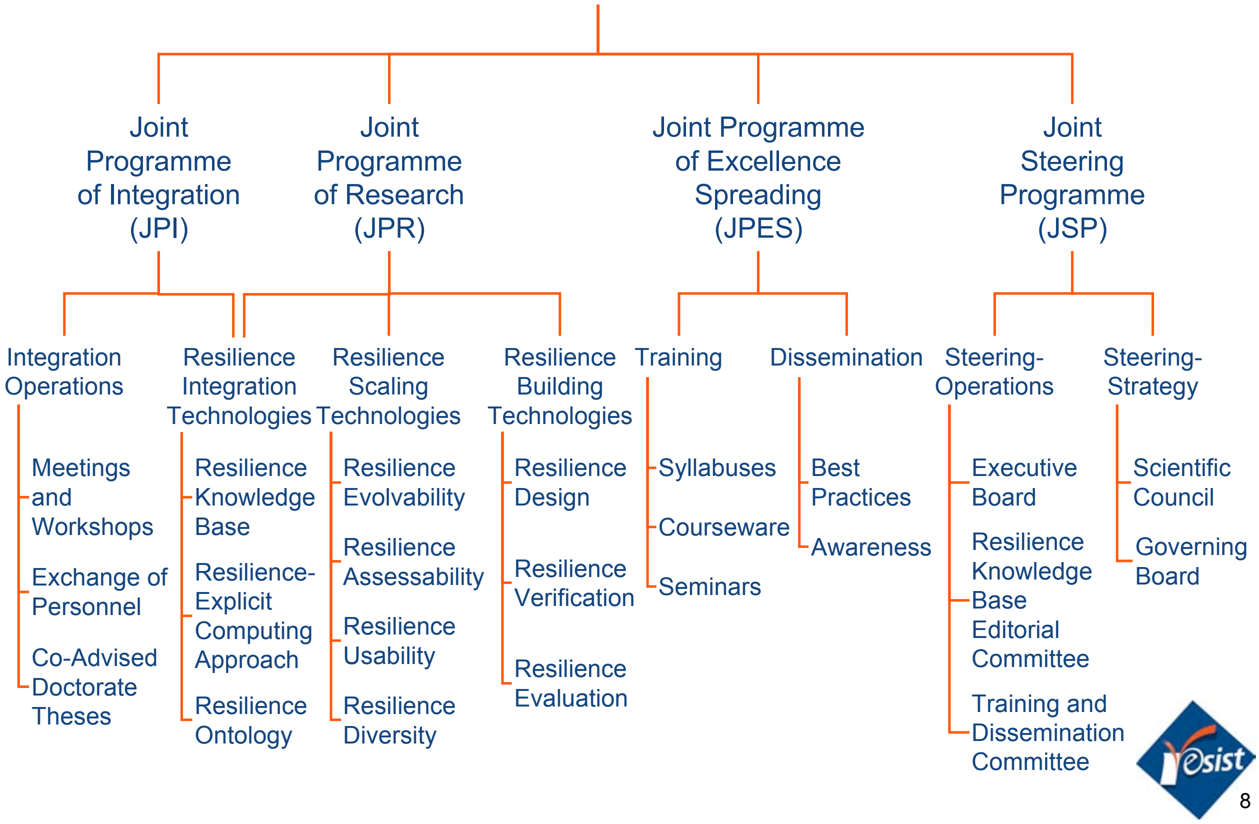


Resilience Building Technologies
- Design
- Verification
- Evaluation

Resilience Scaling Technologies
- Evolvability
- Assessability
- Usability
- Diversity

Resilience Integration Technologies
- Resilience Ontology
- Resilience-Explicit Computing
- Resilience Knowledge Base

Joint Programme of Activities (JPA)



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

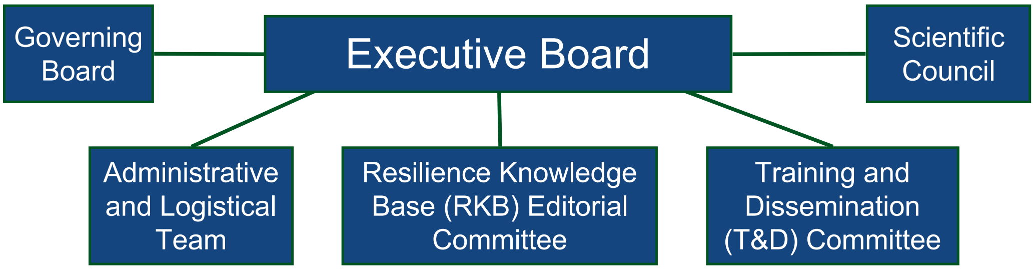
Partnership

	Expertise				Country	Academia (Ac) / Industry (Ind)
	Threat resilience: development or physical Accidental faults (A) / Malicious attacks (M) / Interaction mistakes (I)			Mobile computing		
LAAS-CNRS [coordinator]	A	M		X	FR	Ac
Budapest U.	A				HU	Ac
City U., London	A	M	I		UK	Ac
Darmstadt U.	A	M			DE	Ac
Deep Blue			I		IT	Ind - SME
Eurecom		M		X	FR	Ac
France Telecom R&D	A	M		X	FR	Ind
IBM Research Zurich		M			CH	Ind
IRISA	A			X	FR	Ac
IRIT			I		FR	Ac
Vytautas Magnus U., Kaunas	A				LT	Ac
Lisbon U.	A	M		X	PT	Ac
Newcastle U.	A	M	I		UK	Ac
Pisa U.	A	M	I		IT	Ac
QinetiQ	A	M			UK	Ind
Roma-La Sapienza U.	A			X	IT	Ac
Ulm U.	A				DE	Ac
Southampton U.	Semantic Web				UK	Ac

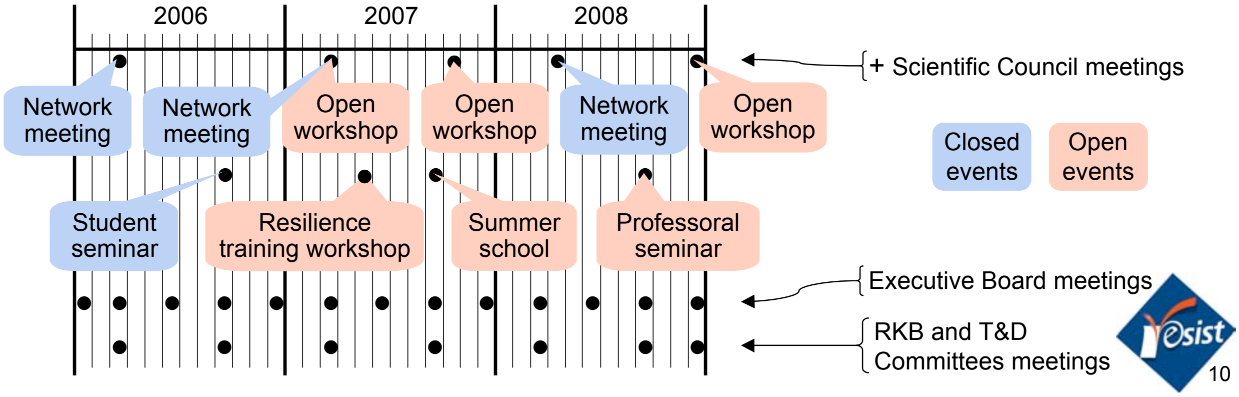
110 researchers plus 61 students, 3 year duration

Organisation

☞ Management


Governing Board
Executive Board
Scientific Council
Administrative and Logistical Team
Resilience Knowledge Base (RKB) Editorial Committee
Training and Dissemination (T&D) Committee

☞ Event Schedule

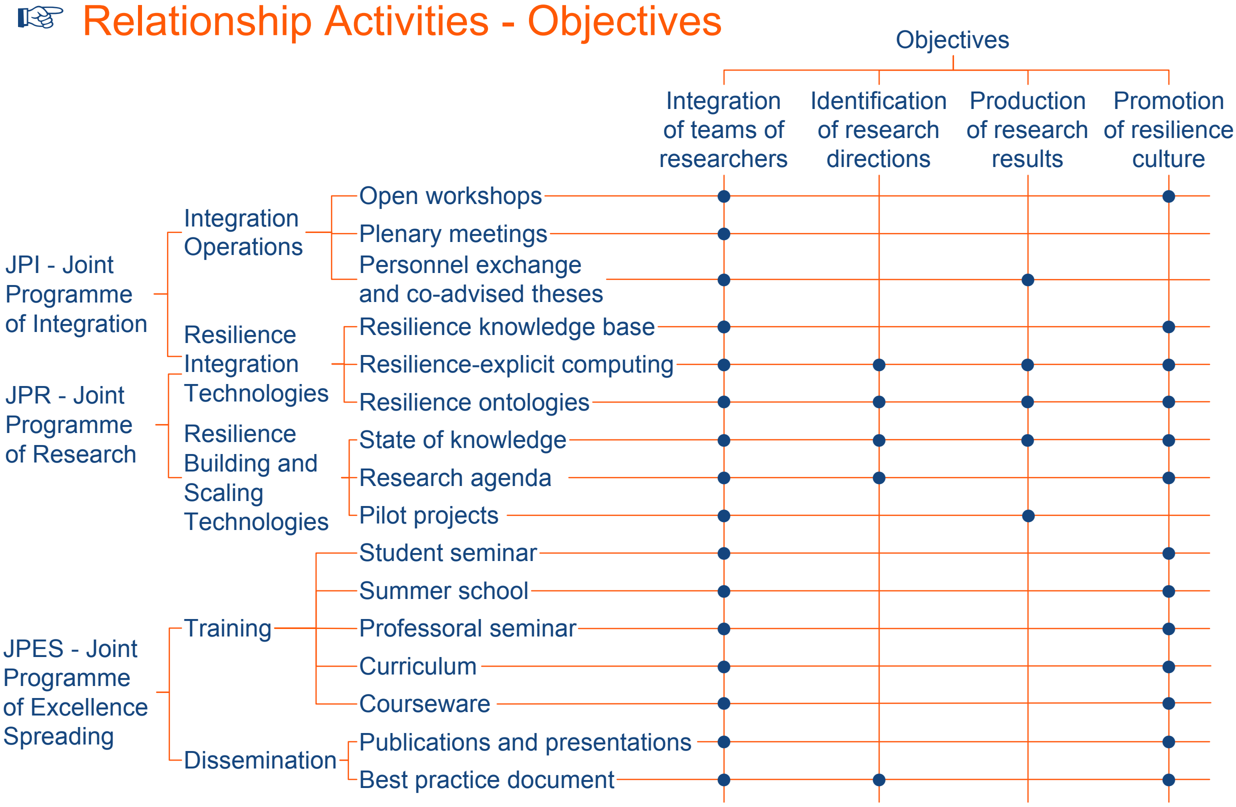


Results

- ❖ Major achievements
  - ➢ 83 co-authors
    - ✓ State of Knowledge in Resilient Computing
    - ✓ Research Agenda in Resilient Computing
  - ➢ Prototype of the Resilience Knowledge Base: 40 millions basic facts
- ❖ Ground work
  - ➢ Resilience-Explicit Computing approach
  - ➢ Best Practice document
  - ➢ Training
    - ✓ Curriculum in Resilient Computing: draft
    - ✓ Courseware in Resilient Computing: outline
- ❖ Organisation of significant events
  - ➢ Plenary network meetings: March 2006, Toulouse, and March 2007 Budapest
  - ➢ Open Workshops: March 2007, Budapest, and October 2007, Roma
  - ➢ Student seminar: September 2006, San Miniato
  - ➢ Resilience Training open workshop: May 2007, Erlangen
  - ➢ Summer school: September 2007, Porquerolles

11

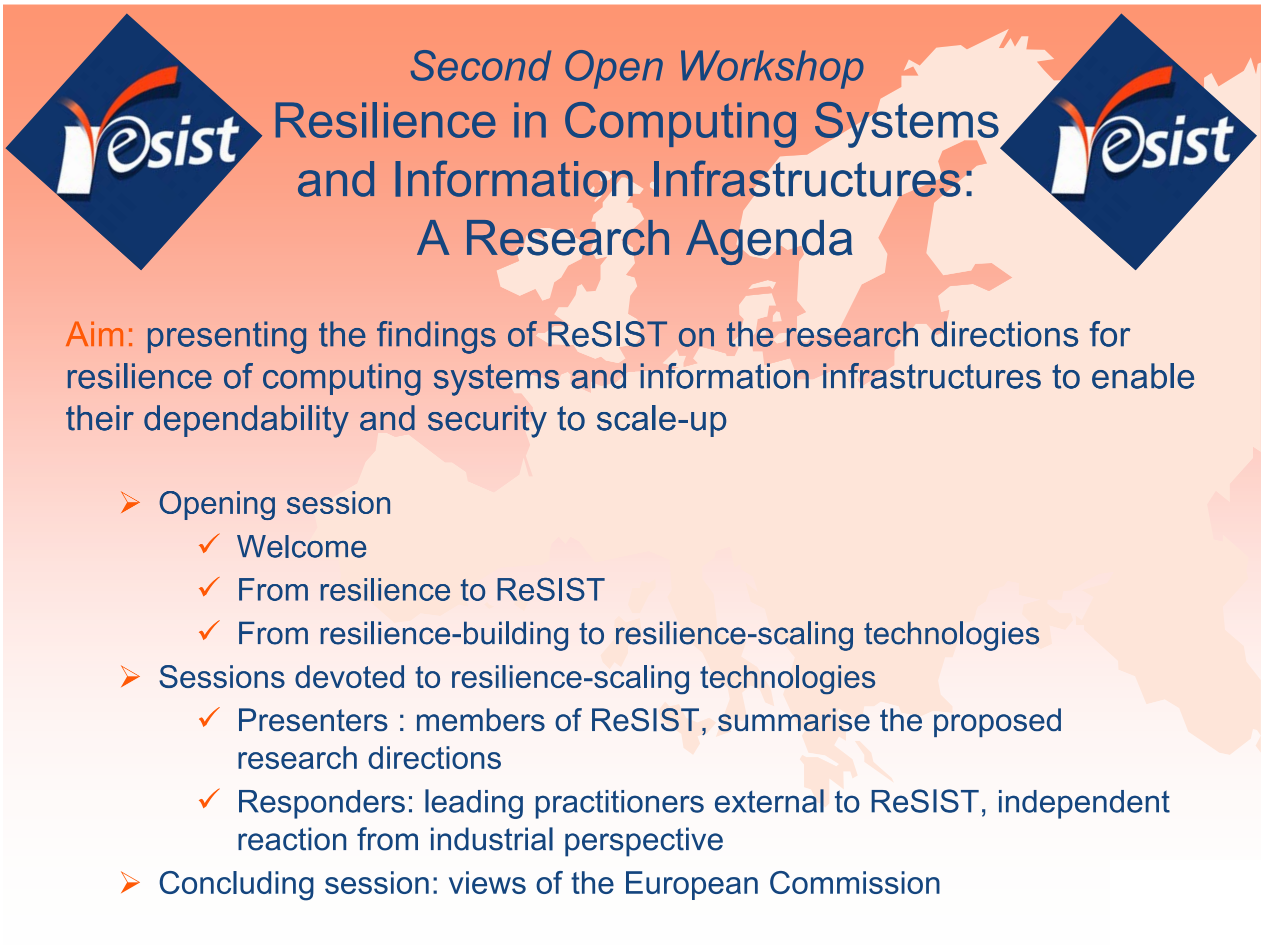
☞ Relationship Activities - Objectives



			Objectives			
			Integration of teams of researchers	Identification of research directions	Production of research results	Promotion of resilience culture
JPI - Joint Programme of Integration	Integration Operations	Open workshops	●			●
		Plenary meetings	●			
		Personnel exchange and co-advised theses	●		●	
	Resilience Integration Technologies	Resilience knowledge base	●			●
		Resilience-explicit computing	●	●	●	●
		Resilience ontologies	●	●	●	●
JPR - Joint Programme of Research	Resilience Building and Scaling Technologies	State of knowledge	●	●	●	●
		Research agenda	●	●		●
		Pilot projects	●		●	
JPES - Joint Programme of Excellence Spreading	Training	Student seminar	●			●
		Summer school	●			●
		Professoral seminar	●			●
		Curriculum	●			●
		Courseware	●			●
	Dissemination	Publications and presentations	●			●
		Best practice document	●	●		●

☞ Pilot Projects in Resilience Scaling Technologies, by junior researchers and doctorate students: Coming

12

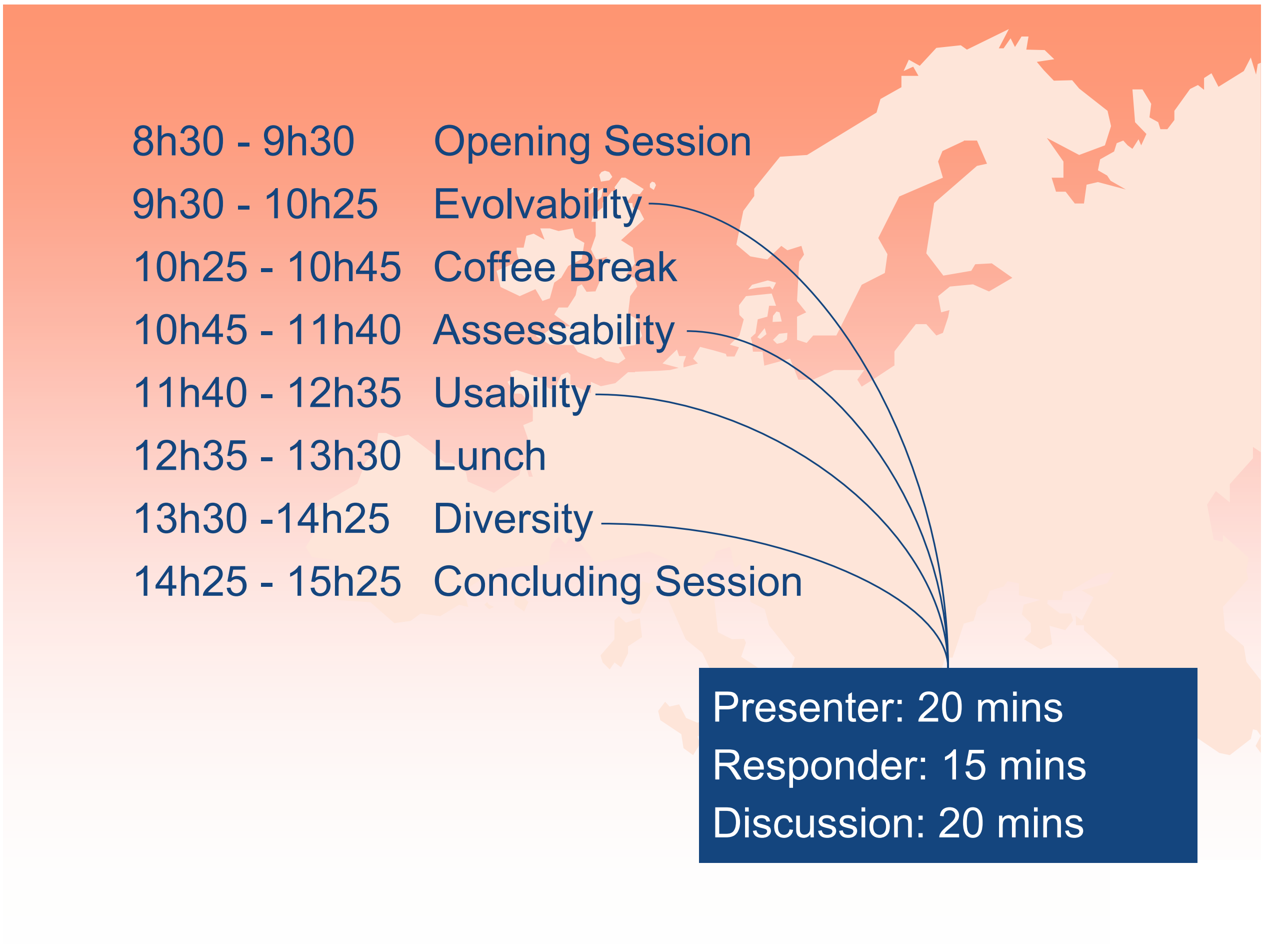


Second Open Workshop

Resilience in Computing Systems and Information Infrastructures: A Research Agenda

Aim: presenting the findings of ReSIST on the research directions for resilience of computing systems and information infrastructures to enable their dependability and security to scale-up

- Opening session
  - ✓ Welcome
  - ✓ From resilience to ReSIST
  - ✓ From resilience-building to resilience-scaling technologies
- Sessions devoted to resilience-scaling technologies
  - ✓ Presenters : members of ReSIST, summarise the proposed research directions
  - ✓ Responders: leading practitioners external to ReSIST, independent reaction from industrial perspective
- Concluding session: views of the European Commission



8h30 - 9h30	Opening Session
9h30 - 10h25	Evolvability
10h25 - 10h45	Coffee Break
10h45 - 11h40	Assessability
11h40 - 12h35	Usability
12h35 - 13h30	Lunch
13h30 -14h25	Diversity
14h25 - 15h25	Concluding Session

Presenter: 20 mins
Responder: 15 mins
Discussion: 20 mins

ReSIST

Resilience for Survivability in IST

A European Network of Excellence

Information Society Technologies

SIXTH FRAMEWORK PROGRAMME

From Resilience-Building to Resilience-Scaling Technologies

Michel Banâtre

Content

- Resilient building technologies
- Ubiquity
- One example
- The scaling challenge
- Conclusion

Resilience-Building Technologies (1)

Current state

- ReSIST’s DoW
  - "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)”.

Resilience-Building Technologies (2)

Current state

- State of art of the current knowledge and ongoing research on methods and techniques for building resilient systems dealing with different aspects of resilience building and the corresponding identified sub disciplinary areas:
  - Resilience architecting and implementation paradigms,
  - Resilience algorithms and mechanisms,
  - Resilient socio-technical systems,
  - Resilience evaluation,
  - Resilience verification.

D12 deliverable: Resilience-Building Technologies: State of Knowledge
(available on the Resist web site).

Resilience-Building Technologies (3)

Arch

- Resilience architecting and implementation paradigms
  - Identification of four research lines
    - Services oriented architectures
    - Mobiles services and their infrastructures
      - Exploitation of large scale networks (flexibility, interoperability)
    - Building resilient architectures with off-the-shelf components
    - Intrusion tolerant architectures

Resilience-Building Technologies (4)

Algo

- Resilience algotithms and mechanisms
  - Discussion of main categories of algorithms and protocols that underlie fault tolerance and distributed systems
    - Taking into account the scalability problem as part of their basic formulation
      - Number of nodes,
      - Number of faults to deal with,
  - E-voting
    - Secrecy of vote,
    - Protection from tampering

Resilience-Building Technologies (5)

Socio

- Resilient socio-technical systems
  - Integrating the analysis and design of the technical and human organisational subsets of ubiquitous systems
    - The process of reasoning about complex socio-technical systems
    - Reasoning about both the human and automated parts of a system in combination, (and taking into account their difference).

Resilience-Building Technologies (6)

Eval

- Methods and tools for resilience evaluation
  - Compositional modelling for large and evolving systems
  - Evaluation with respect to malicious threats
  - Dependability benchmarking
  - Diversity, i.e. probability of common-mode failure between redundant components

Resilience-Building Technologies (8)

Verif

- Methods and tools for verifying resilience
  - Formal methods
    - Deductive theorem proving
    - Model checking
    - Symbolic execution and abstract interpretation
  - Robustness testing
    - Fault injection, …
    - *….strong resist partner competences…*

Content

- Resilient building technologies
- Ubiquity
- One example
- The scaling challenge
- Conclusion

Ubiquity

- Pervasive computing,
- Ubiquitous systems,
- Ubiquitous network,
- …

Ubiquity (1)

- Ubiquitous/ pervasive computing
  - To provide “*spontaneous*” services/ applications
    - Explicit interactions between the user and the computers are reduced at the minimum level
    - The service is driven automatically by the events of the real world
      - “Invisible computers”
  - Sensors, tags
  - Wireless communication
  - HCI, (wearable computers)
  - Mobility
  - …

Ubiquity (2)

- Ubiquitous systems
  - Transparency for computation, (grid computing)
  - Transparency for the storage (P2P architecture)
    - « The network is the computer »
- Assumptions/constraints
  - Number of nodes forming any one system (large scale systems)
  - Variety of component types and of their interaction with users,
  - Heterogeneity of architecture (hardware and software)
  - Heterogeneity of autonomous organisations involved in making the system

Ubiquity (3)

- Ubiquitous networks
  - Heterogenous networks
    - Fixed and wireless networks
    - Cellular and short distance wireless communication architectures
    - Heterogenous network administrations
  - Seamless communication
    - Heterogenity is « invisible »

Content

- Resilient building technologies
- Ubiquity
- One example
- The scaling challenge
- Conclusion

One example

Resilient ambient systems (GF2)

Before, data can be produced on reliable server (well known solutions based on redundancy)

Now, new devices create data during disconnection period (wireless and mobile architectures) without any accessible reliable server.

- Short-range wireless communications
  (WiFi, BlueTooth, etc…)
- Mobile terminals
  (cell phones, PDAs, digital cameras, mobile sensors, mobile robots, …)
- New data
  (Pictures, movies, schedules, contact lists, etc…)

➡ Risk of data loss when the device fails

A collaborative backup system could solve with this problem

One example

Resilient ambient systems (GE2)

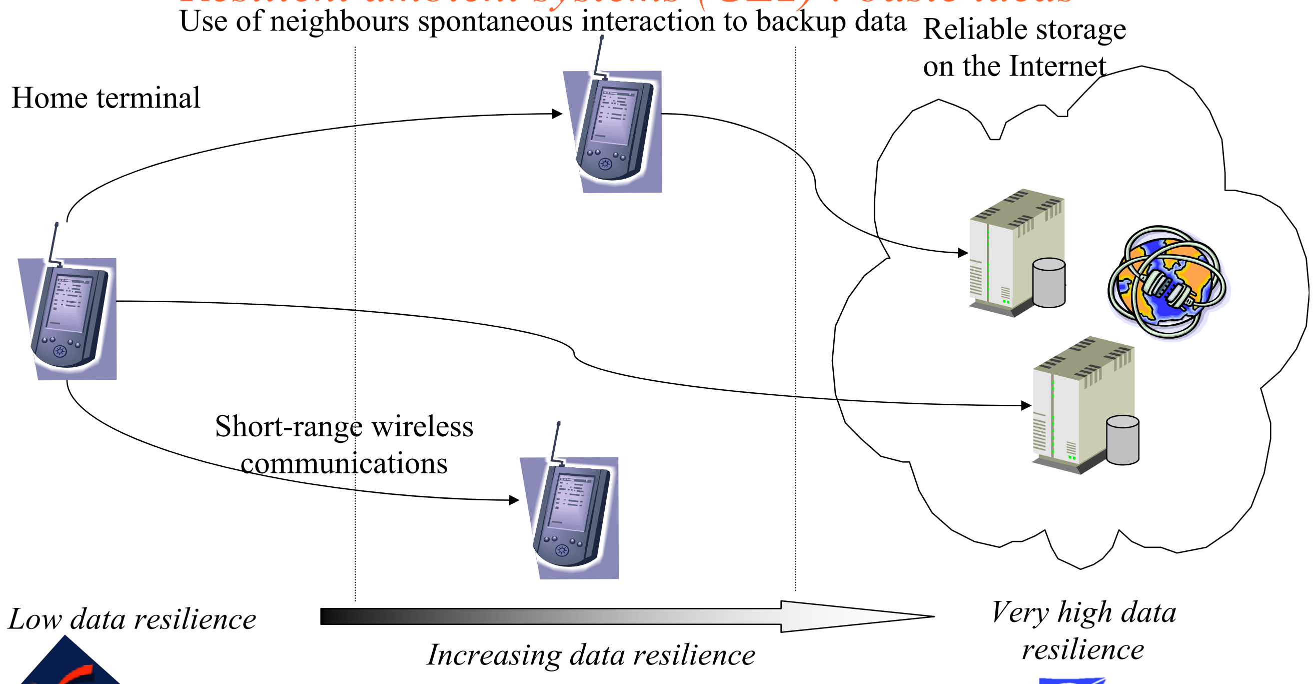
- One simple scenario :
  - Alice takes notes on her devices during a meeting
  - After the meeting, she takes the bus home
  - Once at home, she notices that she has lost her PDA

➡ Lost of the device ⇒ Loss of data

- But, thanks to the “collaborative backup” service , Alice recovers her data from the Internet once at home
  - The data have been transparently and spontaneously backed-up on neighbour terminals by “collaborative backup” service.

One example

Resilient ambient systems (GE2) : basic ideas


Use of neighbours spontaneous interaction to backup data
Reliable storage on the Internet
Home terminal
Short-range wireless communications
Low data resilience
Increasing data resilience
Very high data resilience

One example

Resilient ambient systems (GE2) : some research issues

- Handling data coherency and data dissemination
  - Fragmentation, replication, etc...
  - Implementation of truly replicated services
    - How to migrate replicas
    - How to ensure atomic updates of a dynamic set of migrating replicas
    - …
- Resource management
  - Network management
    - Wireless communication management (spontaneous communication)
  - Device -PDA-
    - Battery/power management
    - Memory management
- Security
  - Data encryption
  - Trust between terminals

One example

Resilient ambient systems (GE2): applications

- Personal devices
  - PDA
  - Cellphones (see- http://www.laas.fr/mosaic)
- Robotics
  - Mobile robots realizing collaborative tasks (swarm robots)
- Mobile sensors networks
  - Delivery tracking
  - Contagious disease tracking (for animals)

Content

- Resilient building technologies
- Ubiquity
- One example
- The scaling challenge
- Conclusion

The scaling challenge (1)

- To ensure the resilience of these new ubiquitous systems
  - *To identify the different research problems (or gaps) which have to be solve.*
  - To find solutions to these problems

The scaling challenge (2)

- Identifying a roadmap of integrated research using the current resilience-*building* technologies to develop the required resilience-*scaling* technologies
  - Evolvability,
    - To preserve the system’s functional correctness across steps of its evolution and its resilience
  - Assessability,
    - To assess their ability to function properly and to provide the quality of service that they will deliver under both nominal and stressful conditions
  - Usability
    - Human interaction and the potential effects of their action (strongly related to pervasive computing)
  - Diversity
    - To provide the service exploiting components replication facilities

Content

- Resilient building technologies
- Ubiquity
- One example
- The scaling challenge
- Conclusion

Conclusion

- The resilience scaling technologies have just been introduced
  - Place to the detailled presentations of these technologies and their associated gaps.

D13: From Resilience-Building to Resilience Scaling Technologies: Directions

Evolvability: Research directions

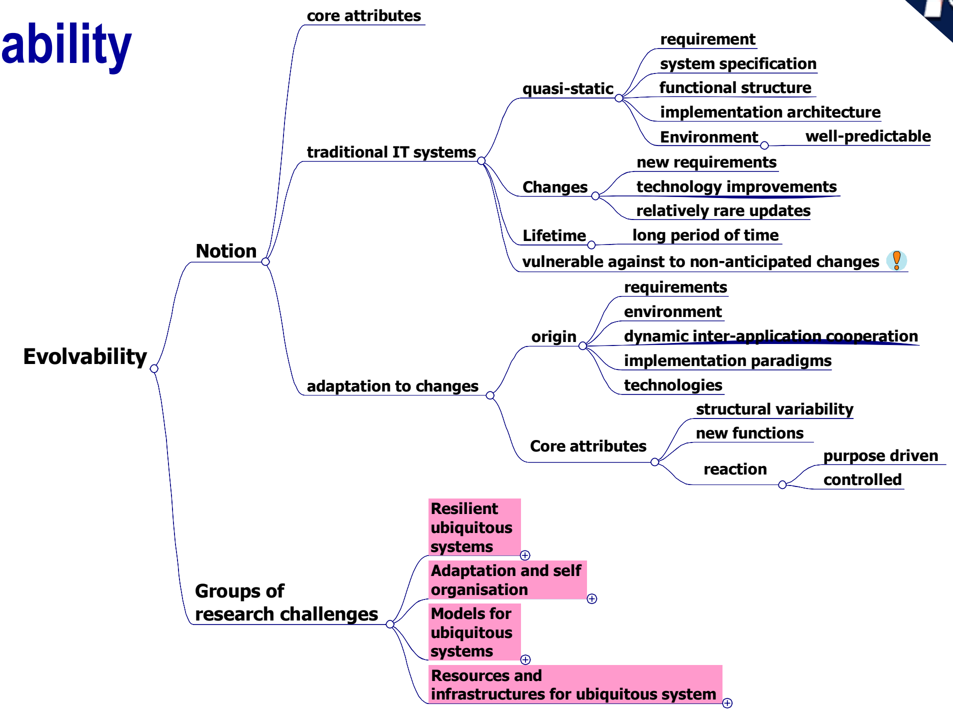
András Pataricza

Budapest University of Technology and Economics

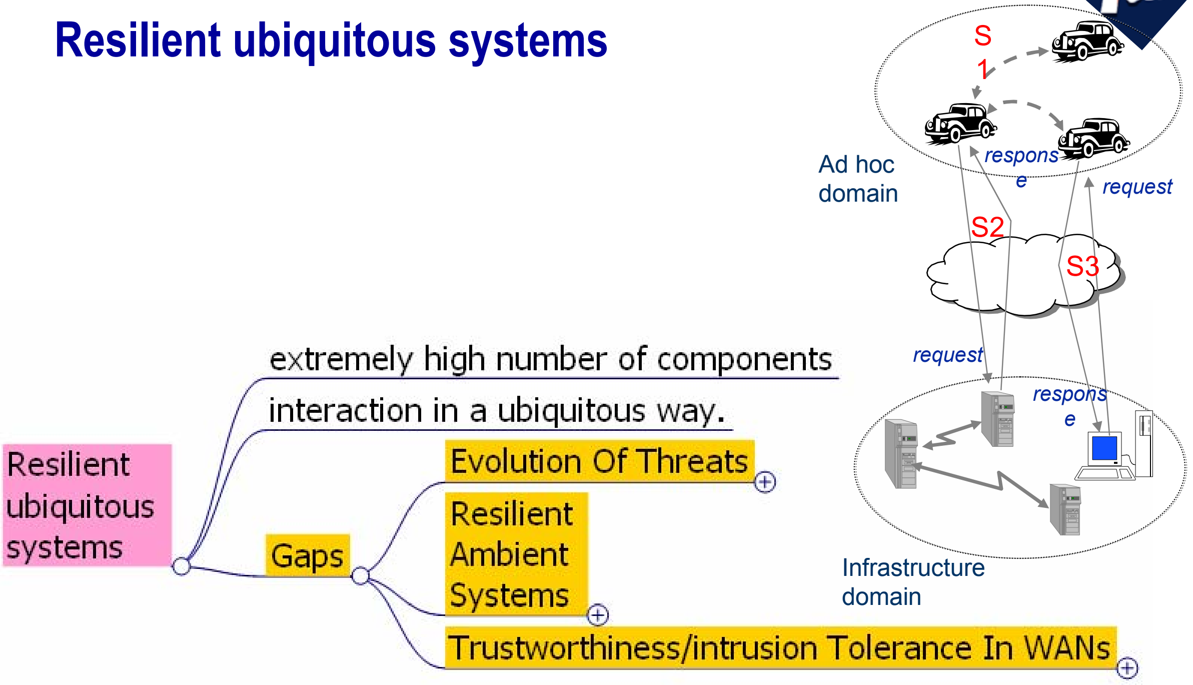
pataric@mit.bme.hu

- András Kövi, Diola Abi Haidar, Roberto Baldoni, Sandra Basnyat, Christian Cachin, Miguel Correia, Marc Dacier, Jean-Charles Fabre, László Gönczy, Fabrizio Grandoni, Michael Harrisson, Marc-Olivier Killijian, Chidung Lac, David Navarre, Nuno F. Neves, Péter Pásztor, Gergely Pintér, Petern Popov, David Powell, HariGovind Ramasamy, Michel Raynal, Yves Roudier, Matthieu Roy, Paulo Sousa, Mark-Alexander Sujan
- Review team
- University of Budapest, City University, LAAS-CNRS, University of Pisa, Eurecom, France Telecom, IBM, University of Roma, IRIT, University of Lisbon, University of Newcastle, IRISA, University of Warwick

Evolvability

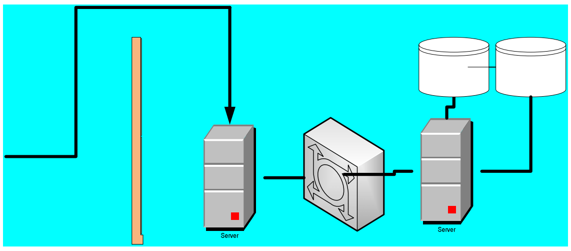


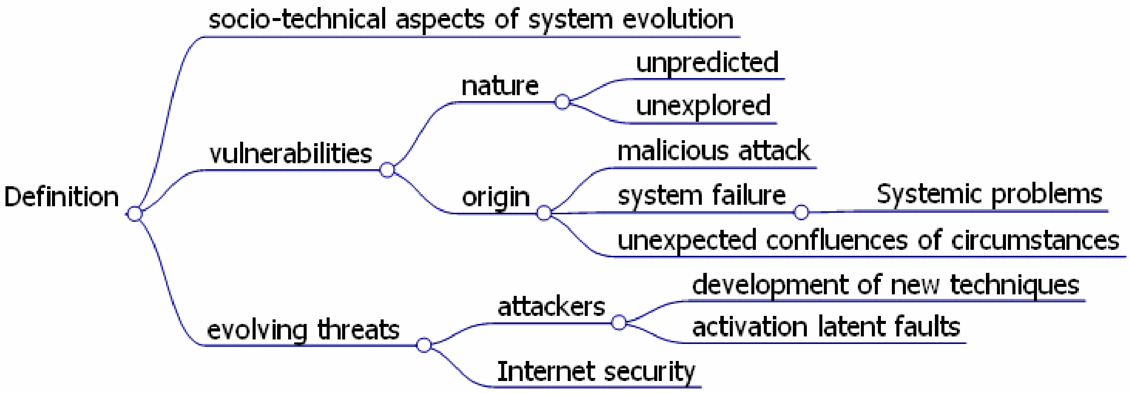
Resilient ubiquitous systems



S
1
respons
e
request
Ad hoc
domain
S2
S3
request
respons
e
Infrastructure
domain
Resilient ubiquitous systems
extremely high number of components
interaction in a ubiquitous way.
Gaps
Evolution Of Threats
Resilient Ambient Systems
Trustworthiness/intrusion Tolerance In WANs

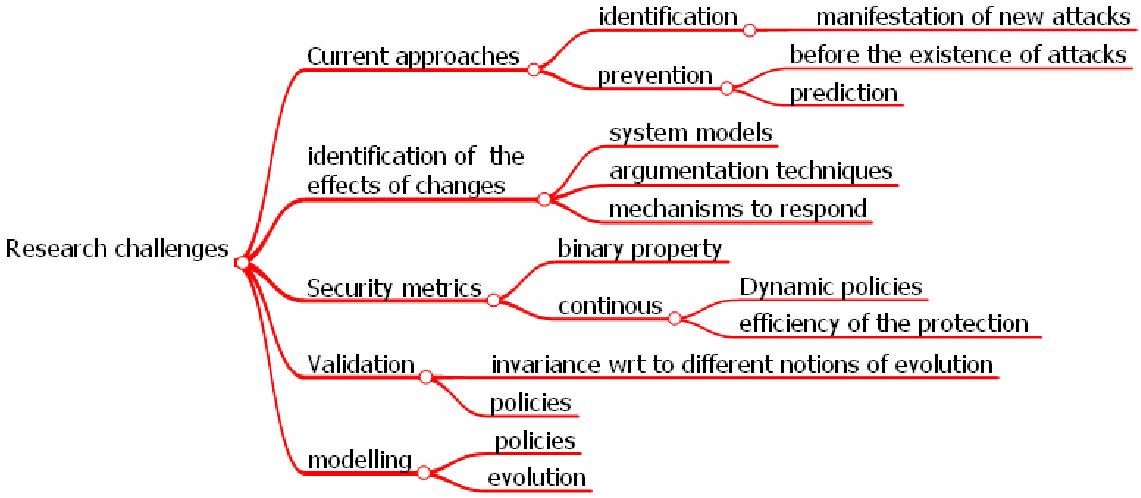
Evolution Of Threats





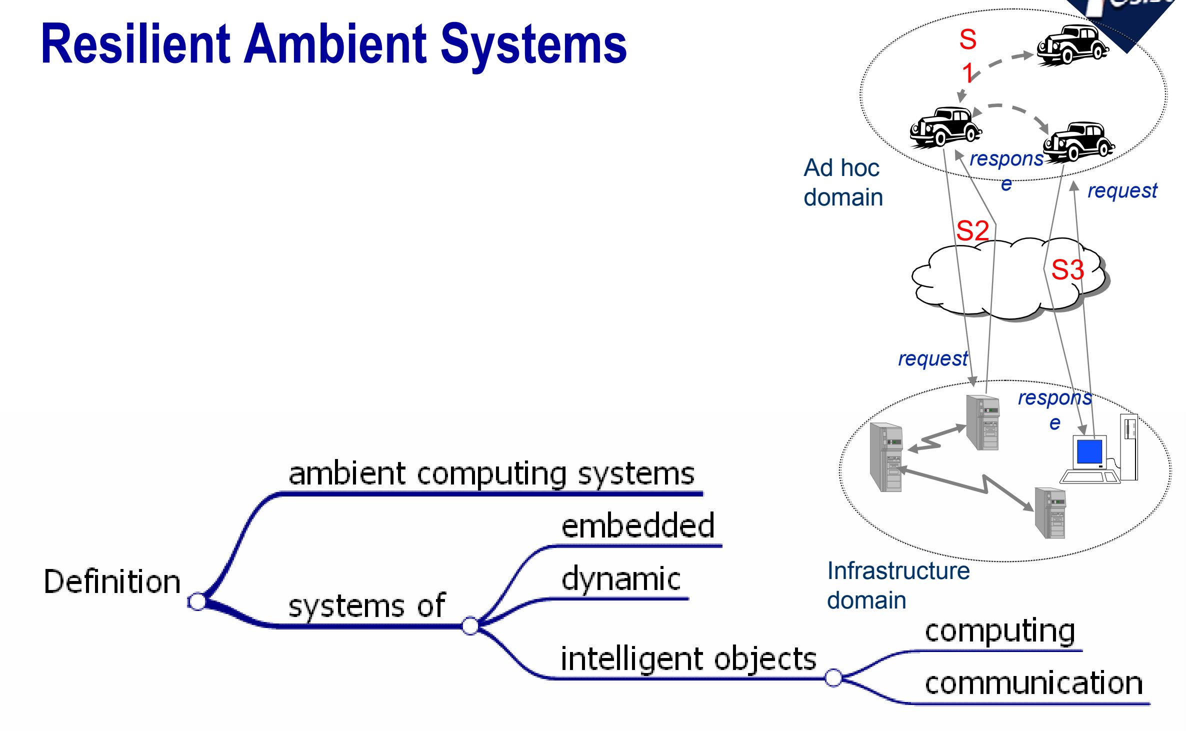
- Definition
  - socio-technical aspects of system evolution
  - vulnerabilities
    - nature
      - unpredicted
      - unexplored
    - origin
      - malicious attack
      - system failure
        - Systemic problems
      - unexpected confluences of circumstances
  - evolving threats
    - attackers
      - development of new techniques
      - activation latent faults
    - Internet security

Evolution Of Threats - Research challenges

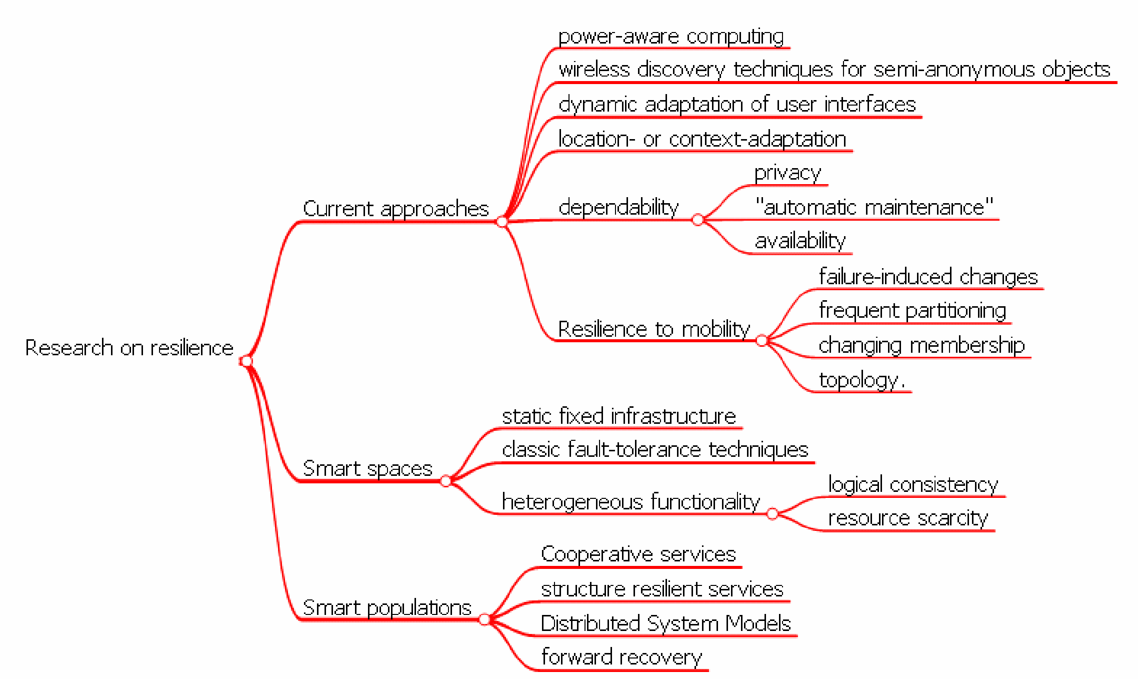


- Research challenges
  - Current approaches
    - identification
      - manifestation of new attacks
    - prevention
      - before the existence of attacks
      - prediction
  - identification of the effects of changes
    - system models
    - argumentation techniques
    - mechanisms to respond
  - Security metrics
    - binary property
    - continous
      - Dynamic policies
      - efficiency of the protection
  - Validation
    - invariance wrt to different notions of evolution
    - policies
  - modelling
    - policies
    - evolution

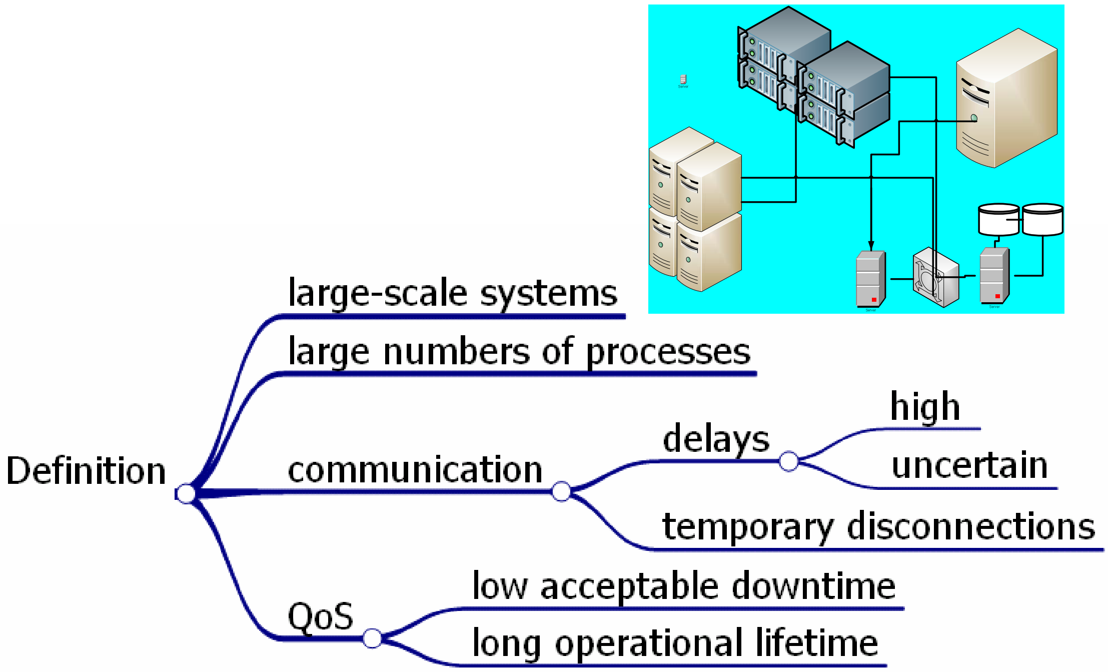
Resilient Ambient Systems



Resilient Ambient Systems - Research challenges

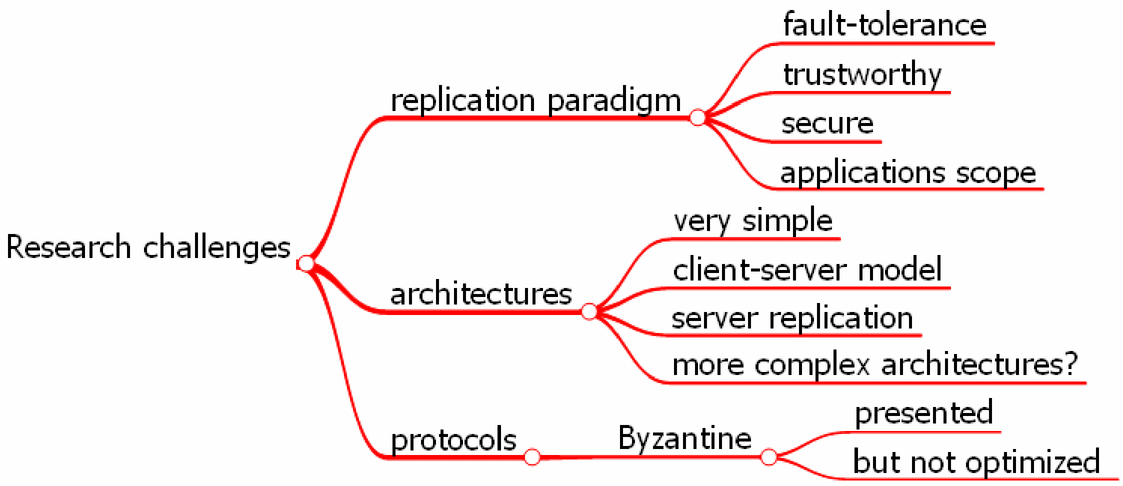


Trustworthiness/intrusion Tolerance in WANs



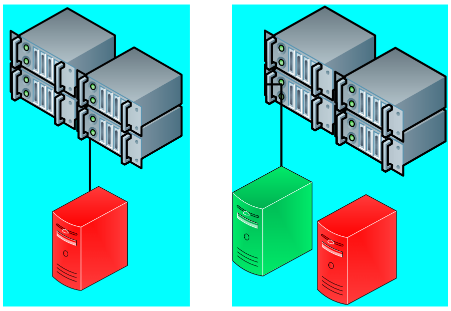
- Definition
  - large-scale systems
  - large numbers of processes
  - communication
    - delays
      - high
      - uncertain
    - temporary disconnections
  - QoS
    - low acceptable downtime
    - long operational lifetime

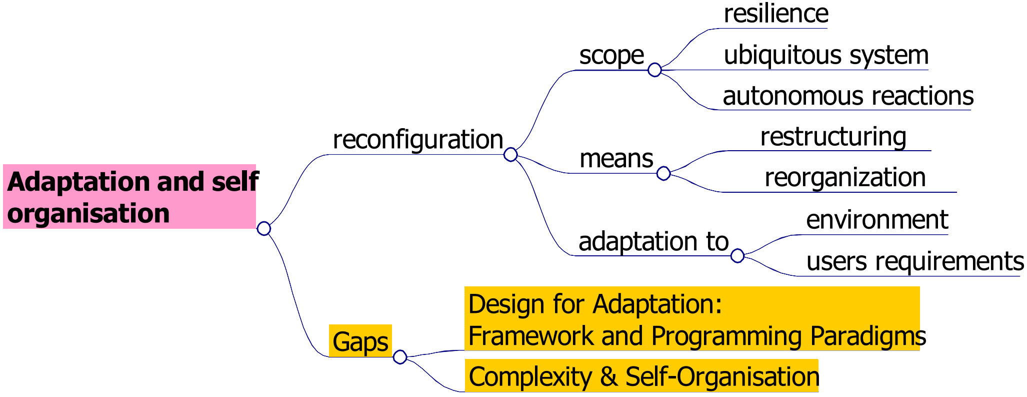
Trustworthiness/intrusion Tolerance in WANs – Research challenges



- Research challenges
  - replication paradigm
    - fault-tolerance
    - trustworthy
    - secure
    - applications scope
  - architectures
    - very simple
    - client-server model
    - server replication
    - more complex architectures?
  - protocols
    - Byzantine
      - presented
      - but not optimized

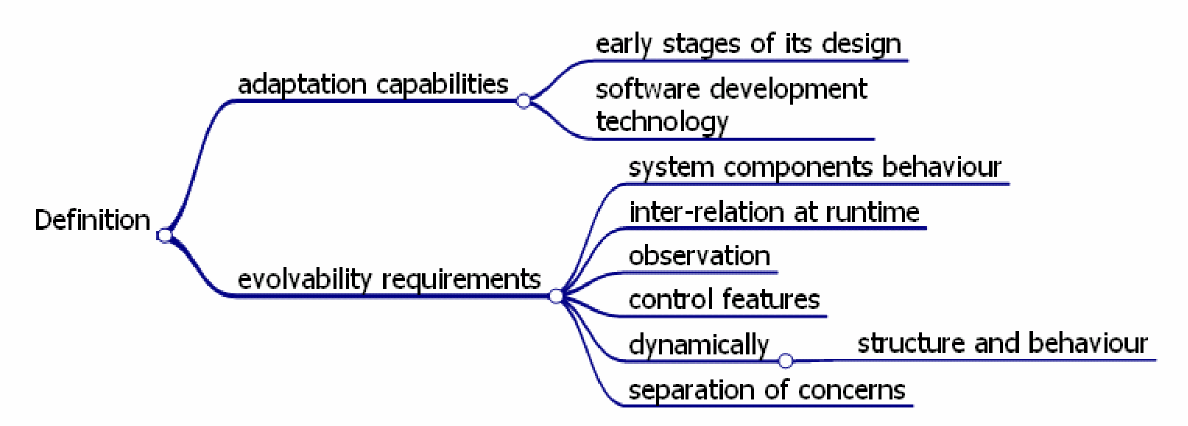
Adaptation





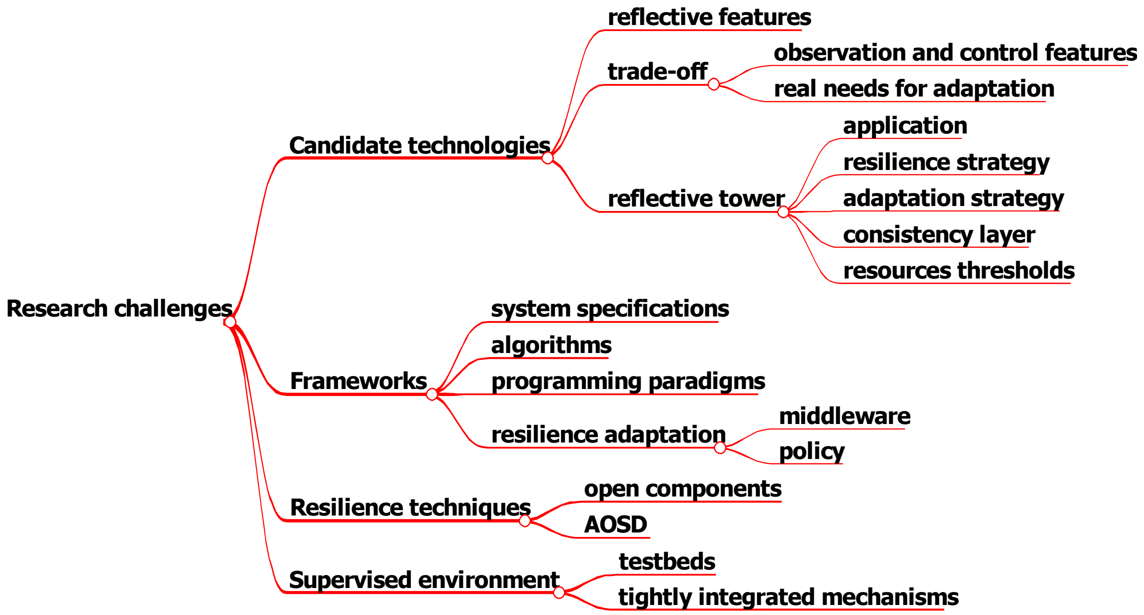
- Adaptation and self organisation
  - reconfiguration
    - scope
      - resilience
      - ubiquitous system
      - autonomous reactions
    - means
      - restructuring
      - reorganization
    - adaptation to
      - environment
      - users requirements
  - Gaps
    - Design for Adaptation: Framework and Programming Paradigms
    - Complexity & Self-Organisation

Design for Adaptation



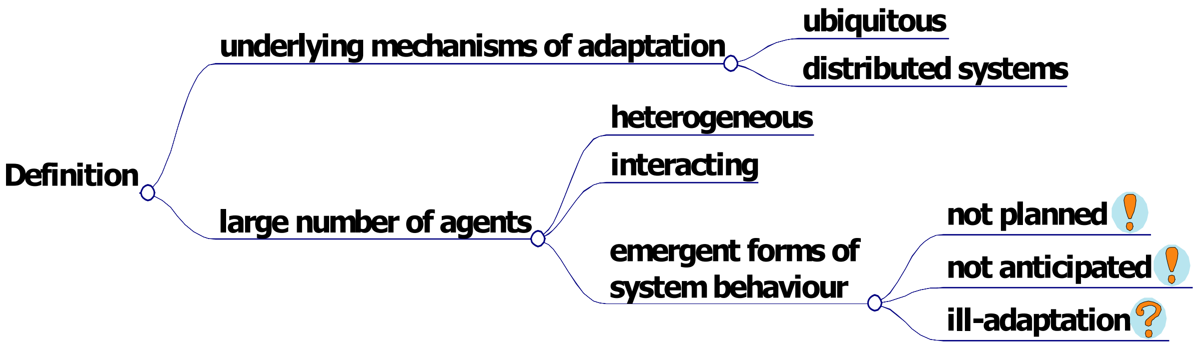
- Definition
  - adaptation capabilities
    - early stages of its design
    - software development technology
  - evolvability requirements
    - system components behaviour
    - inter-relation at runtime
    - observation
    - control features
    - dynamically
      - structure and behaviour
    - separation of concerns

Design for Adaptation – Research challanges



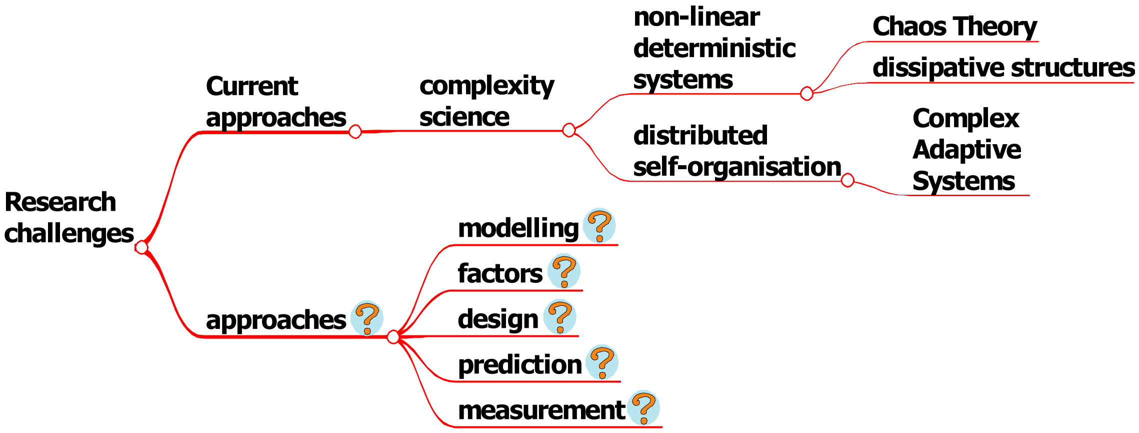
- Research challenges
  - Candidate technologies
    - reflective features
    - trade-off
      - observation and control features
      - real needs for adaptation
    - reflective tower
      - application
      - resilience strategy
      - adaptation strategy
      - consistency layer
      - resources thresholds
  - Frameworks
    - system specifications
    - algorithms
    - programming paradigms
    - resilience adaptation
      - middleware
      - policy
  - Resilience techniques
    - open components
    - AOSD
  - Supervised environment
    - testbeds
    - tightly integrated mechanisms

Complexity & Self-organization



- Definition
  - underlying mechanisms of adaptation
    - ubiquitous
    - distributed systems
  - large number of agents
    - heterogeneous
    - interacting
    - emergent forms of system behaviour
      - not planned !
      - not anticipated !
      - ill-adaptation ?

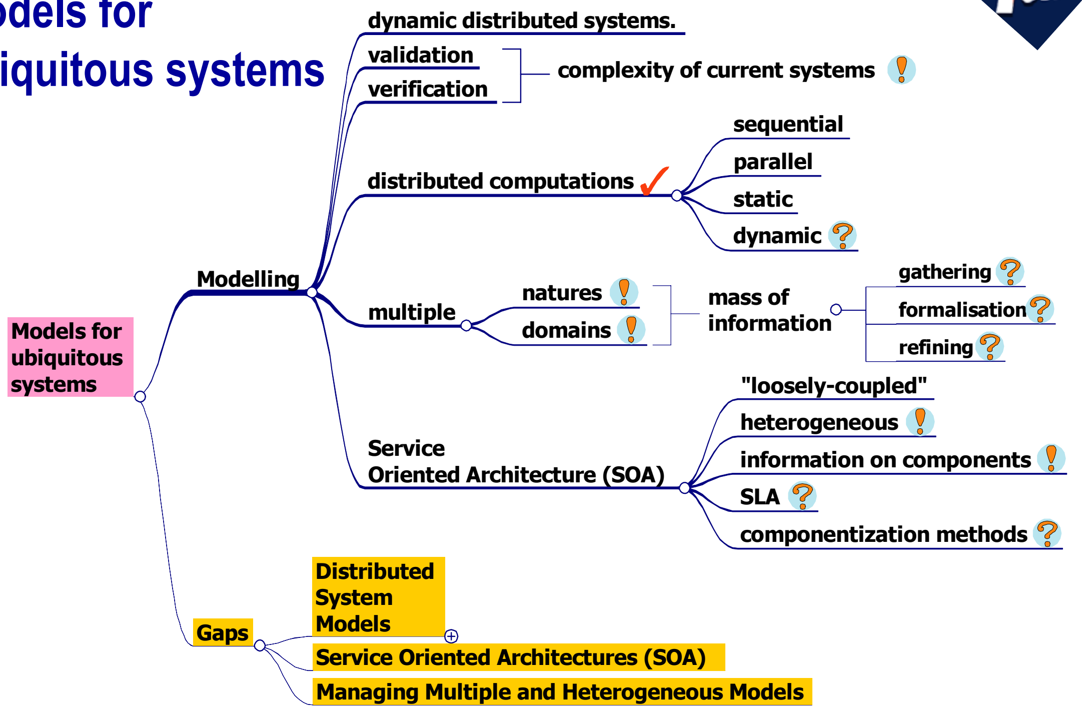
Complexity & Self-organization – Research challenges



Research challenges

- Current approaches
  - complexity science
    - non-linear deterministic systems
      - Chaos Theory
      - dissipative structures
    - distributed self-organisation
      - Complex Adaptive Systems
- approaches ?
  - modelling ?
  - factors ?
  - design ?
  - prediction ?
  - measurement ?

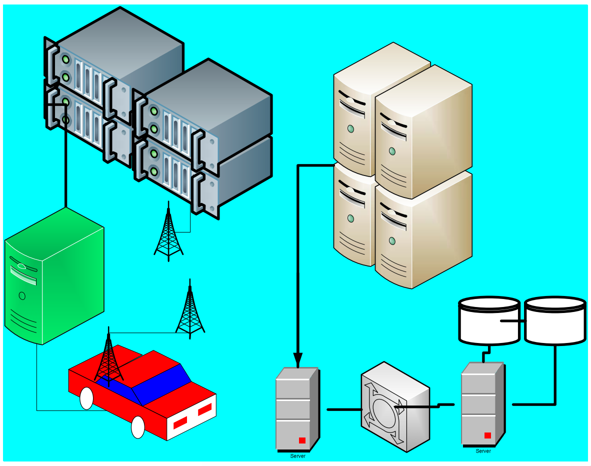
Models for ubiquitous systems

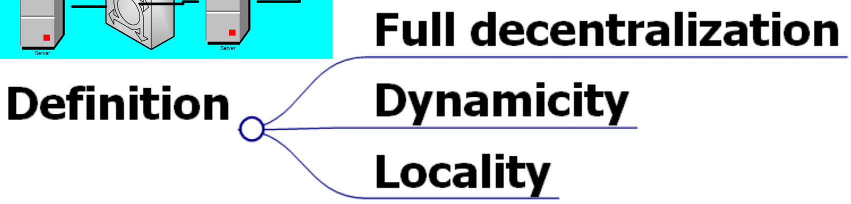


Models for ubiquitous systems

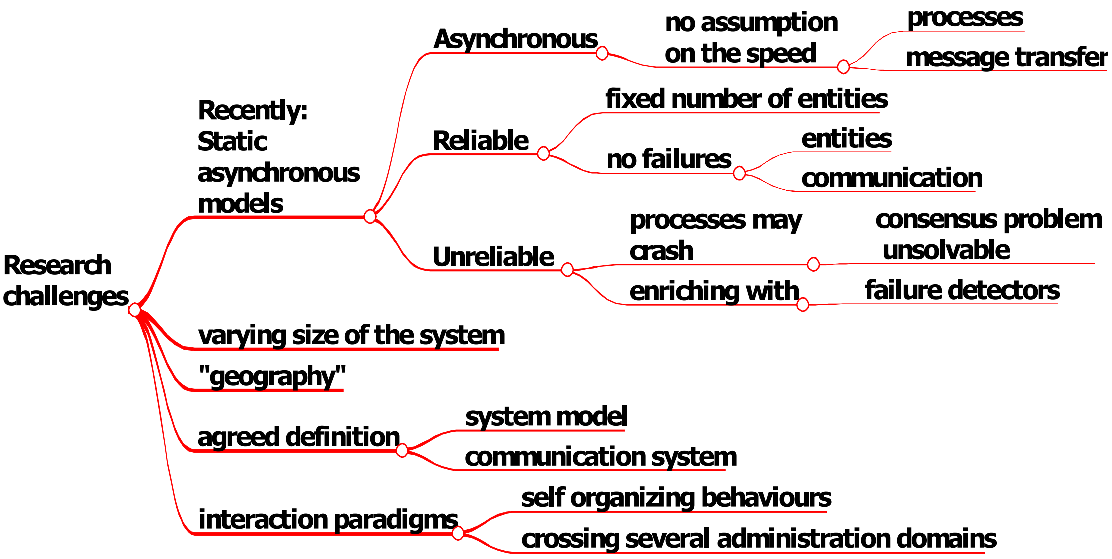
- Modelling
  - dynamic distributed systems.
  - validation
  - verification
    - complexity of current systems !
  - distributed computations ✓
    - sequential
    - parallel
    - static
    - dynamic ?
  - multiple
    - natures !
    - domains !
      - mass of information
        - gathering ?
        - formalisation ?
        - refining ?
  - Service Oriented Architecture (SOA)
    - "loosely-coupled"
    - heterogeneous !
    - information on components !
    - SLA ?
    - componentization methods ?
- Gaps
  - Distributed System Models ⊕
  - Service Oriented Architectures (SOA)
  - Managing Multiple and Heterogeneous Models

Distributed System Models

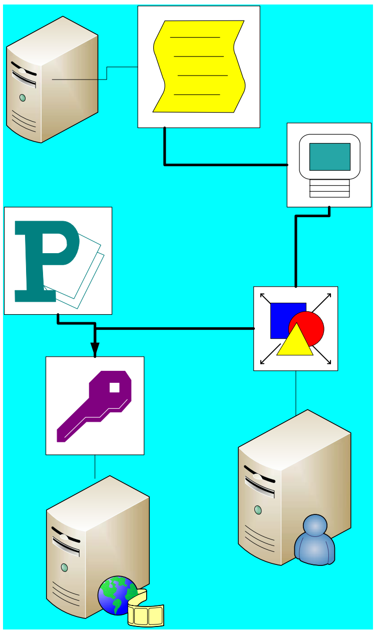


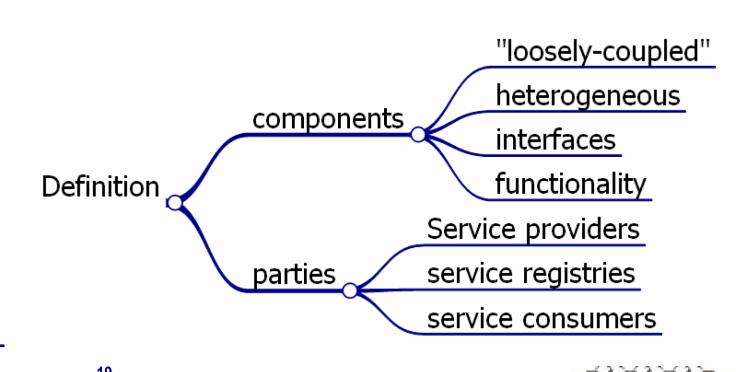


Distributed System Models - Research challenges



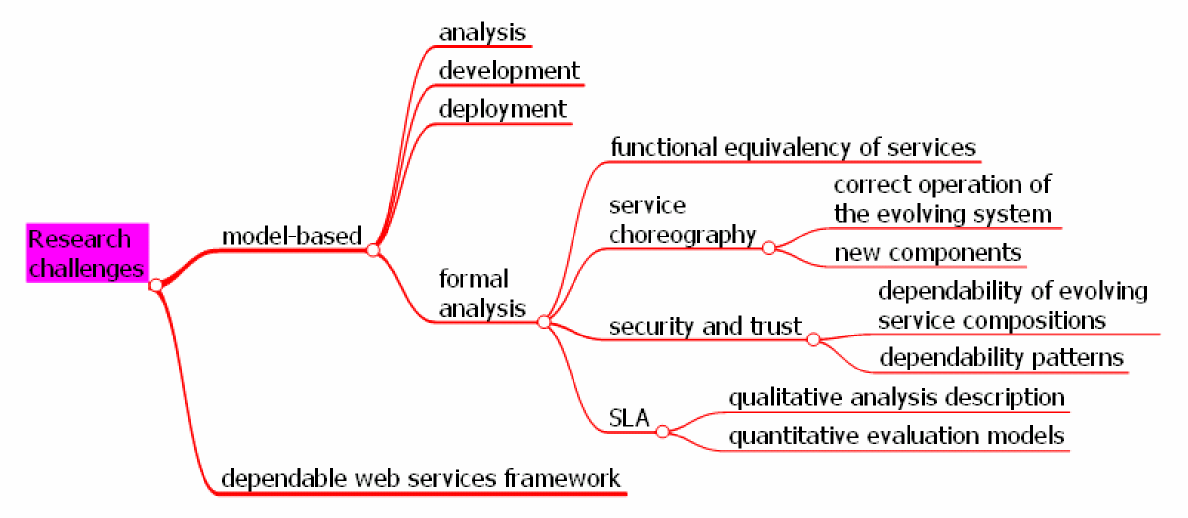
SOA





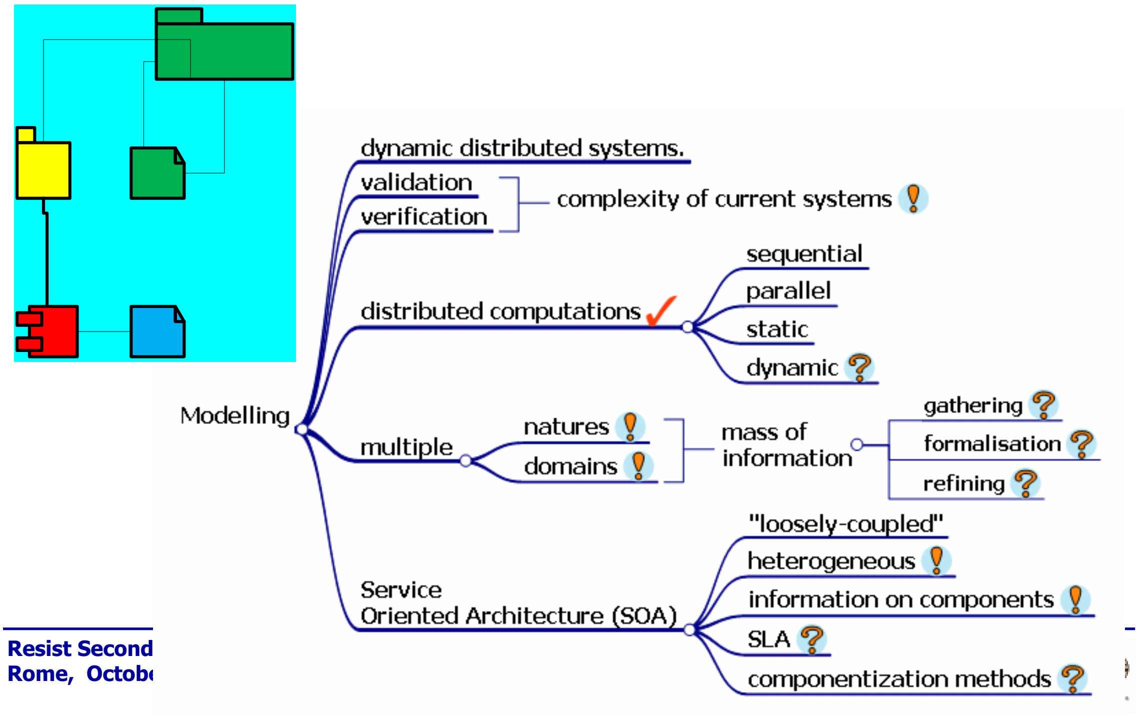
- Definition
  - components
    - "loosely-coupled"
    - heterogeneous
    - interfaces
    - functionality
  - parties
    - Service providers
    - service registries
    - service consumers

SOA – Research challenges



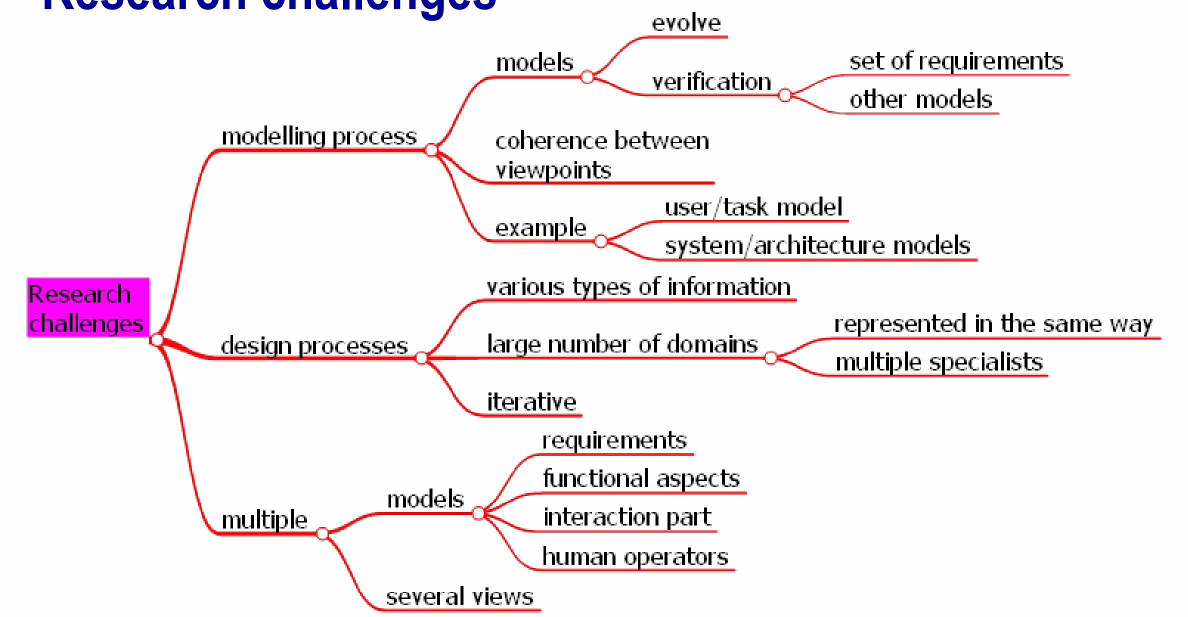
- Research challenges
  - model-based
    - analysis
    - development
    - deployment
    - formal analysis
      - functional equivalency of services
      - service choreography
        - correct operation of the evolving system
        - new components
      - security and trust
        - dependability of evolving service compositions
        - dependability patterns
      - SLA
        - qualitative analysis description
        - quantitative evaluation models
  - dependable web services framework

Managing Multiple and Heterogeneous Models



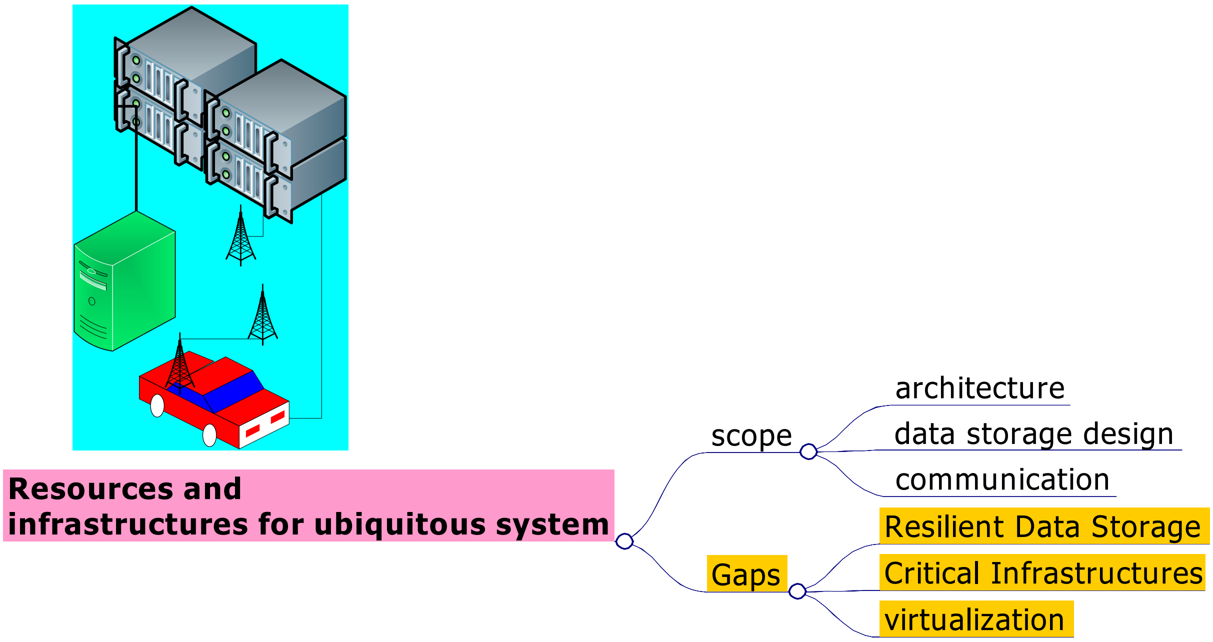
- Modelling
  - dynamic distributed systems.
  - validation
  - verification
    - complexity of current systems !
  - distributed computations ✓
    - sequential
    - parallel
    - static
    - dynamic ?
  - multiple
    - natures !
    - domains !
      - mass of information
        - gathering ?
        - formalisation ?
        - refining ?
  - Service Oriented Architecture (SOA)
    - "loosely-coupled"
    - heterogeneous !
    - information on components !
    - SLA ?
    - componentization methods ?

Managing Multiple and Heterogeneous Models – Research challenges



- Research challenges
  - modelling process
    - models
      - evolve
      - verification
        - set of requirements
        - other models
    - coherence between viewpoints
    - example
      - user/task model
      - system/architecture models
  - design processes
    - various types of information
    - large number of domains
      - represented in the same way
      - multiple specialists
    - iterative
  - multiple
    - models
      - requirements
      - functional aspects
      - interaction part
      - human operators
    - several views

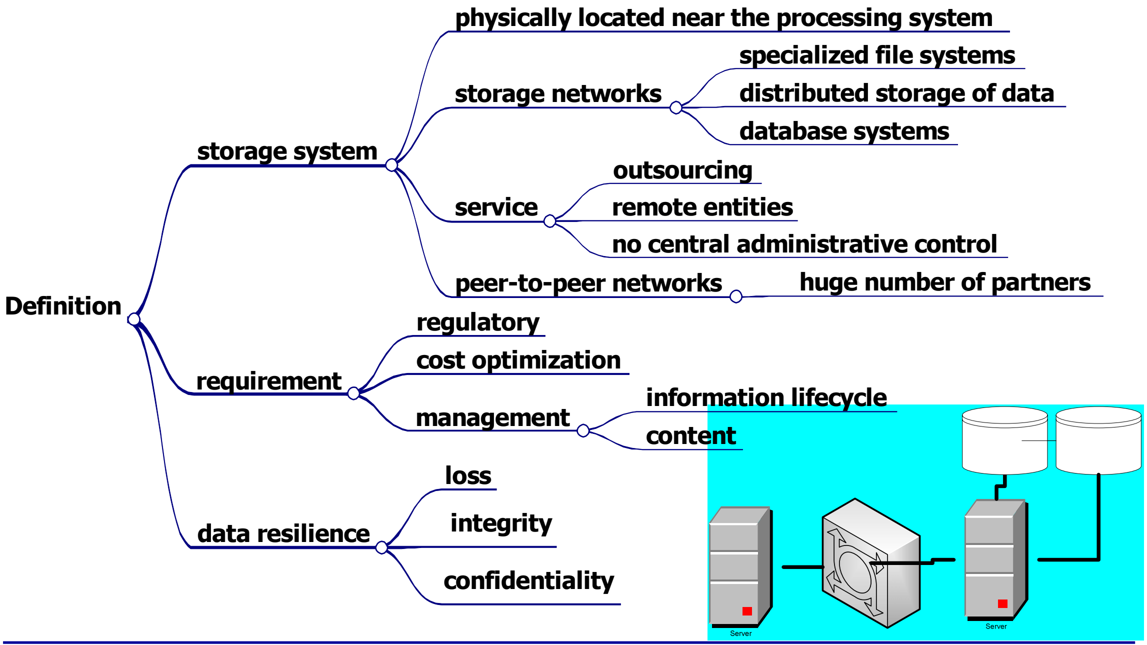
Resources & infrastructures for ubiquitous systems



Resources and infrastructures for ubiquitous system

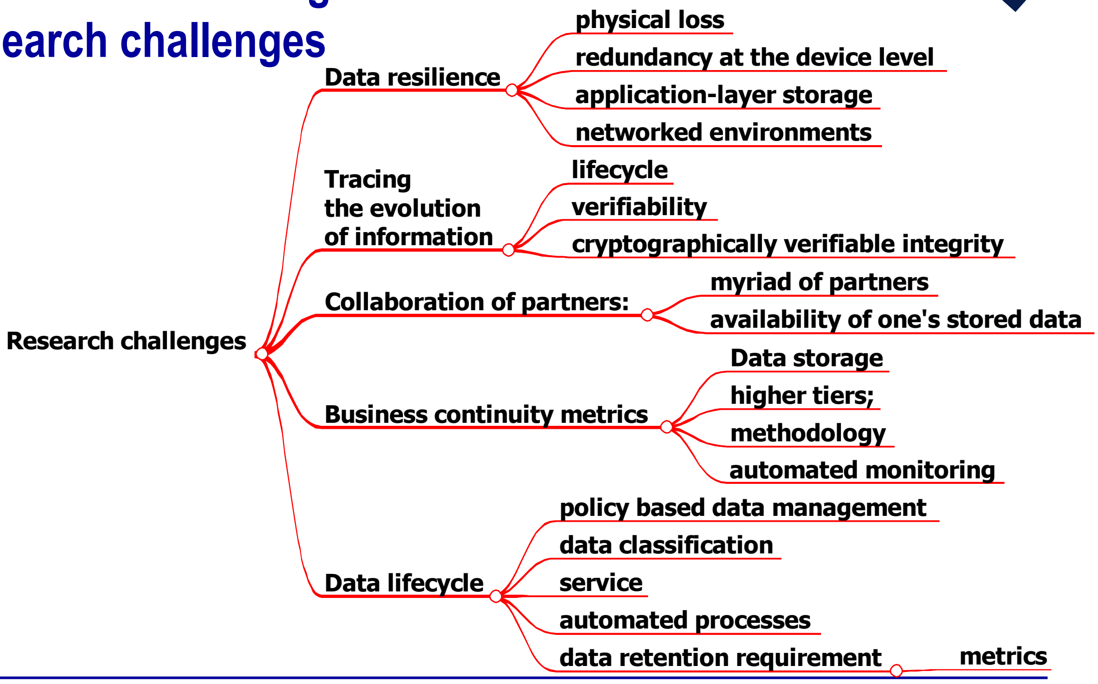
- scope
  - architecture
  - data storage design
  - communication
- Gaps
  - Resilient Data Storage
  - Critical Infrastructures
  - virtualization

Resilient Data Storage



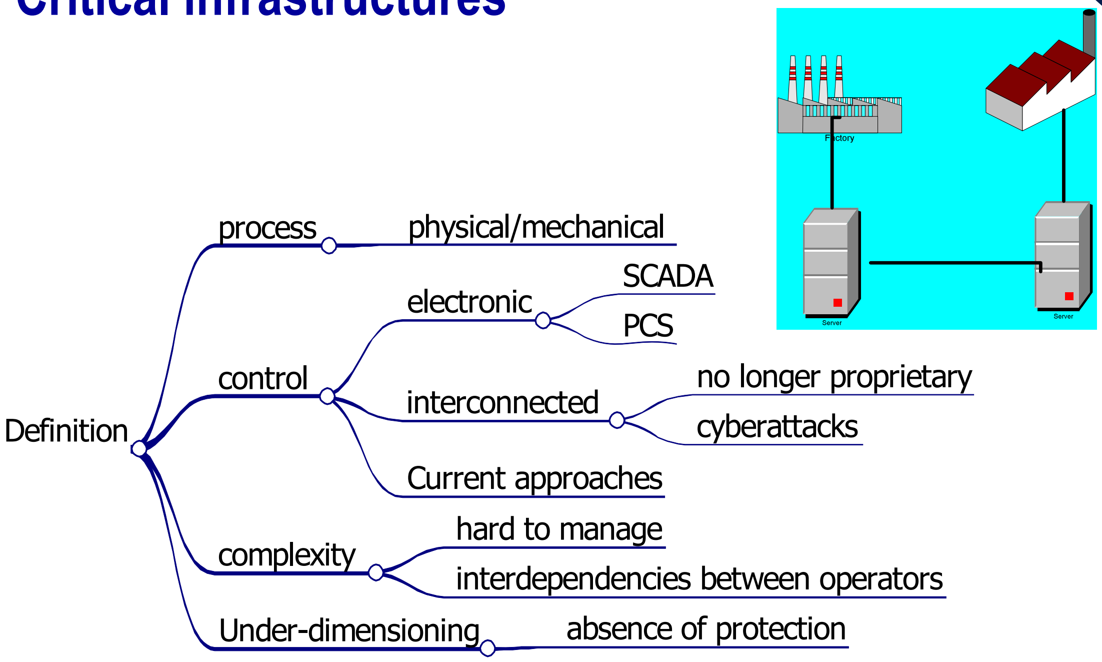
- Definition
  - storage system
    - physically located near the processing system
    - storage networks
      - specialized file systems
      - distributed storage of data
      - database systems
    - service
      - outsourcing
      - remote entities
      - no central administrative control
    - peer-to-peer networks
      - huge number of partners
  - requirement
    - regulatory
    - cost optimization
    - management
      - information lifecycle
      - content
  - data resilience
    - loss
    - integrity
    - confidentiality

Resilient Data Storage – Research challenges

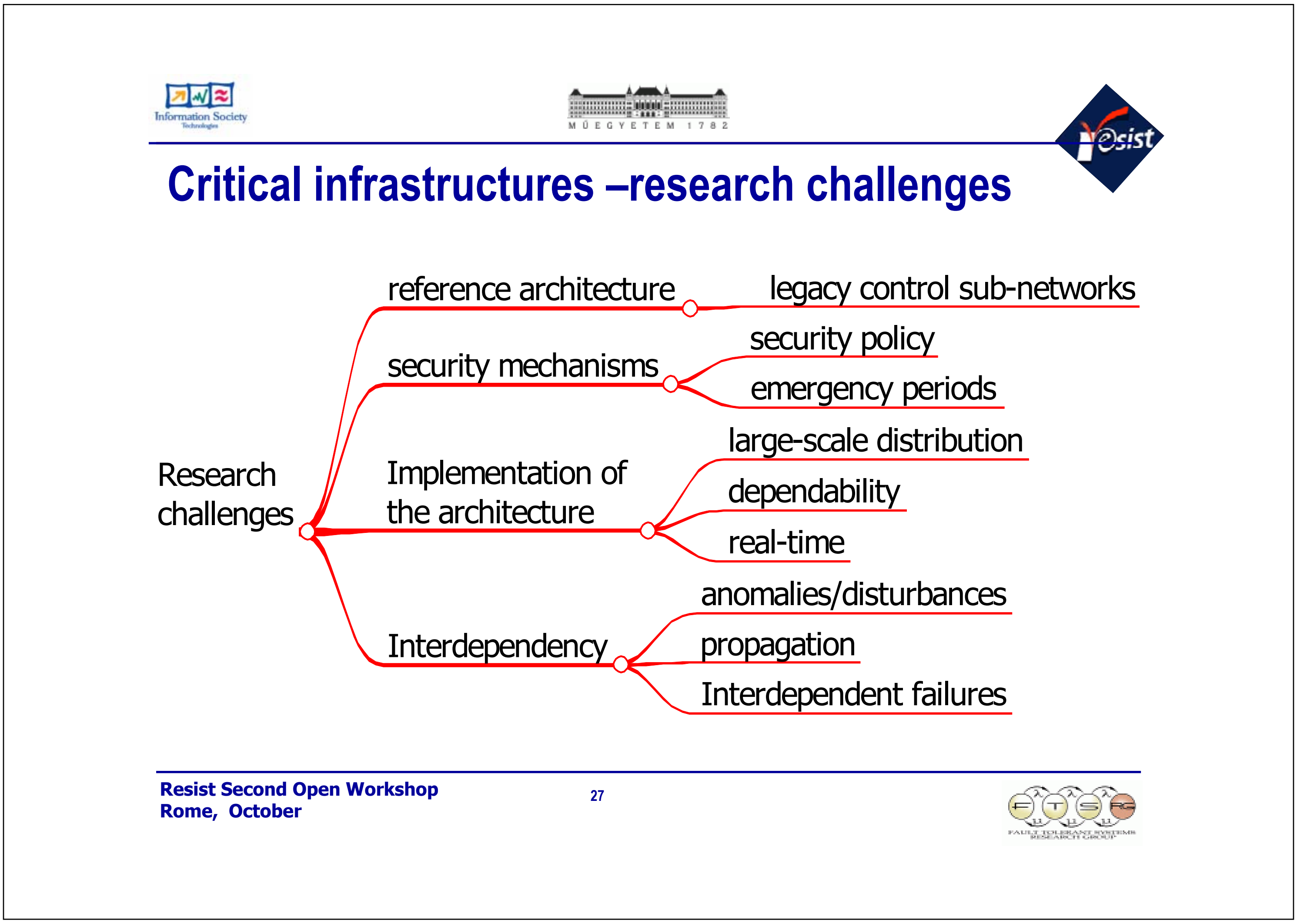


- Research challenges
  - Data resilience
    - physical loss
    - redundancy at the device level
    - application-layer storage
    - networked environments
  - Tracing the evolution of information
    - lifecycle
    - verifiability
    - cryptographically verifiable integrity
  - Collaboration of partners:
    - myriad of partners
    - availability of one's stored data
  - Business continuity metrics
    - Data storage
    - higher tiers;
    - methodology
    - automated monitoring
  - Data lifecycle
    - policy based data management
    - data classification
    - service
    - automated processes
    - data retention requirement
      - metrics

Critical infrastructures

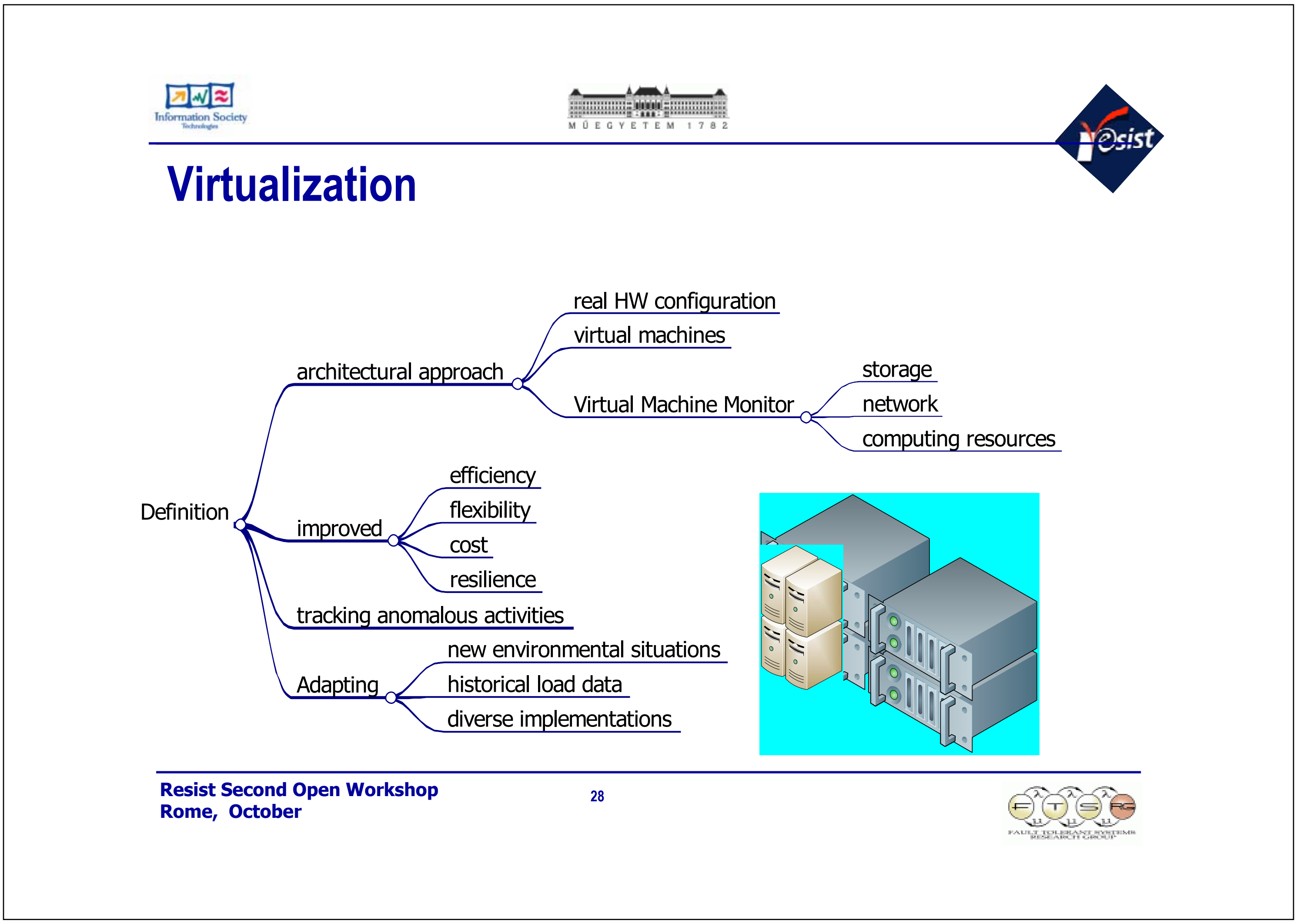


- Definition
  - process
    - physical/mechanical
  - control
    - electronic
      - SCADA
      - PCS
    - interconnected
      - no longer proprietary
      - cyberattacks
    - Current approaches
  - complexity
    - hard to manage
    - interdependencies between operators
  - Under-dimensioning
    - absence of protection



Critical infrastructures –research challenges

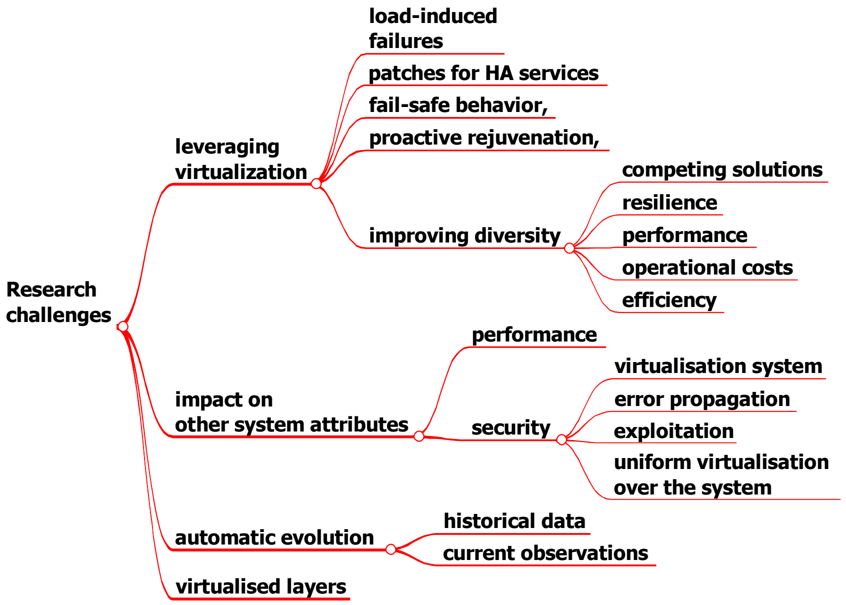
- Research challenges
  - reference architecture
    - legacy control sub-networks
  - security mechanisms
    - security policy
    - emergency periods
  - Implementation of the architecture
    - large-scale distribution
    - dependability
    - real-time
  - Interdependency
    - anomalies/disturbances
    - propagation
    - Interdependent failures



Virtualization

- Definition
  - architectural approach
    - real HW configuration
    - virtual machines
    - Virtual Machine Monitor
      - storage
      - network
      - computing resources
  - improved
    - efficiency
    - flexibility
    - cost
    - resilience
  - tracking anomalous activities
  - Adapting
    - new environmental situations
    - historical load data
    - diverse implementations

Virtualization – Research challanges



Research challenges

leveraging virtualization

load-induced failures

patches for HA services

fail-safe behavior,

proactive rejuvenation,

improving diversity

competing solutions

resilience

performance

operational costs

efficiency

impact on other system attributes

performance

security

virtualisation system

error propagation

exploitation

uniform virtualisation over the system

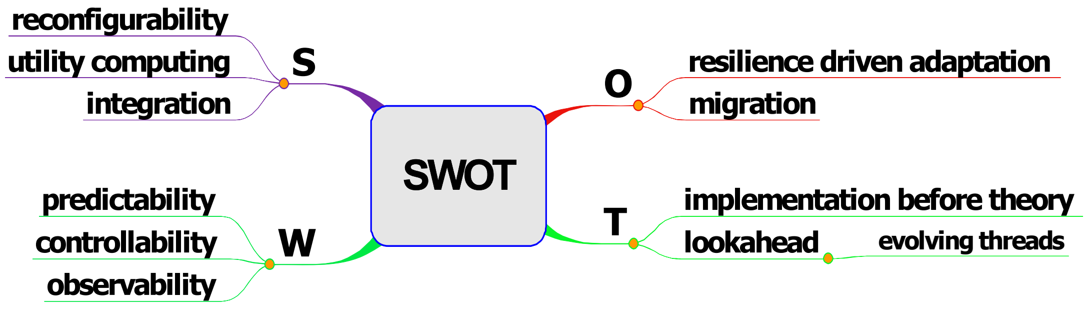
automatic evolution

historical data

current observations

virtualised layers

Summary



SWOT

S

reconfigurability

utility computing

integration

W

predictability

controllability

observability

O

resilience driven adaptation

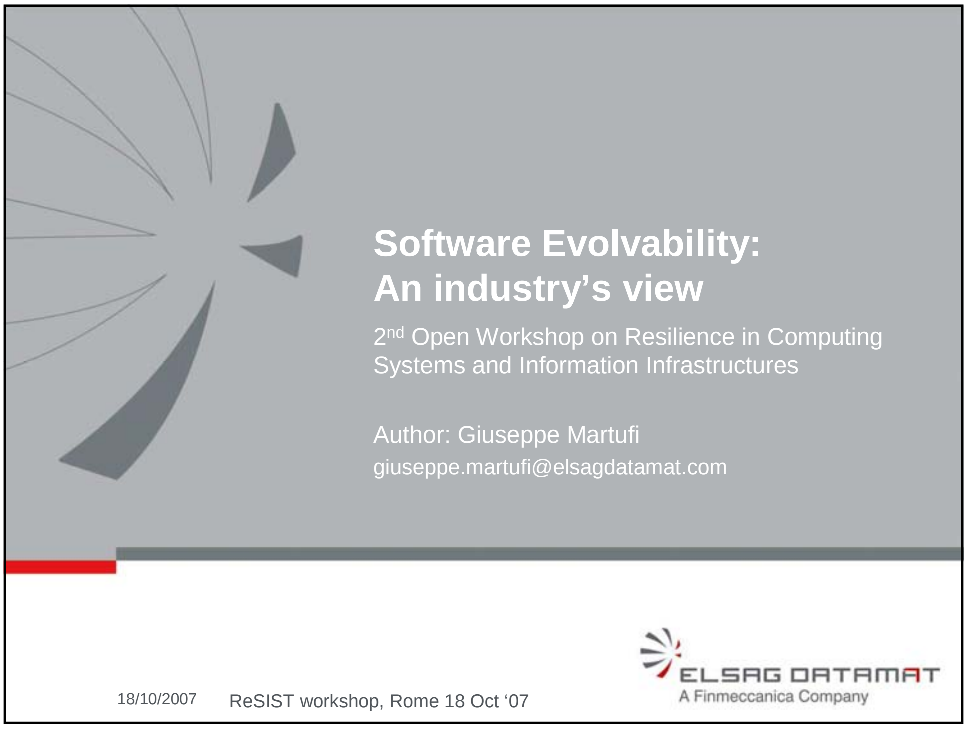
migration

T

implementation before theory

lookahead

evolving threads



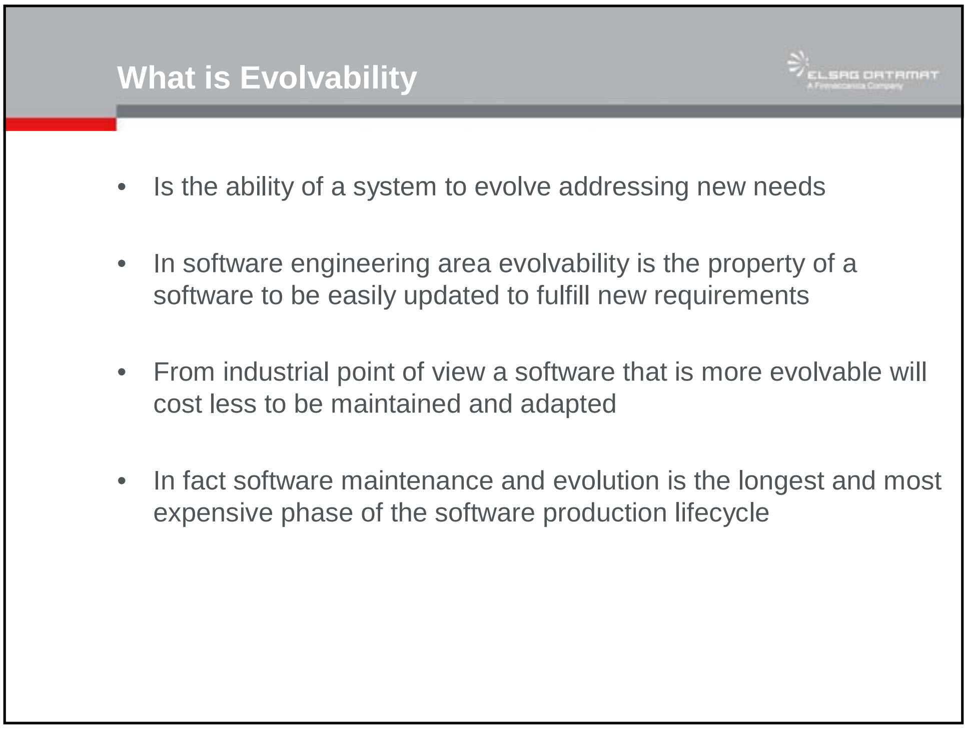
Software Evolvability: An industry's view

2nd Open Workshop on Resilience in Computing Systems and Information Infrastructures

Author: Giuseppe Martufi
giuseppe.martufi@elsagdatamat.com

ELSAG DATAMAT
A Finmeccanica Company

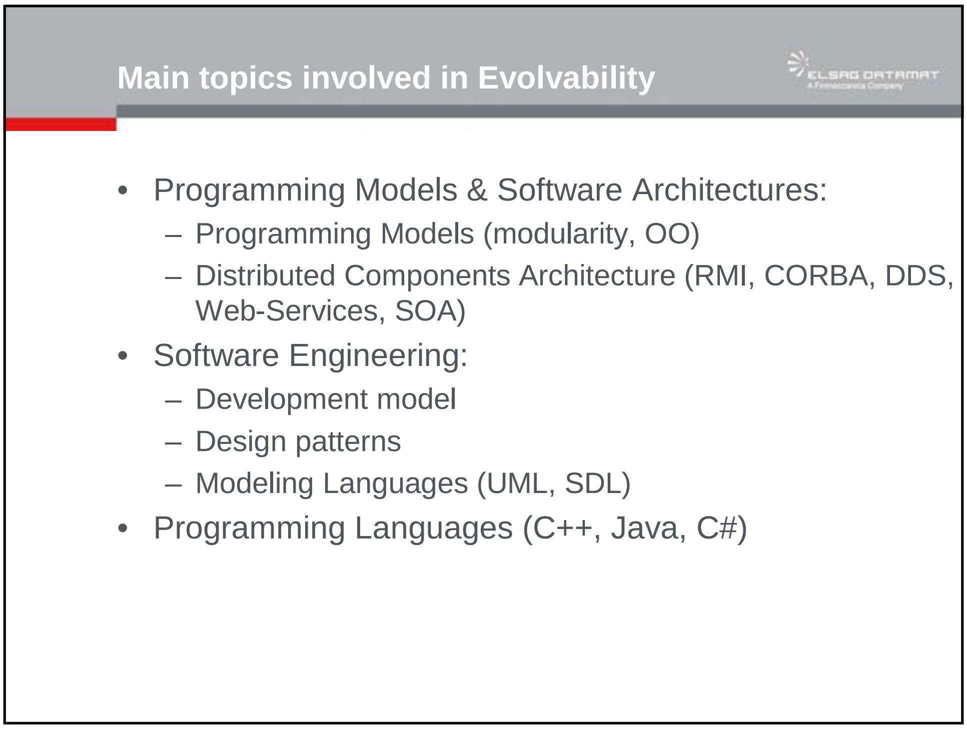
18/10/2007 ReSIST workshop, Rome 18 Oct '07



What is Evolvability

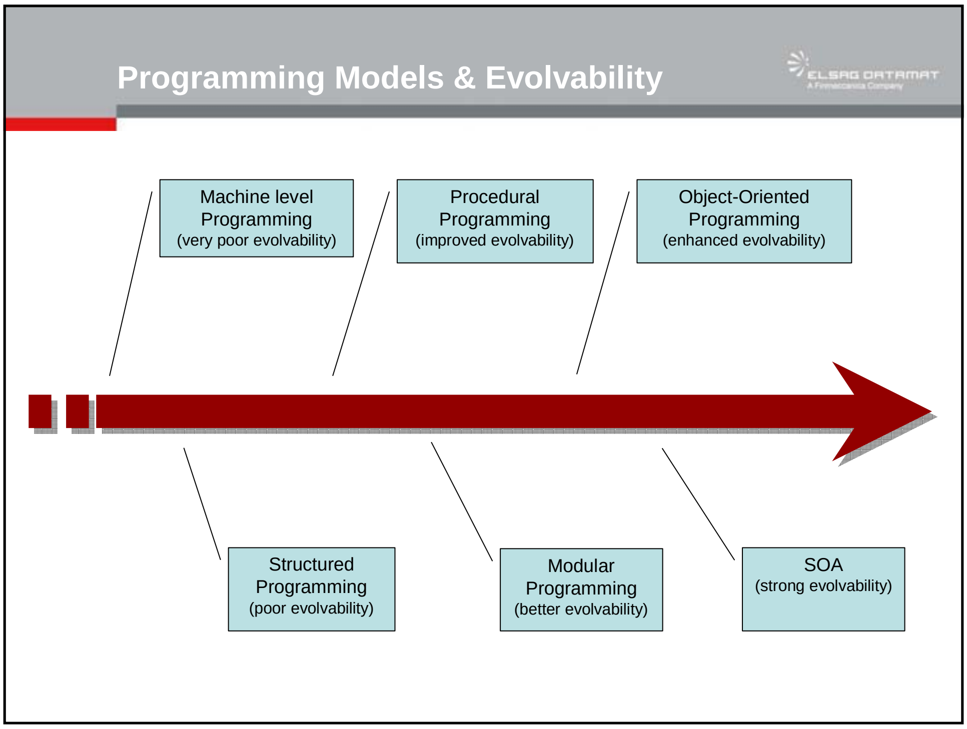
ELSAG DATAMAT
A Finmeccanica Company

- Is the ability of a system to evolve addressing new needs
- In software engineering area evolvability is the property of a software to be easily updated to fulfill new requirements
- From industrial point of view a software that is more evolvable will cost less to be maintained and adapted
- In fact software maintenance and evolution is the longest and most expensive phase of the software production lifecycle



Main topics involved in Evolvability

- Programming Models & Software Architectures:
  - Programming Models (modularity, OO)
  - Distributed Components Architecture (RMI, CORBA, DDS, Web-Services, SOA)
- Software Engineering:
  - Development model
  - Design patterns
  - Modeling Languages (UML, SDL)
- Programming Languages (C++, Java, C#)



Programming Models & Evolvability

Machine level Programming (very poor evolvability)
Procedural Programming (improved evolvability)
Object-Oriented Programming (enhanced evolvability)
Structured Programming (poor evolvability)
Modular Programming (better evolvability)
SOA (strong evolvability)

Component based architectures & Evolvability

- A component-based application is evolvable if it is easily possible to exchange individual components without changing the others.
- Component "distance" is increasing:
  - a first stage all components were contained inside a file
  - in a second stage components have been spread out over a file system
  - the third stage is based upon components distributed over the network
  - in a fourth stage web-based service components are located in different administrated networks and domains, or the Internet (Web 2.0)

http://www.omg.org/

http://www.oasis-open.org/

New development models and Evolvability: Open Source

- Open Source is a community model
- Software development is distributed among programmers that enrich a common product
- Each programmer reuses existing code and improve components/applications based on his own needs
- Frequent sw releases and nightly builds contribute to fast evolution of a product
- Example: GNU/Linux, Apache web server, tomcat, JBoss AS

http://www.gnu.org/

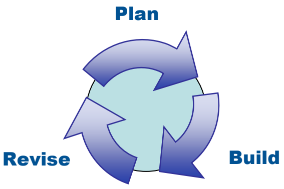
http://www.opensource.org/

The Apache Software Foundation
http://www.apache.org/

New development models and Evolvability: Agile programming

ELSAG DATAMAT
A Finmeccanica Company

- develop software in short amounts of time (iteration)
- iteration includes all the steps of a software project (planning, requirements analysis, design, coding, testing, and documentation)
- a single iteration could not generate a product having all requested functionality, but an intermediate release
- at each iteration software product can be adapted to the emergent state of the project



Agile Alliance

http://www.agilealliance.org/

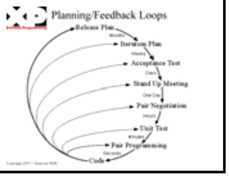
New development models and Evolvability: Extreme Programming (XP)

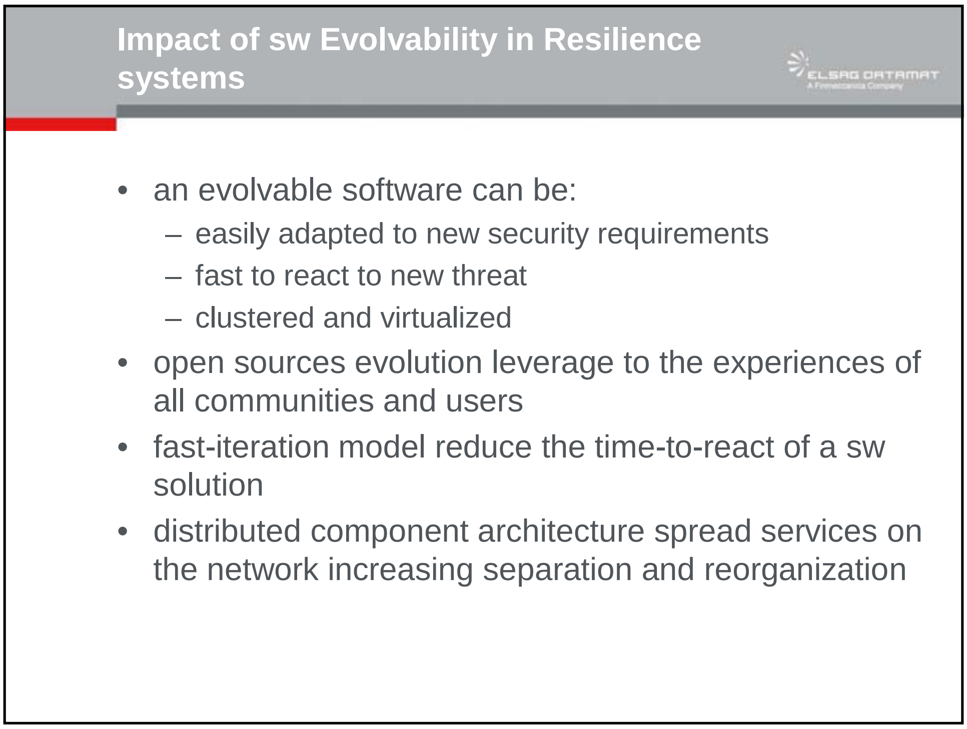
ELSAG DATAMAT
A Finmeccanica Company

- XP encourages starting with the simplest solution. Extra functionality can then be added later.
- It focuses on designing and coding for the needs of today instead of those of tomorrow
- XP can produce evolvable sw:
  - a system made for today does not mean a system closed to the future
  - possible future requirements might change before they become relevant
  - an evolvable approach does not require to address today all future requirements, but to be easy adaptable to new requirements arising tomorrow

Extreme Programming

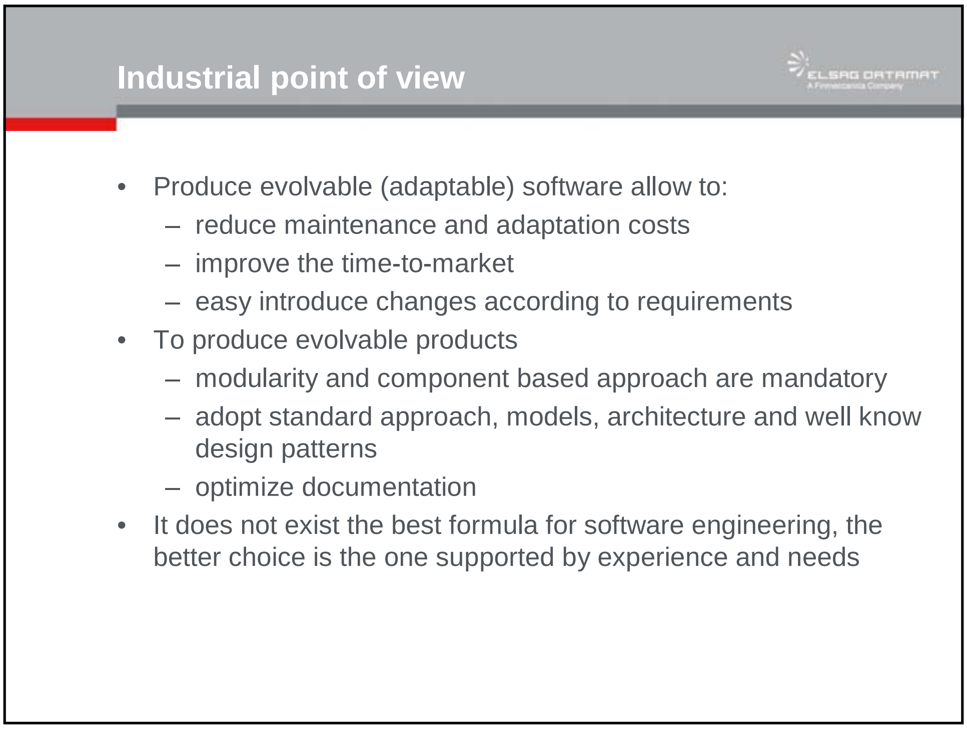
http://www.extremeprogramming.org/





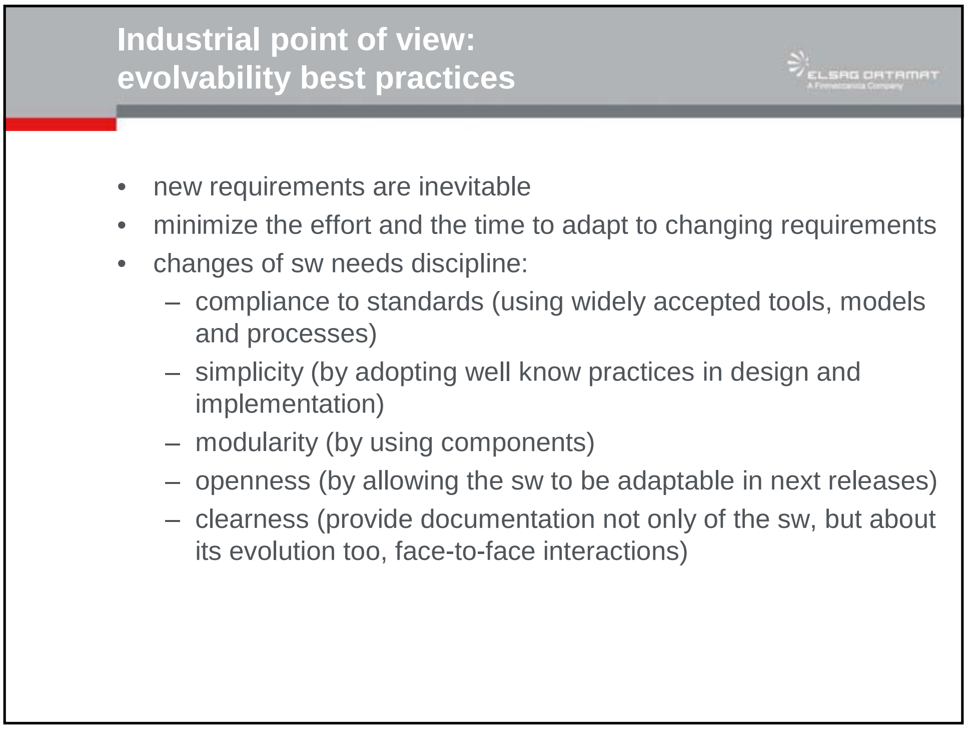
Impact of sw Evolvability in Resilience systems

- an evolvable software can be:
  - easily adapted to new security requirements
  - fast to react to new threat
  - clustered and virtualized
- open sources evolution leverage to the experiences of all communities and users
- fast-iteration model reduce the time-to-react of a sw solution
- distributed component architecture spread services on the network increasing separation and reorganization



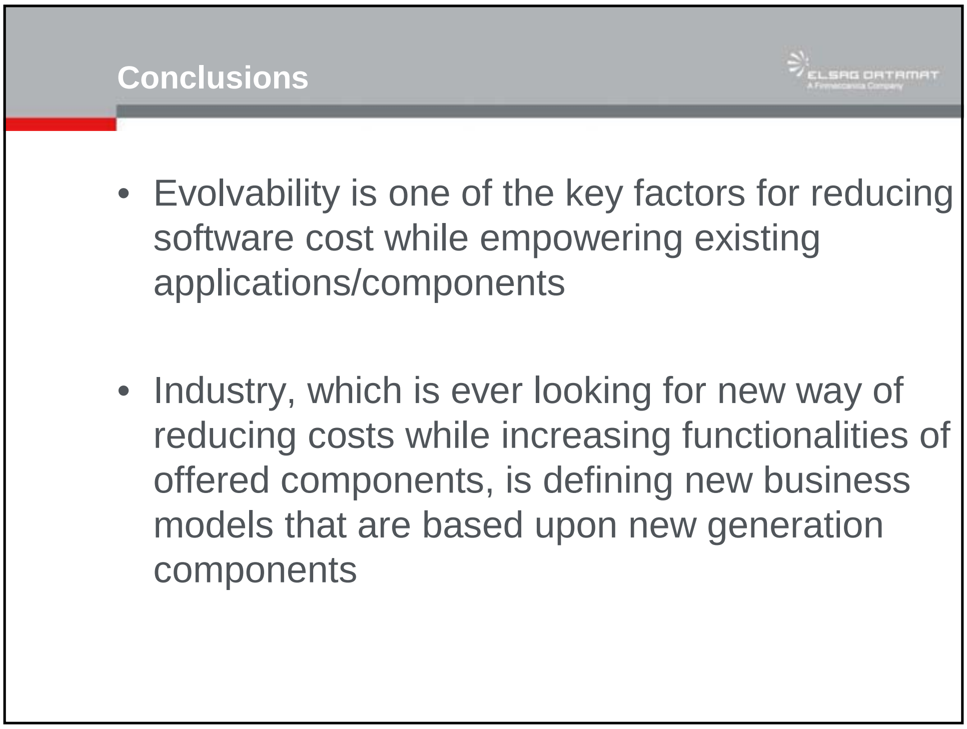
Industrial point of view

- Produce evolvable (adaptable) software allow to:
  - reduce maintenance and adaptation costs
  - improve the time-to-market
  - easy introduce changes according to requirements
- To produce evolvable products
  - modularity and component based approach are mandatory
  - adopt standard approach, models, architecture and well know design patterns
  - optimize documentation
- It does not exist the best formula for software engineering, the better choice is the one supported by experience and needs



Industrial point of view: evolvability best practices

- new requirements are inevitable
- minimize the effort and the time to adapt to changing requirements
- changes of sw needs discipline:
  - compliance to standards (using widely accepted tools, models and processes)
  - simplicity (by adopting well know practices in design and implementation)
  - modularity (by using components)
  - openness (by allowing the sw to be adaptable in next releases)
  - clearness (provide documentation not only of the sw, but about its evolution too, face-to-face interactions)



Conclusions

- Evolvability is one of the key factors for reducing software cost while empowering existing applications/components
- Industry, which is ever looking for new way of reducing costs while increasing functionalities of offered components, is defining new business models that are based upon new generation components

ELSAG DATAMAT FINMECCANICA

Thanks for your attention

18/10/2007 ReSIST workshop, Rome 18 Oct ‘07

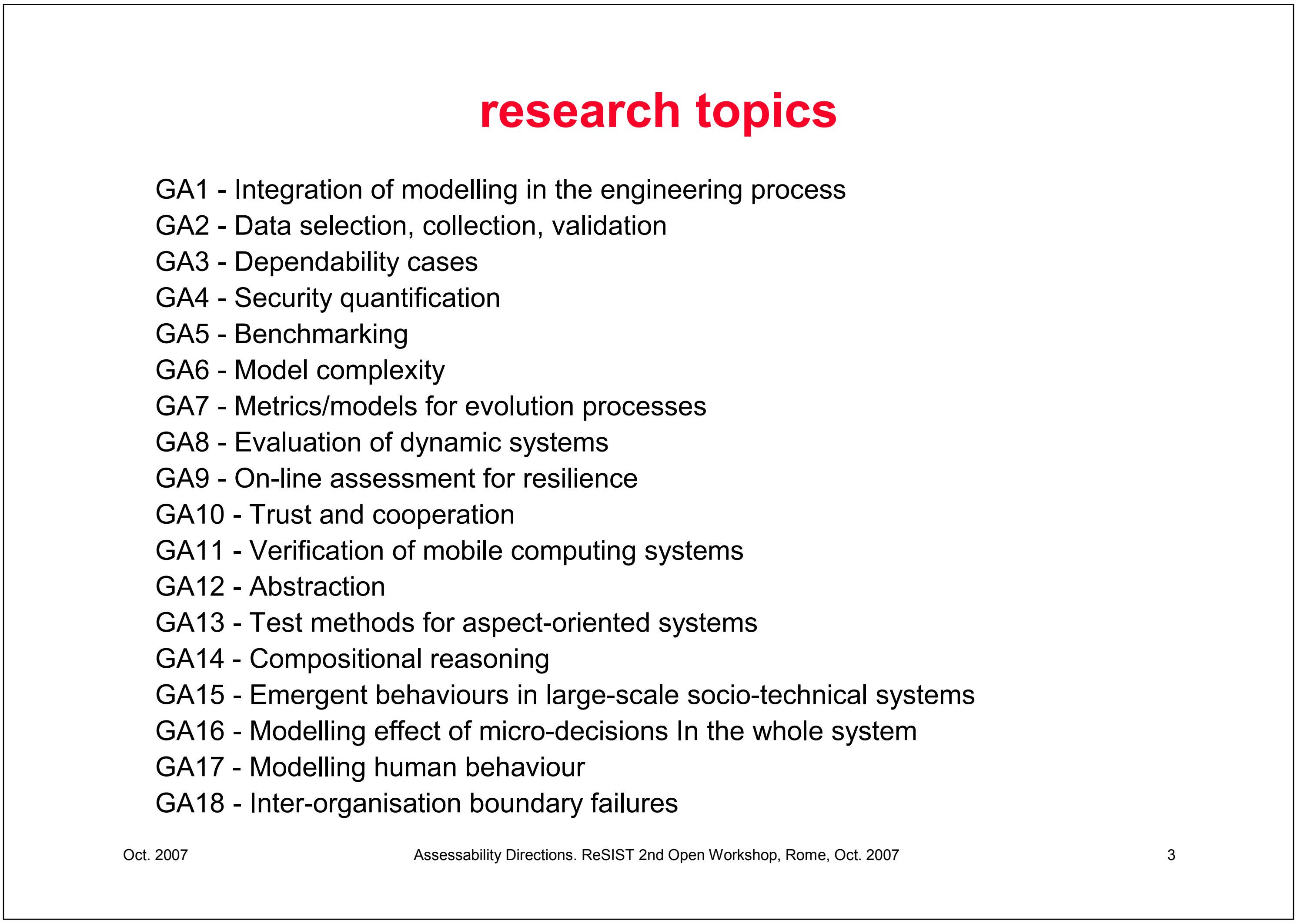
assessability

from resilience-building to resilience-scaling technologies: directions

ReSIST 2nd Open Workshop, Rome, Oct. 2007

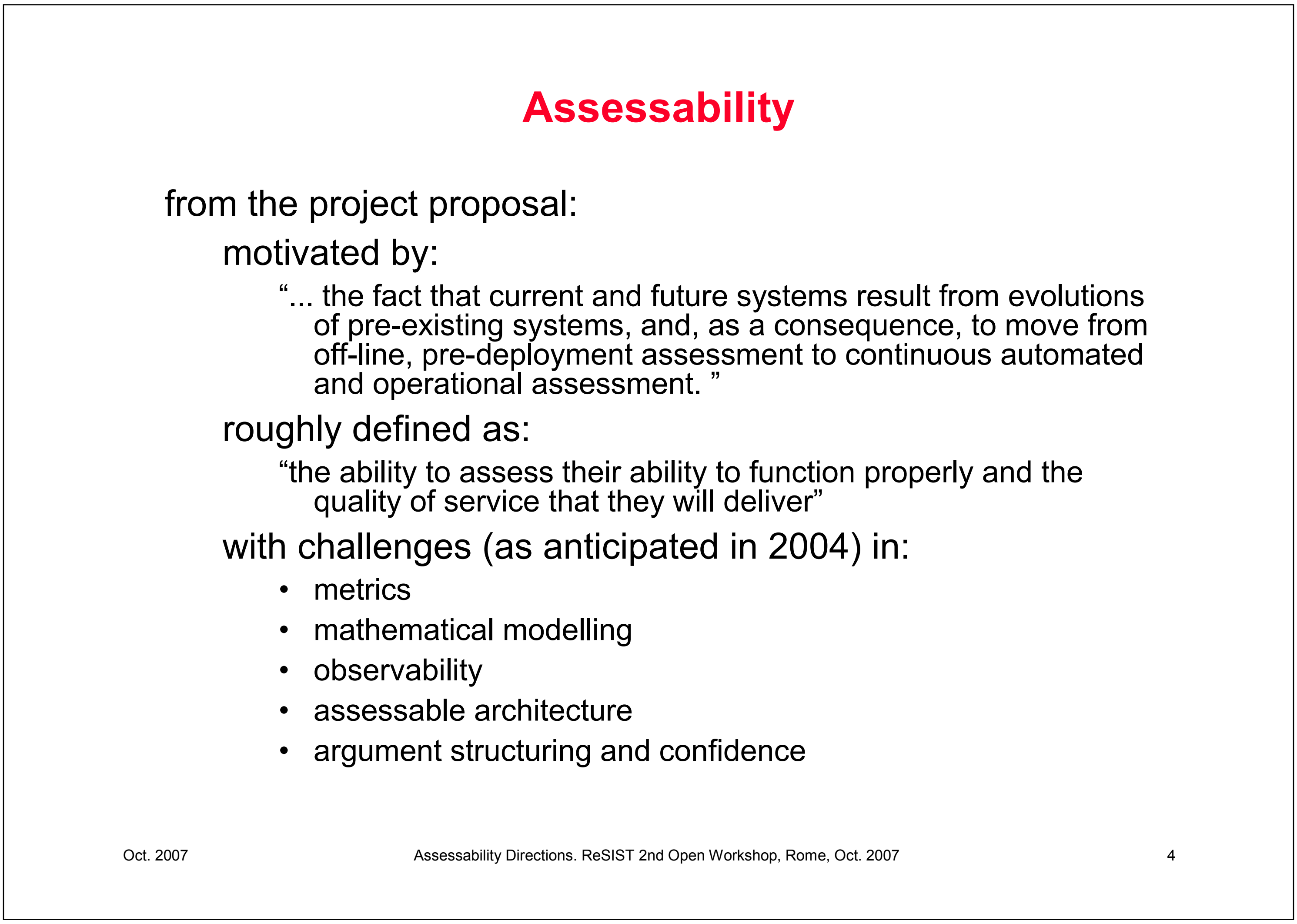
contributors

Cinzia Bernardeschi,
Peter Bokor,
Andrea Bondavalli,
Marc Dacier,
Colin O'Halloran,
Mohamed Kaâniche,
Karama Kanoun,
Marc-Olivier Killijian,
Jean-Claude Laprie,
Giuseppe Lettieri,
Bev Littlewood,
Paolo Lollini,
István Majzik,
Nick Moffat,
Alberto Pasquini,
Péter Pásztor,
Holger Pfeifer,
Peter Popov,
James Riordan,
Nicolas Rivière,
Yves Roudier,
Matthieu Roy,
Lorenzo Strigini,
Neeraj Suri,
Aad van Moorsel,
Hélène Waeselynck



research topics

GA1 - Integration of modelling in the engineering process
GA2 - Data selection, collection, validation
GA3 - Dependability cases
GA4 - Security quantification
GA5 - Benchmarking
GA6 - Model complexity
GA7 - Metrics/models for evolution processes
GA8 - Evaluation of dynamic systems
GA9 - On-line assessment for resilience
GA10 - Trust and cooperation
GA11 - Verification of mobile computing systems
GA12 - Abstraction
GA13 - Test methods for aspect-oriented systems
GA14 - Compositional reasoning
GA15 - Emergent behaviours in large-scale socio-technical systems
GA16 - Modelling effect of micro-decisions In the whole system
GA17 - Modelling human behaviour
GA18 - Inter-organisation boundary failures



Assessability

from the project proposal:

motivated by:

"... the fact that current and future systems result from evolutions of pre-existing systems, and, as a consequence, to move from off-line, pre-deployment assessment to continuous automated and operational assessment. "

roughly defined as:

"the ability to assess their ability to function properly and the quality of service that they will deliver"

with challenges (as anticipated in 2004) in:

- metrics
- mathematical modelling
- observability
- assessable architecture
- argument structuring and confidence

system perspective

characteristics:

- evolvable
- pervasive, mobile
- heterogeneity in scale: small devices, large servers
- everything inter-networked, dynamic coalitions
- new programming approaches

implication for assessability:

- evolving requirements
- large models
- stiff models
- on-line assessment
- self-similarity, chaos

system perspective

two main returning issues in assessability of evolving systems

1. how to assess the impact of **human** behaviour (user, operator)?
   - need for models of human behaviour
     - ✓ malicious behaviour
     - ✓ accidental failures
     - ✓ [illegible]
   - how to involve humans in test beds, e.g. in mobile systems (‘living labs’)
2. how to deal with ever increasing **complexity**
   - on-line solution of formal models, improve composition, abstraction
   - how to measure complex systems, identify emerging behaviour, characterise its complexity, etc.
   - conventional modelling approaches break down in chaotic, self-similar systems

methods & techniques perspective

how do our known methods and techniques (model checking, monte-carlo simulation, Petri net modelling, ...) hold up?

in addition to the complexity challenge, two main issues stand out

1. how to include **stakeholder** perspective (user, business, regulator)?
   - need for higher-level modelling paradigms for various perspectives
   - need for integration of new modelling approaches: game-theoretic, risk analysis, ...
   - how to deal with the sensitivities around benchmarking
2. how to measure and model **security**
   - development of a security metric
   - models of threats, impact, analysis of risk

engineering discipline perspective

why is assessment not an integral part of computer system design, deployment and operation?

we urge for new contributions in:

- resilience **benchmarking**
- **dependability case** construction and argumentation
- inclusion of assessability techniques in **model-driven design** and domain languages
- **demonstration vehicles**

challenge increases: evolving systems implies we must move from design to deployment and operation

assessability conclusion

extensive analysis of research challenges, greatly refining and completing the anticipated challenges

identified the following foci:

- system: *human behaviour* and *complexity*
- methods & techniques: *stakeholder perspective* and *security models & metrics*
- engineering discipline: overarching driver

contributors

Cinzia Bernardeschi,
Peter Bokor,
Andrea Bondavalli,
Marc Dacier,
Colin O'Halloran,
Mohamed Kaâniche,
Karama Kanoun,
Marc-Olivier Killijian,
Jean-Claude Laprie,
Giuseppe Lettieri,
Bev Littlewood,
Paolo Lollini,
István Majzik,
Nick Moffat,
Alberto Pasquini,
Péter Pásztor,
Holger Pfeifer,
Peter Popov,
James Riordan,
Nicolas Rivière,
Yves Roudier,
Matthieu Roy,
Lorenzo Strigini,
Neeraj Suri,
Aad van Moorsel,
Hélène Waeselynck

ReSIST Second Open Workshop Resilience in computing systems and infrastructures: a research agenda

Roma, Italy, 18 October 2007

Assessability

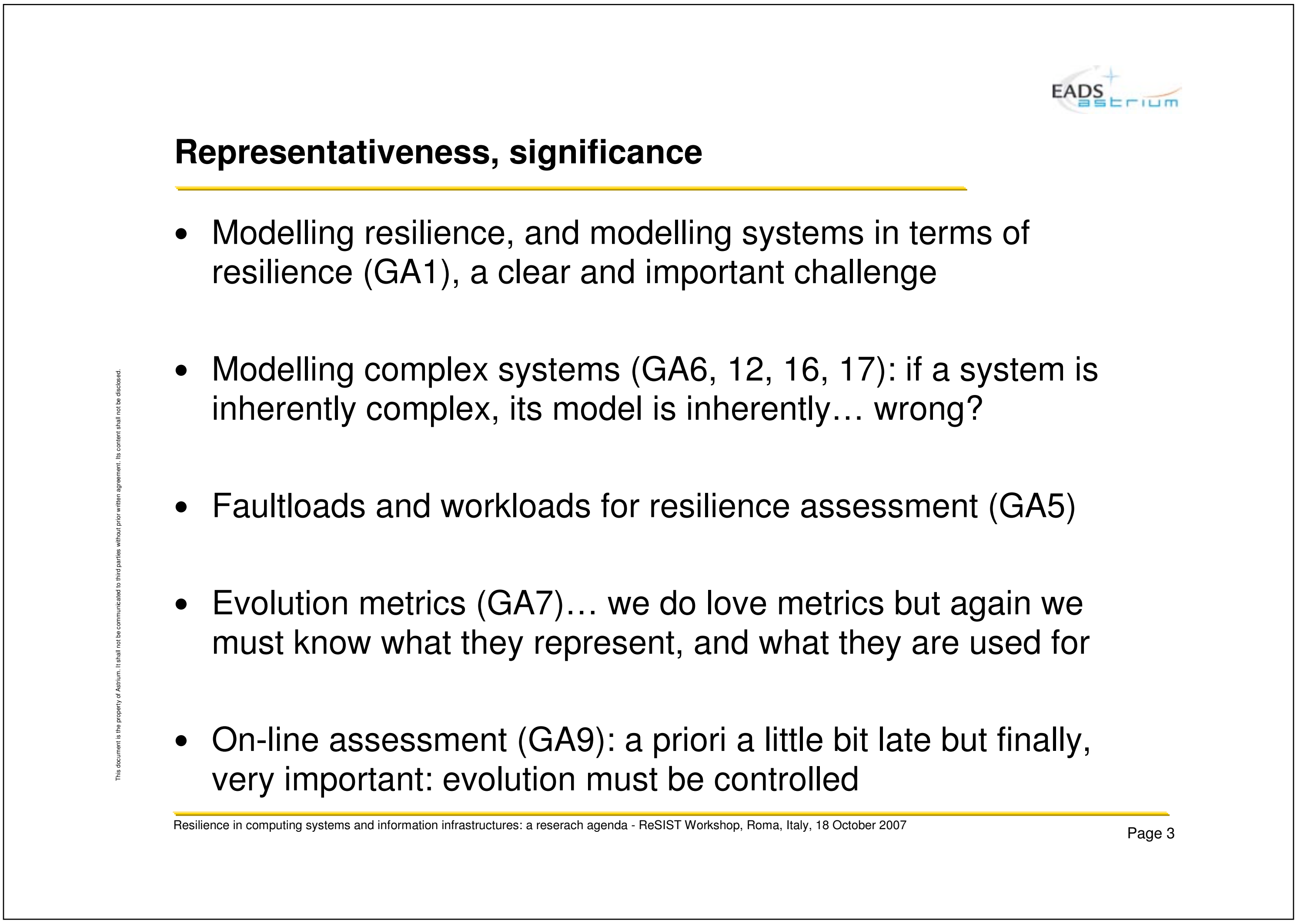
Industry's view

Jean-Paul Blanquart
Astrium Satellites, Toulouse, France

EADS astrium

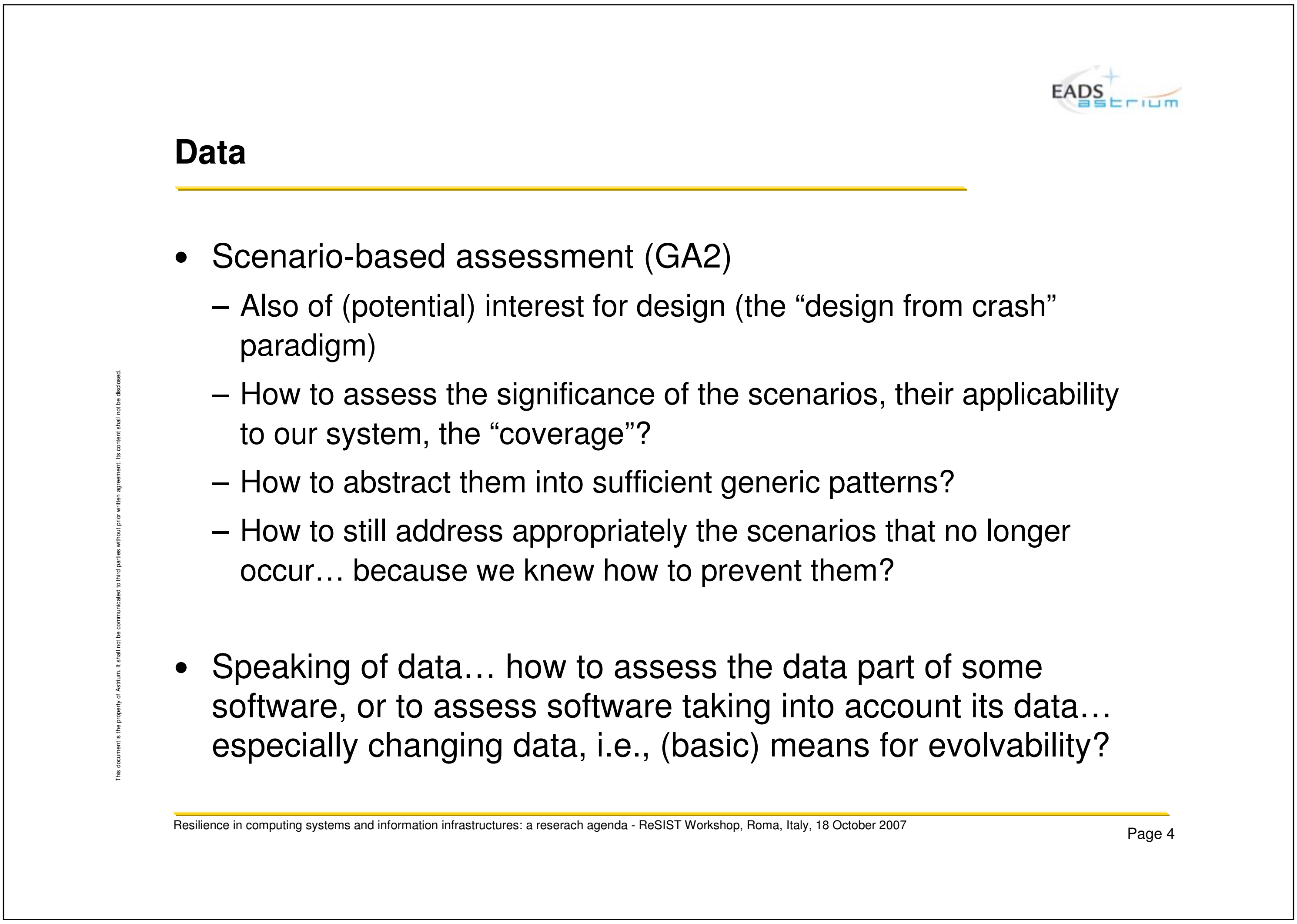
Assessability, gaps and resilience

- An assessability gap is simply a gap:
  - A technology that would be accessible but couldn't be assessed is, in practice, not accessible from industry's viewpoint
- What does resilience assessment means?
  - Resilience has to do with
    - Changes, not necessarily foreseen, clearly identified in advance
    - Robustness
  - Assessment (industry) has to do with
    - Evidence of compliance with respect to some specification, requirements
    - But.. Difference kinds of evidence (technical, informed expert judgement, formally or contractually agreed, …)



Representativeness, significance

- Modelling resilience, and modelling systems in terms of resilience (GA1), a clear and important challenge
- Modelling complex systems (GA6, 12, 16, 17): if a system is inherently complex, its model is inherently… wrong?
- Faultloads and workloads for resilience assessment (GA5)
- Evolution metrics (GA7)… we do love metrics but again we must know what they represent, and what they are used for
- On-line assessment (GA9): a priori a little bit late but finally, very important: evolution must be controlled



Data

- Scenario-based assessment (GA2)
  - Also of (potential) interest for design (the “design from crash” paradigm)
  - How to assess the significance of the scenarios, their applicability to our system, the “coverage”?
  - How to abstract them into sufficient generic patterns?
  - How to still address appropriately the scenarios that no longer occur… because we knew how to prevent them?
- Speaking of data… how to assess the data part of some software, or to assess software taking into account its data… especially changing data, i.e., (basic) means for evolvability?

Quantitative assessment, dependability case (GA3, 4)

- Quantitative assessment… easier acceptance for security than for software reliability?
- Isn’t there some “Heisenberg effect” when trying to measure the characteristics of security attacks?
- Mixing quantitative and qualitative or deterministic claims and arguments into a consistent convincing dependability case
- Dependability case: a framework to formalise and clarify the notion of software criticality?
- Not only final assessment. Important as support to design

Resilience overestimation

- Observed dependability in a stable situation is certainly a bad estimator of resilience though in absence of a good one, the confusion is quite easy.
- Co-evolution of threats and means (GA7)… a nice idea. Note that, as in biology, we shouldn’t imagine necessarily some progress. Many systems evolve towards decreased dependability, badly controlled, because of the difficulty to evaluate the available dependability margins
- Responsibility failures (GA18): not knowing who is in charge is not the only issue. In many cases people don’t even perceive the need for change in roles and responsibilities, especially in case of overestimated resilience

Resilience Scaling Technologies - Usability

Philippe Palanque

LIIHS-IRIT
Université Paul Sabatier
Toulouse – France
http://liihs.irit.fr/palanque
palanque@irit.fr

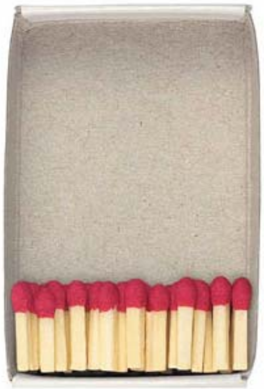
ReSIST 2nd Open Workshop –
Roma – 18 oct 2007

Contributors

- Sandra Basnyat[3], Giorgio Faconti[6], Jérémie Guiochet[4], Michael Harrison[5], Matthieu Roy[4], Lorenzo Strigini[2], Daniel Toth[1], Marco Winckler[3]
- Review panel
- [1]University of Budapest, [2]City University, [3]IRIT, [4]LAAS-CNRS, [5]University of Newcastle, [6]University of Pisa
- Propose a usability-centered reading of D13 (from resilience building to resilience scaling technologies: directions)

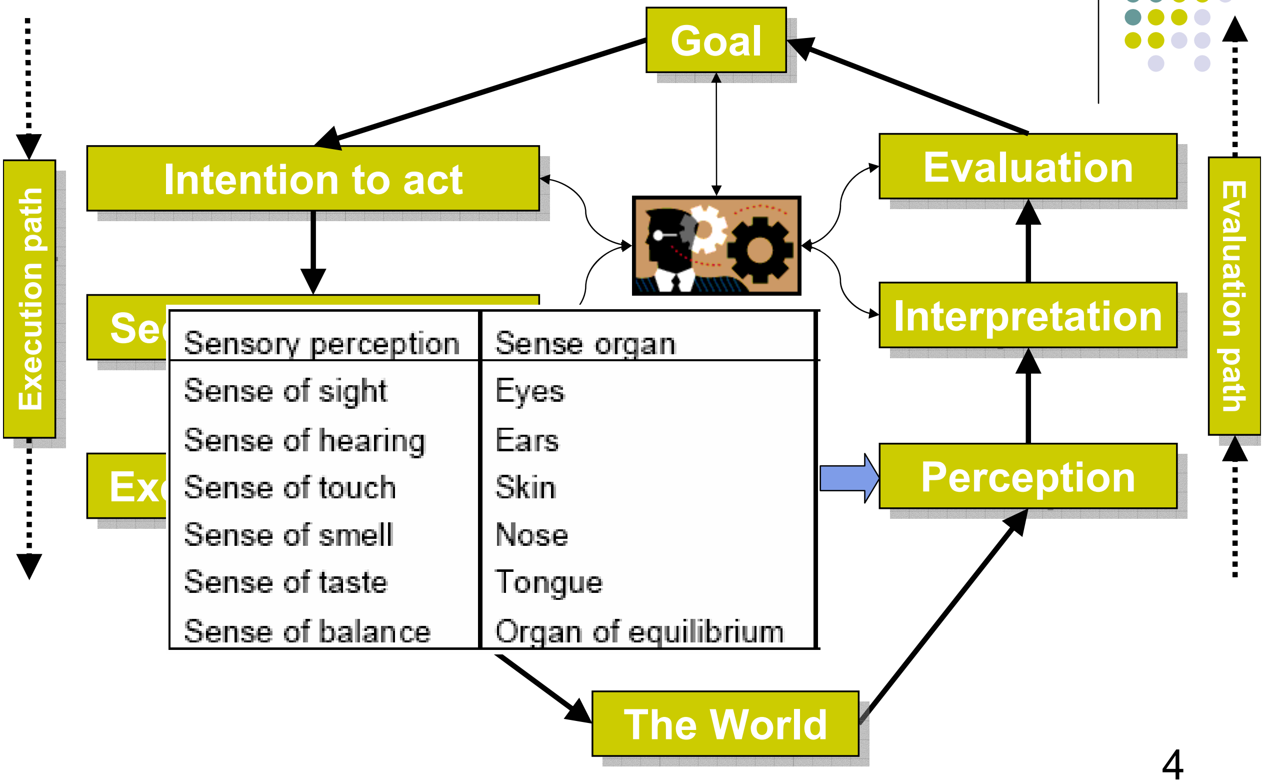
Definition

Neilsen’s definition [Nie
ability is a quality attribut
rfaces are to use”
word "usability" also refe … se-of-
during the design proces
) **learnability** (how easy is i … ks the
rst time they encounter the
) (… learned the design, how quickly can
ne
) r … turn to the design after
not … re-establish proficienc
- d) (… users make, how sever
err … recover from the errors
- e) s … it to use the design?)



- Other or … er to **utility**, **efficie**
satisfac … ed set of users can
specifie … lar environment.

Action Theory – Norman 86



Sensory perception	Sense organ
Sense of sight	Eyes
Sense of hearing	Ears
Sense of touch	Skin
Sense of smell	Nose
Sense of taste	Tongue
Sense of balance	Organ of equilibrium

4

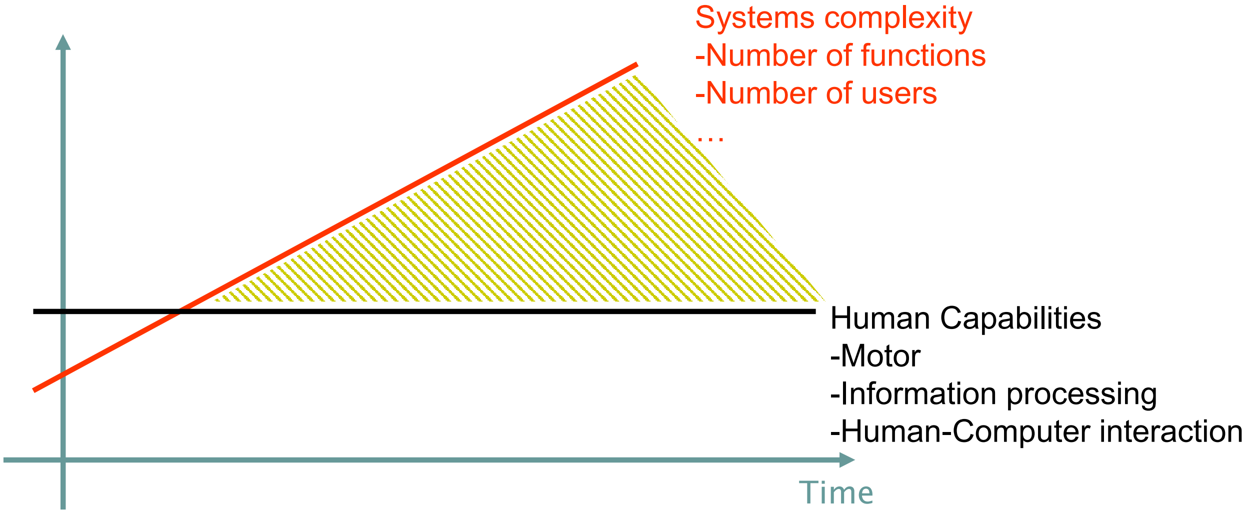
Resilience Scaling Technologies

- **Diversity**
- **Assessability**
- **Evolvability**

- **Usability**: At the core of a research domain
  - ACM SIGCHI largest SIG (Special Interest Group) at ACM
  - 8.87% of downloaded papers in the ACM DL (first of all SIGs)
  - UPA (Usability Professional Association)
  - World Usability Day every year

5

Usability - Diversity



Diversity of input/output/interaction to increase communication bandwidth (multimodal interfaces, interaction design, …)

6

Usability - Diversity

- Diversity on Input/output devices and interaction techniques
- Diversity of users
  - Web applications (e-gov, …)
  - Gaming (want to know more about that?)
  - Command and control systems (responsibility, …)
  - Peace keeping operations (OTW) (language, training, …)
- Diversity of contexts of use

7

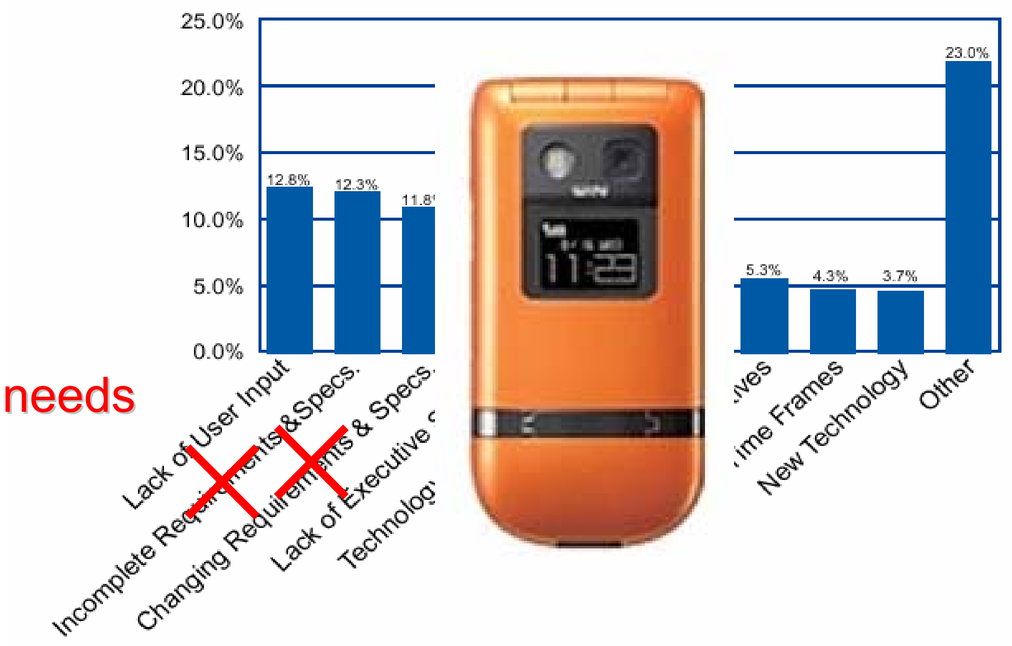
Usability - Assessability

- COST action 294 MAUSE on MAturing USability Evaluation Methods
  - Methods
  - Tools
  - Formative - Summative evaluation
- Usability laboratories
- Usability heuristics
- What do to with the measures … Prodi-Berlusconi debate "you use statistics like a drunk man on the street uses a pavement lamp; not for seeing better but for standing still"

8

Designing for Evolvability

Why Software Projects Fail (source Boehm 2006) - Average overrun: 89.9% on cost, 121% on schedule, with 61% of content



352 companies - 8,000 software projects. Source: *The Standish Group, 1995*

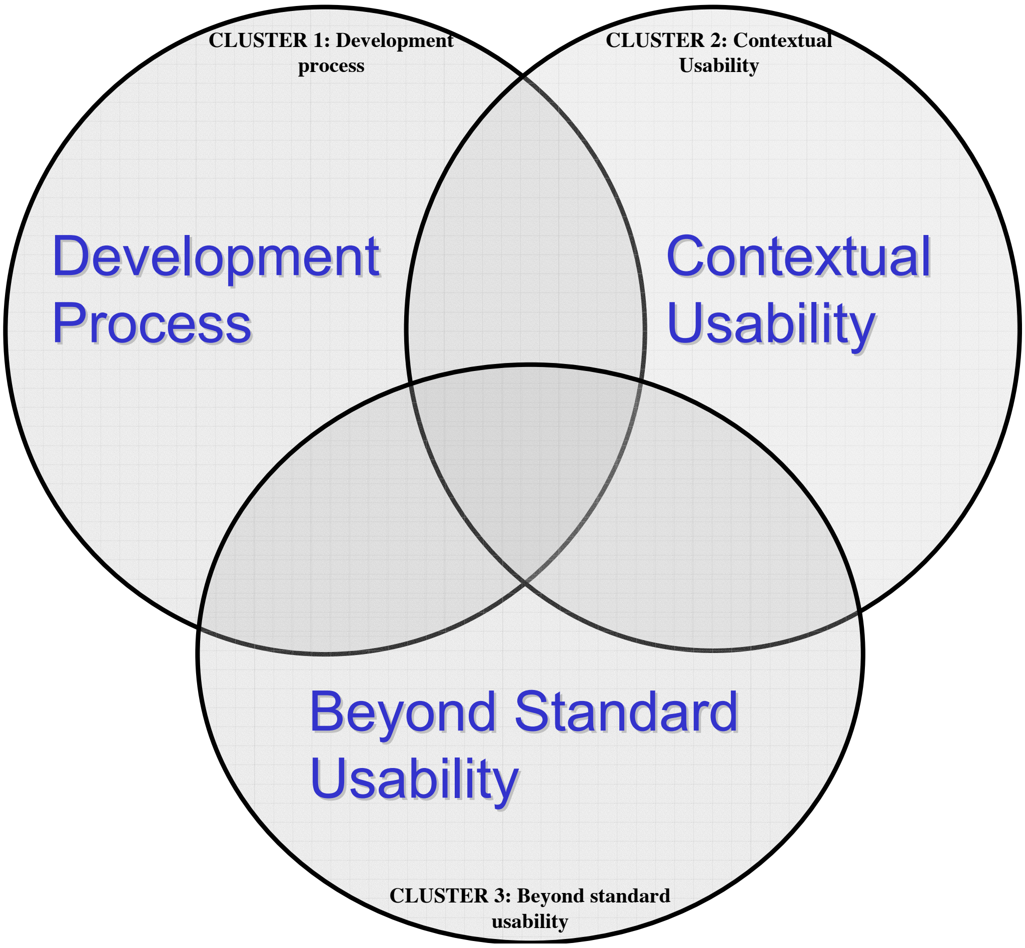
Usability – Evolvability

- Users evolve too
  - Practice
  - Training
  - Aging
- Evolution by means of barriers
  - Barrier = systems that prevent or stop ar
  - Ammunition loading problem in tanks
    - Recurrent problem
    - No recorded problem on operation
    - Solution to re-design and deploy new load
    - Usage study on operation (3 days)
- Same philosophy in software (patches) - what about the resilience of such systems?
- Problem with web applications

Overview of the Talk

- Introduction to Usability principles
  - Definition
  - The specificity of Usability with respect to the other resilience scaling technologies
- Categorisation of the identified research gaps
- Detailed presentation of the research gaps descriptions
- Conclusions

11



CLUSTER 1: Development process

CLUSTER 2: Contextual Usability

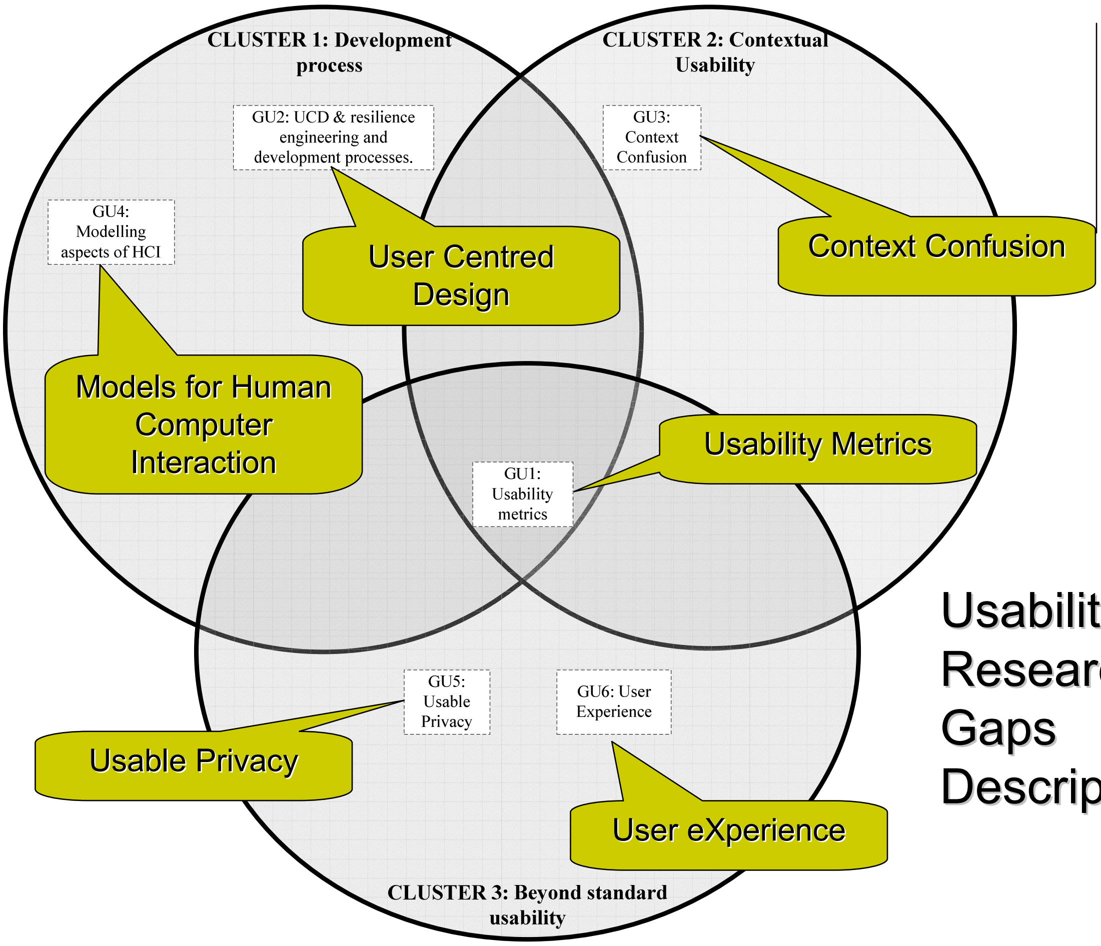
Development Process

Contextual Usability

Beyond Standard Usability

CLUSTER 3: Beyond standard usability

12



CLUSTER 1: Development process

GU2: UCD & resilience engineering and development processes.

GU4: Modelling aspects of HCI

CLUSTER 2: Contextual Usability

GU3: Context Confusion

GU1: Usability metrics

GU5: Usable Privacy

GU6: User Experience

CLUSTER 3: Beyond standard usability

User Centred Design

Context Confusion

Models for Human Computer Interaction

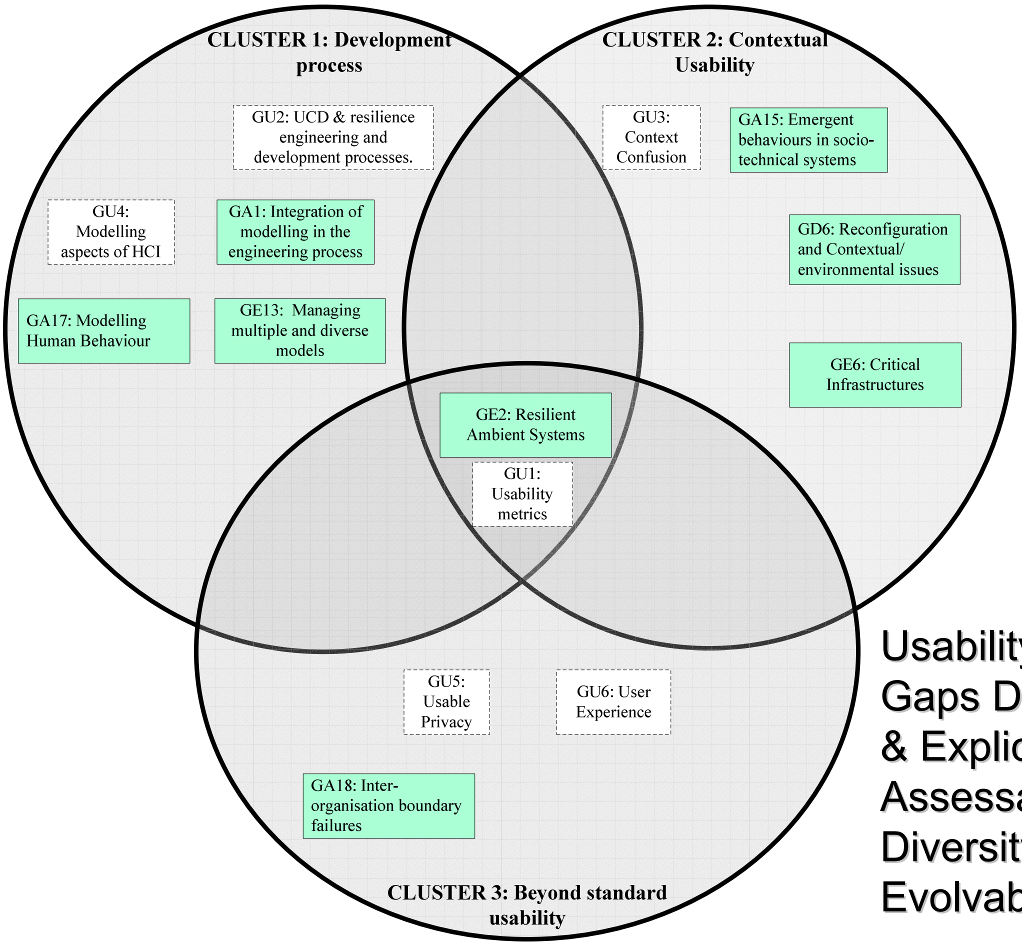
Usability Metrics

Usable Privacy

User eXperience

Usability Research Gaps Descriptions

13



CLUSTER 1: Development process

GU2: UCD & resilience engineering and development processes.

GU4: Modelling aspects of HCI

GA1: Integration of modelling in the engineering process

GA17: Modelling Human Behaviour

GE13: Managing multiple and diverse models

CLUSTER 2: Contextual Usability

GU3: Context Confusion

GA15: Emergent behaviours in socio-technical systems

GD6: Reconfiguration and Contextual/ environmental issues

GE6: Critical Infrastructures

GE2: Resilient Ambient Systems

GU1: Usability metrics

GU5: Usable Privacy

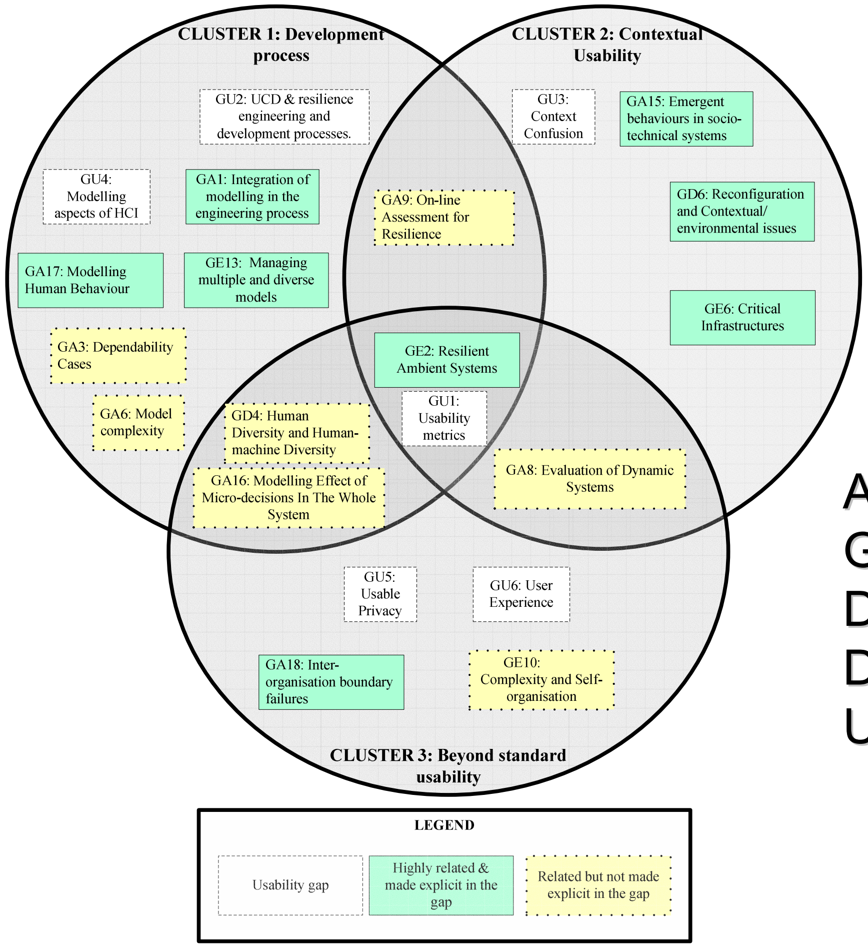
GU6: User Experience

GA18: Inter-organisation boundary failures

CLUSTER 3: Beyond standard usability

Usability Research Gaps Descriptions & Explicit Gaps – Assessability – Diversity - Evolvability

14



CLUSTER 1: Development process

GU2: UCD & resilience engineering and development processes.

GU4: Modelling aspects of HCI

GA1: Integration of modelling in the engineering process

GA17: Modelling Human Behaviour

GE13: Managing multiple and diverse models

GA3: Dependability Cases

GA6: Model complexity

CLUSTER 2: Contextual Usability

GU3: Context Confusion

GA15: Emergent behaviours in socio-technical systems

GA9: On-line Assessment for Resilience

GD6: Reconfiguration and Contextual/ environmental issues

GE6: Critical Infrastructures

GE2: Resilient Ambient Systems

GU1: Usability metrics

GD4: Human Diversity and Human-machine Diversity

GA16: Modelling Effect of Micro-decisions In The Whole System

GA8: Evaluation of Dynamic Systems

GU5: Usable Privacy

GU6: User Experience

GA18: Inter-organisation boundary failures

GE10: Complexity and Self-organisation

CLUSTER 3: Beyond standard usability

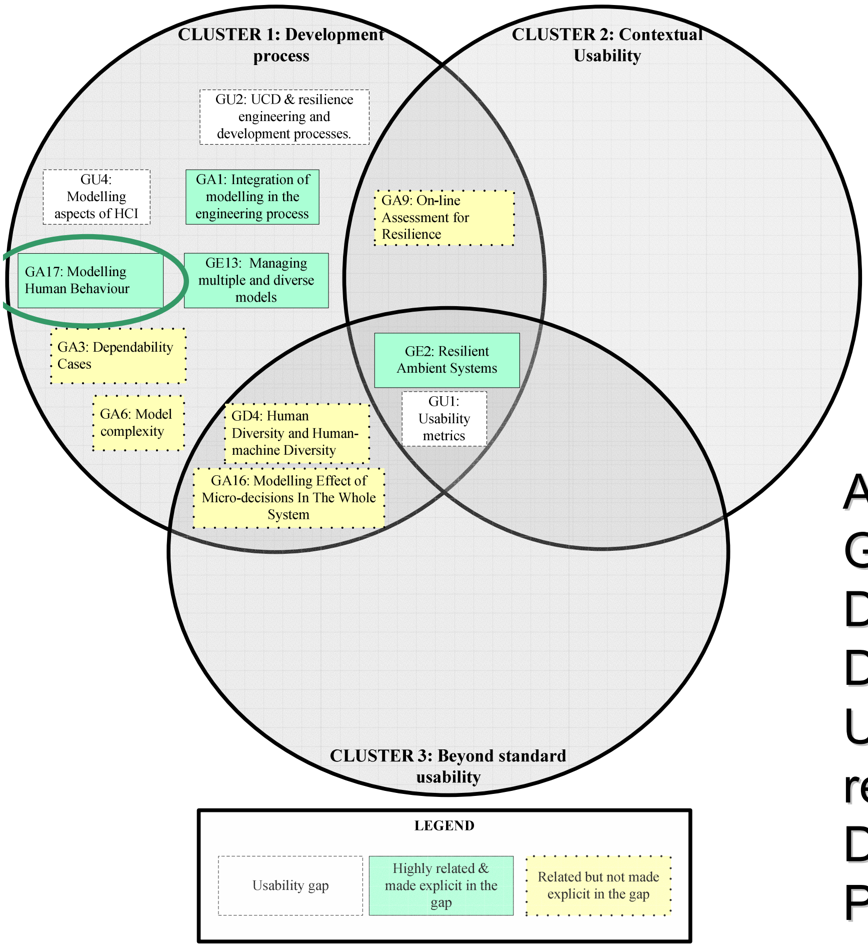
LEGEND

Usability gap

Highly related & made explicit in the gap

Related but not made explicit in the gap

All the Research Gaps Descriptions Dealing with Usability



CLUSTER 1: Development process

GU2: UCD & resilience engineering and development processes.

GU4: Modelling aspects of HCI

GA1: Integration of modelling in the engineering process

GA17: Modelling Human Behaviour

GE13: Managing multiple and diverse models

GA3: Dependability Cases

GA6: Model complexity

CLUSTER 2: Contextual Usability

GA9: On-line Assessment for Resilience

GE2: Resilient Ambient Systems

GU1: Usability metrics

GD4: Human Diversity and Human-machine Diversity

GA16: Modelling Effect of Micro-decisions In The Whole System

CLUSTER 3: Beyond standard usability

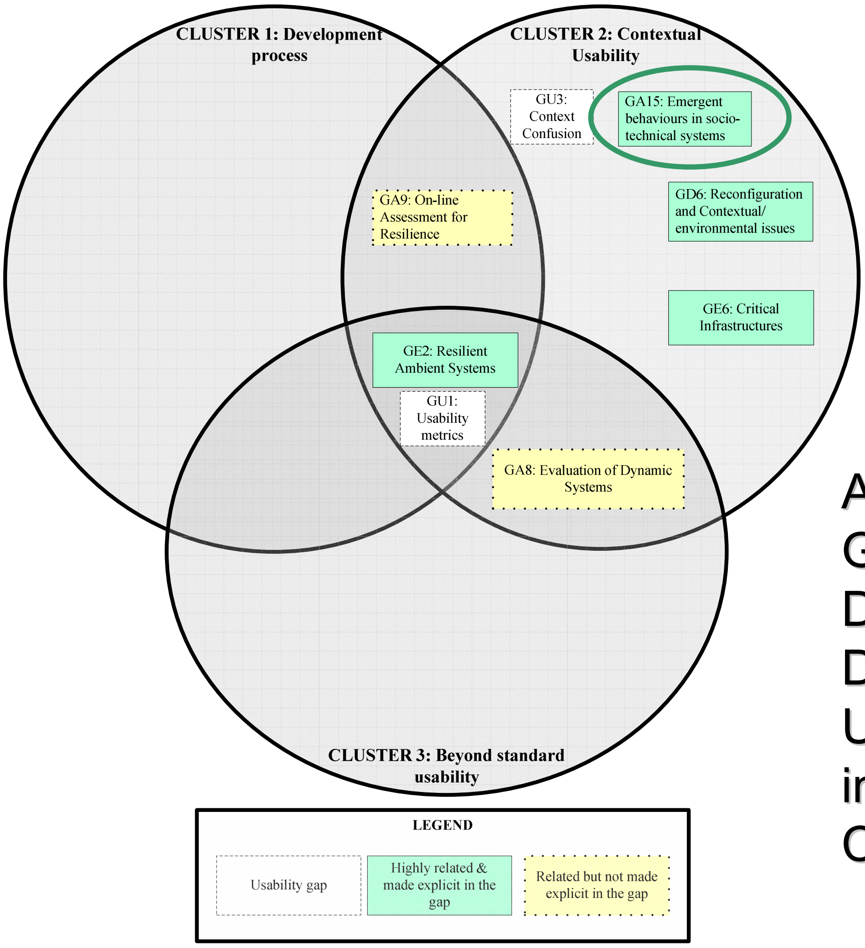
LEGEND

Usability gap

Highly related & made explicit in the gap

Related but not made explicit in the gap

All the Research Gaps Descriptions Dealing with Usability and related to Development Processes



CLUSTER 1: Development process

CLUSTER 2: Contextual Usability

CLUSTER 3: Beyond standard usability

GU3: Context Confusion

GA15: Emergent behaviours in socio-technical systems

GA9: On-line Assessment for Resilience

GD6: Reconfiguration and Contextual/ environmental issues

GE6: Critical Infrastructures

GE2: Resilient Ambient Systems

GU1: Usability metrics

GA8: Evaluation of Dynamic Systems

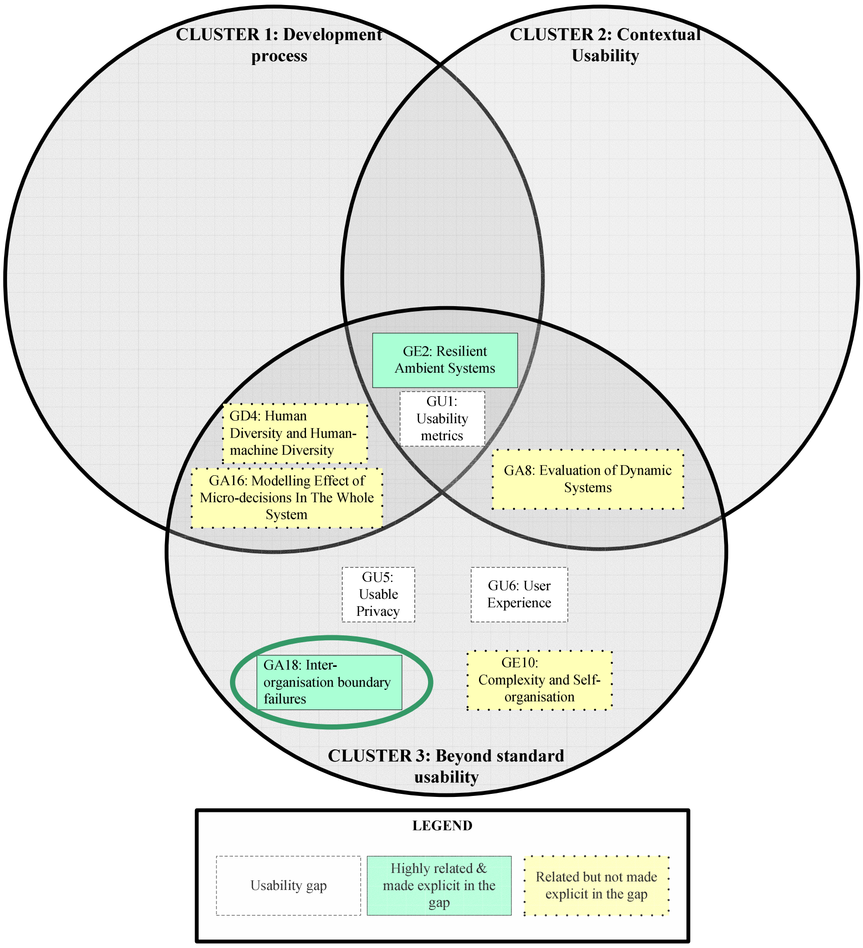
LEGEND

Usability gap

Highly related & made explicit in the gap

Related but not made explicit in the gap

All the Research Gaps Descriptions Dealing with Usability influenced by Context



CLUSTER 1: Development process

CLUSTER 2: Contextual Usability

CLUSTER 3: Beyond standard usability

GE2: Resilient Ambient Systems

GU1: Usability metrics

GD4: Human Diversity and Human-machine Diversity

GA16: Modelling Effect of Micro-decisions In The Whole System

GA8: Evaluation of Dynamic Systems

GU5: Usable Privacy

GU6: User Experience

GA18: Inter-organisation boundary failures

GE10: Complexity and Self-organisation

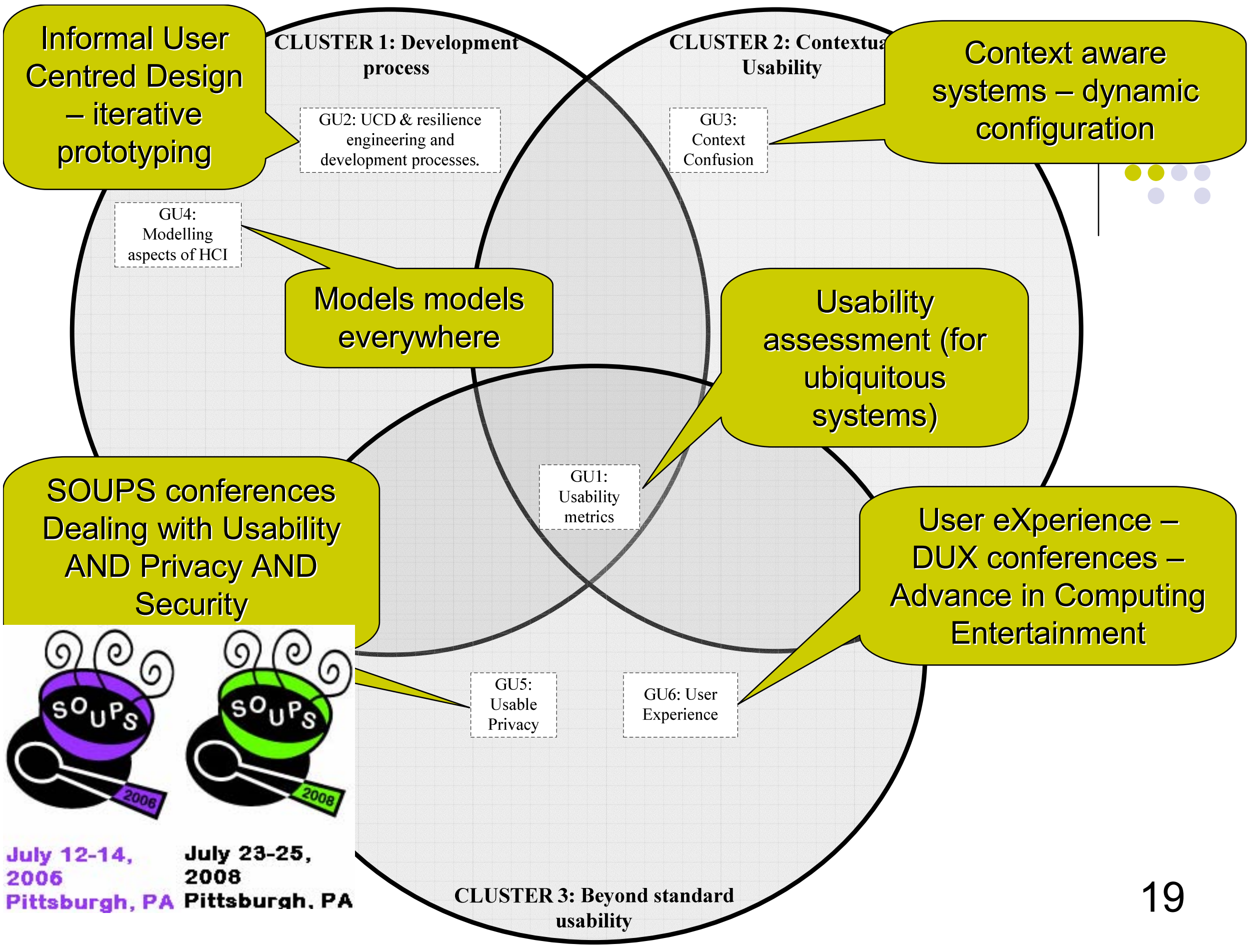
LEGEND

Usability gap

Highly related & made explicit in the gap

Related but not made explicit in the gap

All the Research Gaps Descriptions Dealing with Usability and rasing new issues (not addressed by standard Usability)


CLUSTER 1: Development process

CLUSTER 2: Contextual Usability

CLUSTER 3: Beyond standard usability

GU1: Usability metrics

GU2: UCD & resilience engineering and development processes.

GU3: Context Confusion

GU4: Modelling aspects of HCI

GU5: Usable Privacy

GU6: User Experience

Informal User Centred Design – iterative prototyping

Context aware systems – dynamic configuration

Models models everywhere

Usability assessment (for ubiquitous systems)

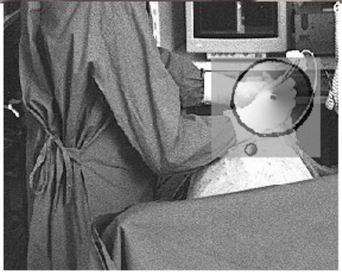
SOUPS conferences Dealing with Usability AND Privacy AND Security

User eXperience – DUX conferences – Advance in Computing Entertainment

July 12-14, 2006
Pittsburgh, PA

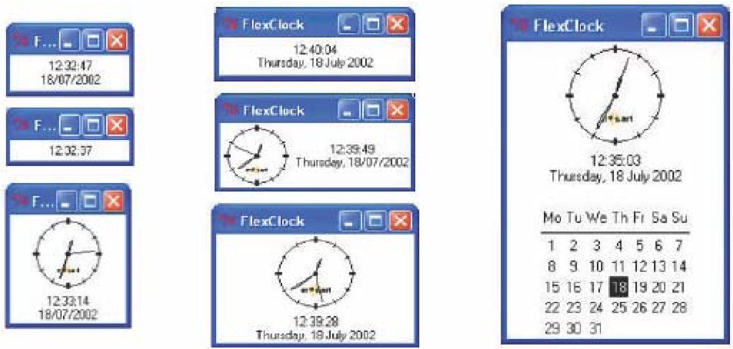
July 23-25, 2008
Pittsburgh, PA

0) Context



1) Contextual Usability

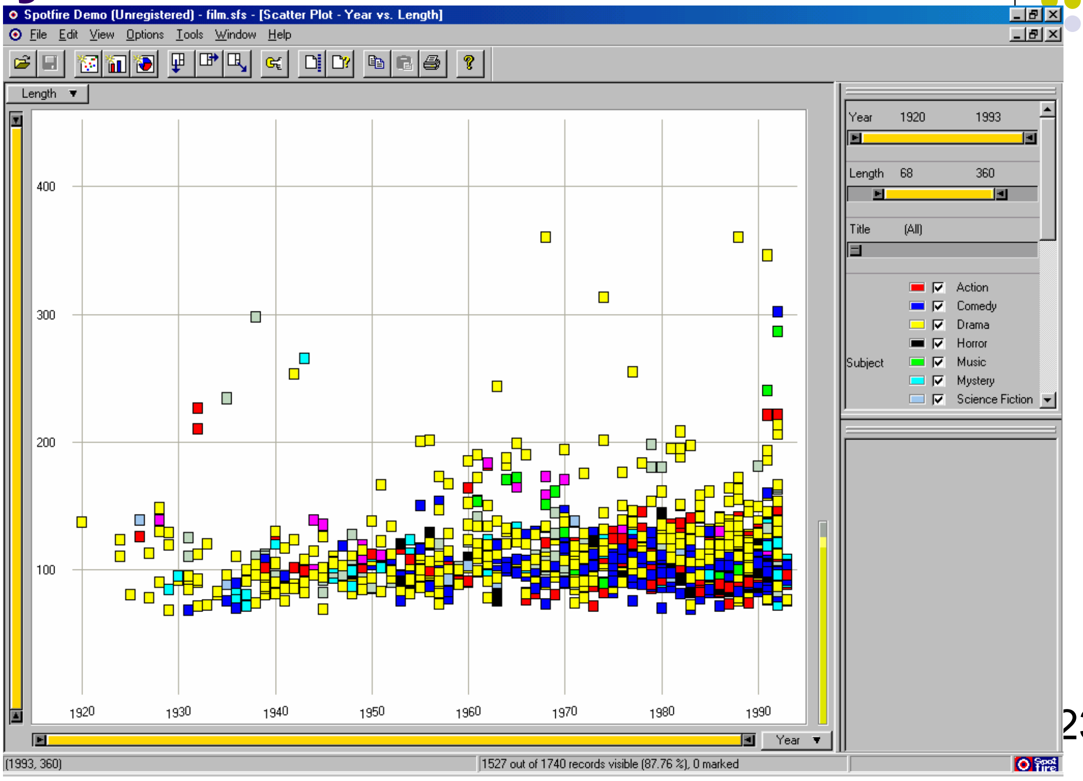
- Plasticity of user interfaces
  - Diversity of contexts
  - Dynamic evolvability of the presentation
  - Assessability of the usability of context aware systems (Usability Metrics GU1)
    - Of each presentation
    - Of the evolvability (context confusion GU3)
- Roles migration - function allocation – authority sharing
  - Modes
  - Keeping the user in t
- User Errors (context
  - Reducing the likeliho
  - Reducing the impact
  - Increasing the recove



2) Usability Metrics - Assessment

- UEMs conducted by experts
  - Usability Inspection Methods, Guideline Reviews, …
  - Any type of interactive systems
- UEMs involving the user (User Centred Design GU2)
  - Empirical evaluation, observations, …
  - Any type of interactive systems (from low-fi prototypes to deployed applications)
- Computer supported UEMs
  - Automatic testing based on guidelines, …
  - Task or system models-based evaluations (modelling aspects of HCI GU4), metrics-based evaluation, …
  - Applications with standardized interaction techniques (Web, WIMP)

3) Development Process - Dynamic Queries (Ahlberg et al. 94)



Spotfire Demo [Unregistered] - film.sfs - [Scatter Plot - Year vs. Length]

(1993, 360)

1527 out of 1740 records visible (87.76 %), 0 marked

23

3) Development process

- There is a need for (GU4 Modelling aspects of HCI)
  - Methods
  - Processes
  - Notations
  - Tools
- to deal with the user interface design, construction and evaluation (GU1 Usability Metrics)
- to address the new challenges raised by ubiquitous systems and to support
  - Diversity of users and contexts of use (GU3 context confusion)
  - Evolvability of needs and uses situations (GU3 context confusion)
  - Assessability of the usability (GU1 usability metrics)
- Designing for usability makes things more complicated

24

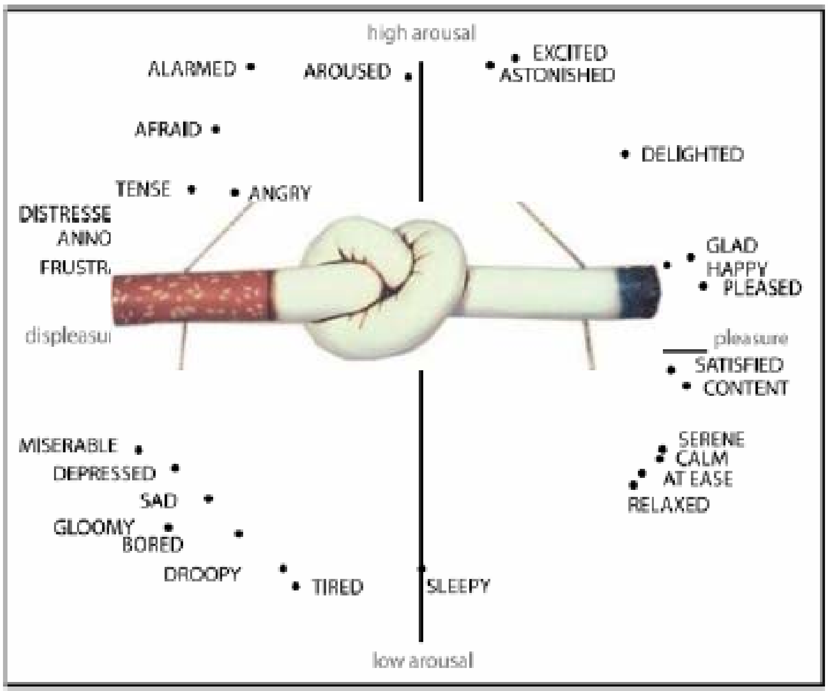
4) Beyond Standard Usability

D

Somew

it st

bef



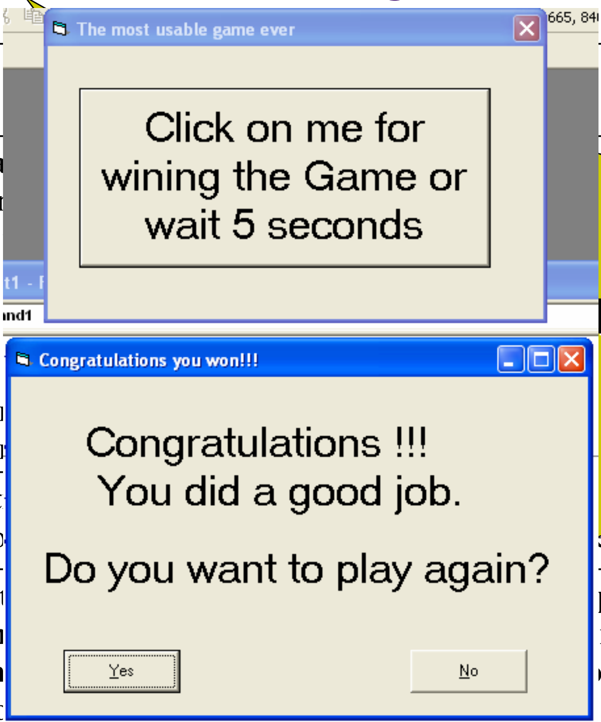
Two-dimensional affective space defined by valence and arousal: The circumplex model of affect (Russell, 1980).

e it

ends

UX versus Usability

		UX focus
Holistic	**Do-goa** **Instru** for • • **Efficie** **Perfor**	…e competent, be happy) …e balanced toward …atic and pragmatic …s chair is not …e at all but I'll buy it) …ffects trust)
Subjective	**Object** to o	…sk/interpret how the …eels)
Positive	**Avoid t** **Hygien** **Preven** errc	**positive** **rs** **on**



The most usable game ever

Click on me for wining the Game or wait 5 seconds

Congratulations you won!!!

Congratulations !!!
You did a good job.

Do you want to play again?

Conclusion

- 6 research gap descriptions have been provided and presented (central to usability)
- They define a set of important research challenges for addressing resilience of interactive sytems (paving the way for the next 18 months of ReSIST)
- They do not cover all the issues … by far
  - Management
  - Training
  - Work procedures
  - Cooperative activities
  - …

27

In Usability t i the key

- Whatever tool y l b use them differe
- You may build t machine the res
- You may inform do as they want
- You may define process but the and easiest for

Thank you for your attention

Questions ?

Top 10 Games Industry Facts

- 1. US computer and video game software sales grew six percent in 2006 to $7.4 billion – almost tripling industry software sales since 1996.
- 2. Sixty-seven percent of American heads of households play computer and video games.
- 3. The average game *player* is 33 years old and has been playing games for 12 years.
- 4. The average age of the most frequent game *buyer* is 38 years old. In 2007, 92 percent of computer game buyers and 80 percent of console game buyers were over the age of 18.
- 5. Eighty-five percent of all games sold in 2006 were rated "E" for Everyone, "T" for Teen, or "E10+" for Everyone 10+. For more information on ratings, please see www.esrb.org.
- 6. Eighty-six percent of game players under the age of 18 report that they get their parents' permission when renting or buying games, and 91 percent say their parents are present when they buy games.
- 7. Thirty-six percent of American parents say they play computer and video games. Further, 80 percent of gamer parents say they play video games with their kids. Sixty-six percent feel that playing games has brought their families closer together.
- 8. Thirty-eight percent of all game players are women. In fact, women over the age of 18 represent a significantly greater portion of the game-playing population (31%) than boys age 17 or younger (20%).
- 9. In 2007, 24 percent of Americans over the age of 50 played video games, an increase from nine percent in 1999.
- 10. Forty-nine percent of game players say they play games online one or more hours per week. In addition, 34 percent of heads of households play games on a wireless device, such as a cell phone or PDA, up from 20 percent in 2002.

Back

Comments on ‘Resilience Scaling Technologies – Usability’: presented by Philippe Palanque

Colin Corbridge

DSTL, UK

General Comments

- Good connection between the themes: evolvability, assessability, usability, and diversity. Appropriate choice of themes except:
- ‘Usability’, is it too focused on the individual (driver is ‘ubiquity/mobility’ rather than ‘pervasive’)? Is there another higher level ‘cross cutting theme’? Does the emphasis on usability detract from consideration of organisational policies, procedures, culture etc?
- No work on ‘people related requirements’ in relation to resilience. Particularly important in terms of contracting for ‘services’ rather than ‘equipment’ (If it isn’t in the requirements then it is not likely to be considered’). There are also a significant issues associated with acceptance in relation to human factors requirements which will also impact on any people related resilience issues

Cluster 1: Development Process

- Modelling of human behaviour – beyond individuals and modelling of socio-technical systems. Modelling of ICT in organisations (c.f. GE13 Managing multiple and diverse models).
- Standardisation: multiple standards to 'influence' particularly system level standards such as ISO 13407 (Human Centred Design Processes for Interactive Systems) and ISO PAS 18152 (A Specification for the Process Assessment of Human System Issues – Life Cycle Issues). Integration of resilience alongside usability will be a challenge. Continuous assessment throughout design is important – links to accessibility.
- Work to examine translation of HF task data into UML class diagrams and hence interface specifications being conducted by the Human Factors Integration Defence Technology in the UK (www.hfidtc.com)
- Other exploitation paths – avoidance of 'shelfware'. Is there a plan to achieve this? Website – design heuristics, best practice document*, distillation of knowledge generated.

Cluster 2: Contextual Usability

- Focus on 'user goals' to understand user behaviour in different contexts. Getting the 'right information at the right time' to the user. What is 'enough information'?
- Consideration of other analytical methods that are less context specific e.g. Cognitive Work Analysis. Designers can't foresee all possible system states – therefore focus on constraints which influence the operation of the system.
- Plasticity of user interfaces may pose difficulties in the military domain
- Discovery/demonstration of emergent properties by modelling potentially exciting developments.

Cluster 3: Beyond Standard Usability

- Does user preference = performance? Evidence from work on Dynamic Function Allocation suggests this may not be true.
- How are we going to measure UX? Potential for highly innovative cross-disciplinary work here on extending ‘traditional’ usability metrics, tools and techniques.
- Privacy a key issue of significant importance and therefore good to see this being addressed. User’s perception of ‘risk’ would be an interesting avenue of investigation to pursue in relation to this topic.

Diversity:
Directions for research

presented by Lorenzo Strigini

Centre for Software Reliability
City University, London, U.K.
strigini@csr.city.ac.uk

Second Open Workshop - Resilience in Computing Systems and Information Infrastructures: A Research Agenda, 18 October 2007

slide 1

Contributors

Eugenio Alberdi, Peter Ayton, Christian Cachin, Miguel Correia, Marc Dacier, Ilir Gashi, Philippe Palanque, Peter Popov, Lorenzo Strigini, Vladimir Stankovic

(City University, London; IRIT, Toulouse; IBM; LAAS-CNRS; University of Lisbon; Eurecom)

and numerous reviewers

slide 2

Outline

- redundancy, diversity for resilience of ubiquitous systems
- diversity: what we have and what we lack
- some research challenges identified in ReSIST

Laudata sii, Diversita`
 delle creature, sirena
del mondo. [...]

D'Annunzio

Praise to you,
O Diversity of creatures,
siren of the world

Laudata sii, Diversita`
delle creature, sirena
del mondo. [...]

D'Annunzio

Praise to you,
O Diversity of creatures,
siren of the world

NOT our meaning of "diversity"

(but somewhat related)

Premise: Redundancy, diversity, resilience, ..

- interest in "Resilience" stresses dependability *despite imperfect knowledge* of threats and possible failure modes
- important role for redundancy
  - avoiding system failure despite broad ranges of component failures
- redundancy is effective if the chance of redundant parts failing together is small enough: diversity
  - desired: diversity *of failures*
  - pursued via: diversity of *construction* and *exposure*
  - linking means to results is (difficult) area for research
    - + pursued in the computing area over the last 20-30 years

Redundancy, diversity, resilience: the ReSIST angle

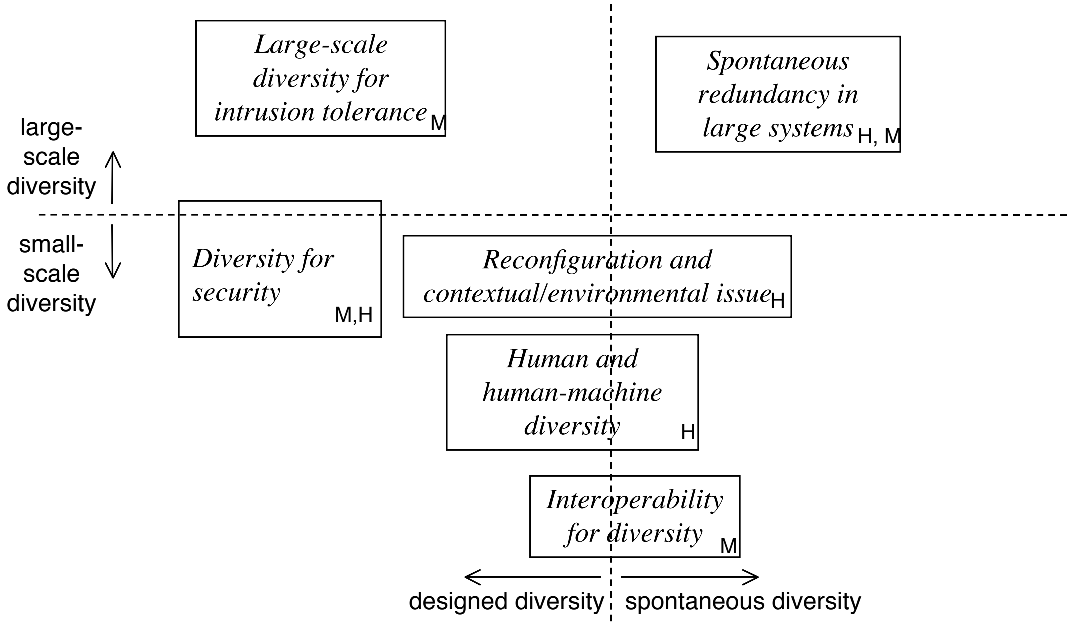
- redundancy to provide resilience... despite imperfect knowledge of threats/failures
- "ubiquitous ICT systems" - ReSIST's topic - provide many sources of *imperfection of knowledge*:
  - openness
  - change
  - enemies
  - multiple owners/managers
- ... as well as potential for redundancy
- *but also* for catastrophic common-mode or propagated failures
- thus new potential and need for *ensuring*, *exploiting, assessing* diversity

Past research about diversity ...

- has produced important results, with a focus on *embedded, small, closed, modular-redundant, safety critical control* systems
- hence necessary directions of expansion of research:

from	*towards*
small-scale diversity	large-scale diversity
dealing with unintended faults	dealing with malice as well
systems made of hardware and software	systems including people
closely controlled ("designed") diversity	more "spontaneous" diversity

The landscape of open problems



Large-scale diversity for intrusion tolerance M

Spontaneous redundancy in large systems H, M

large-scale diversity

small-scale diversity

Diversity for security M,H

Reconfiguration and contextual/environmental issue H

Human and human-machine diversity H

Interoperability for diversity M

designed diversity

spontaneous diversity

Legend:
H: involves consideration of human components
M: considers not only accidental faults, but malicious attacks

Scale of diversity

- current uses of diversity, and thus focus of past research, are "small scale"
  - e.g. safety-critical control systems with
    - + 2 channels, with 2-way diversity
    - + 2+2 channels, with 4-way diversity
    - + 4+1 channels, with 2-way diversity
- "small-scale" diversity is also present in ubiquitous systems, with new problems ...
- but what if we have potential for 10,100,..10^n-way diversity?
  the mathematics change... the experimental difficulties change...

Some challenges in small-scale diversity

- Interoperability for diversity
  - competing off-the-shelf products offer (almost) free diversity
  - but minor incompatibilities frustrate the would-be developer of diverse-redundant solutions
  - needed: extensions to selection methods and wrapping mechanisms, especially for run-time evolving configurations
- Reconfiguration and contextual/environmental issues
  - multiple/multimodal human-machine interfaces used to improve interaction
  - needed: methods for *using towards resilience:* assessing diversity aspects, planning reconfiguration for resilience

Some challenges in small-scale diversity -2

- Diversity for security
  - an attractive idea, some prototypes, e.g. server diversity, limited detailed analysis. Many options, trade-offs, unknowns
  - needed: more formal analysis of goals, effectiveness, trade-offs; more knowledge about efficacy of methods; designs dealing with collusions and multiple attacks
- Human diversity and human-machine diversity
  - integrated socio-technical systems rely on extensive redundancy between human and machine components
  - needed: extending models to account for humans' heterogeneity and changeability; inclusion of more psychological and sociological knowledge

Some challenges in large-scale diversity

- Large-scale diversity for intrusion tolerance
  - scattering techniques tolerate intrusion if intruders cannot break into too many machines at once. Need to diversify vulnerabilities among many servers
  - needed: more automatic diversification techniques, at various architectural levels; methods for evaluating and selecting
- Spontaneous redundancy in large systems
  - multi-node socio-technical networks with *potential* for redundant service delivery, connectivity, monitoring...
  - needed: methods for *discovering* redundancy, *assessing* actual failure diversity, *organising* the exploitation of spontaneous redundancy

Conclusions?

Important challenges:

- items of technical knowledge needed for deploying effective diversity in large socio-technical systems
- requiring extension of current knowledge in multiple directions

... presented here for discussion

Resilience in Computing Systems and Information Infrastructures: A Research Agenda

Diversity

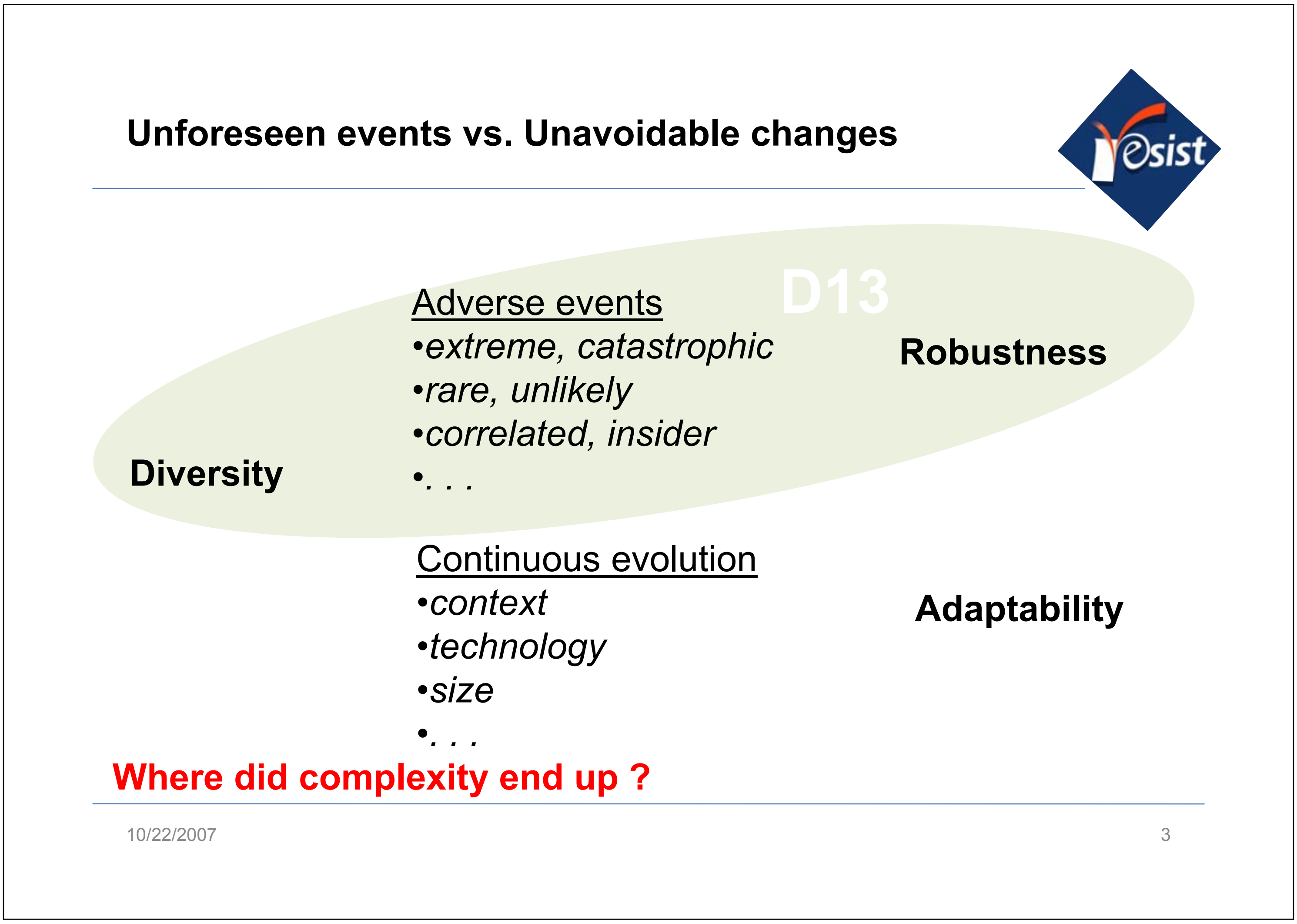
Michele Morganti

2nd ReSIST Open Workshop –18 October 2007 – Rome, Italy

About D13 Diversity at large

Deliverable D13 - From Resilience-Building to Resilience-Scaling Technologies: Directions on Diversity

- Good analysis and assessment
- Valuable conclusions and directions for future research
- Following comments/observations intended solely as contributions to reasoning/discussion
- No implicit or explicit criticism



Unforeseen events vs. Unavoidable changes

D13

Diversity

Adverse events
- *extreme, catastrophic*
- *rare, unlikely*
- *correlated, insider*
- *. . .*

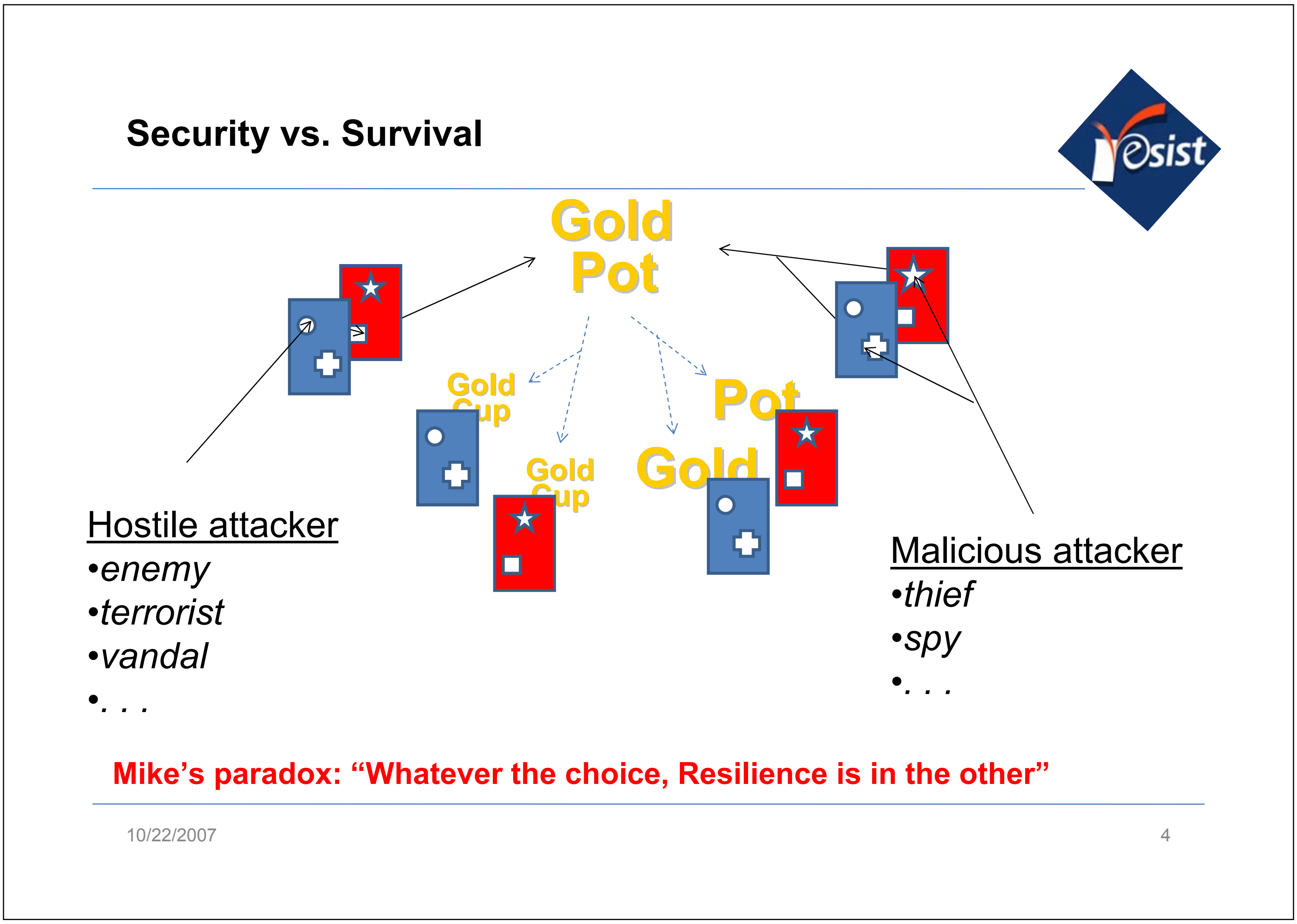
Robustness

Continuous evolution
- *context*
- *technology*
- *size*
- *. . .*

Adaptability

Where did complexity end up ?

10/22/2007 3



Security vs. Survival

Hostile attacker
- *enemy*
- *terrorist*
- *vandal*
- *. . .*

Malicious attacker
- *thief*
- *spy*
- *. . .*

Mike's paradox: "Whatever the choice, Resilience is in the other"

10/22/2007 4

Diversity vs. Redundancy

Fault-Tolerance vs. Performance, Coverage, …

Fault

Continuity
without Degradation

Fault

Survival with some Degradation

High Performance / Low Resilience + **Low Performance / High Resilience**

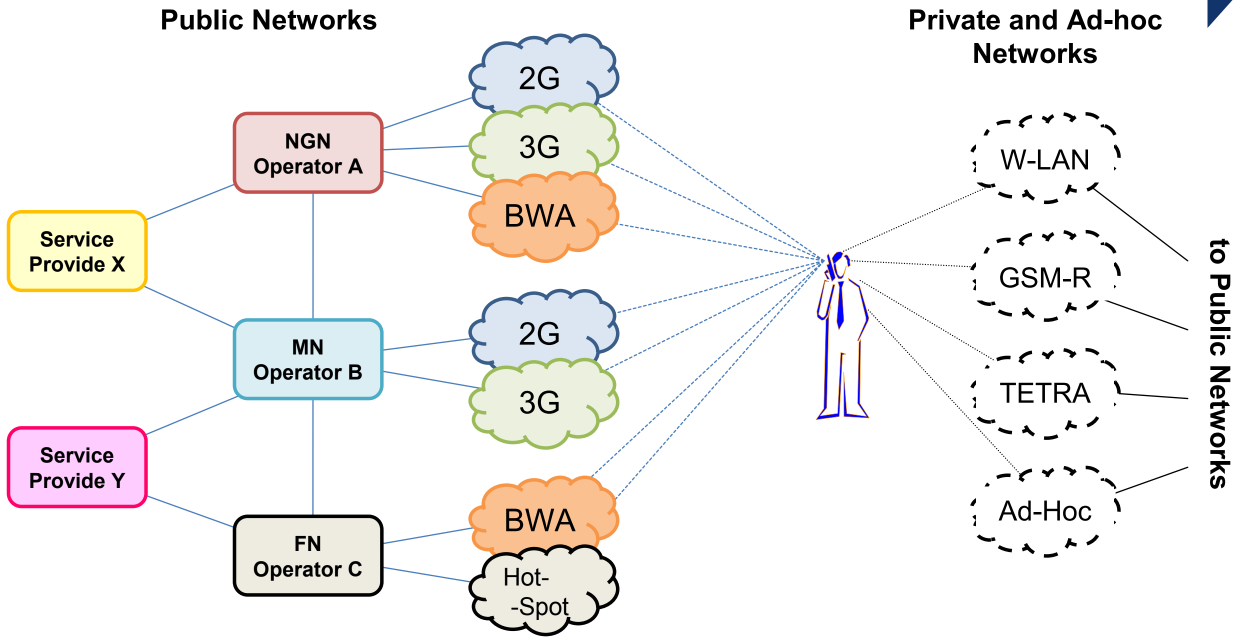
Structural vs. Infrastructural

→ **In-built vs. Outsourced**

→ **Systems vs. Services**

→ **Redundancy vs. Multiplicity**

In-built systems vs. Outsourced services



Same basic functions but totally different characteristics

Space vs. Time related Diversity

D13

Space related
- *replication*
- *segmentation*
- *. . .*

Interoperability
(horizontal & vertical)

Diversity

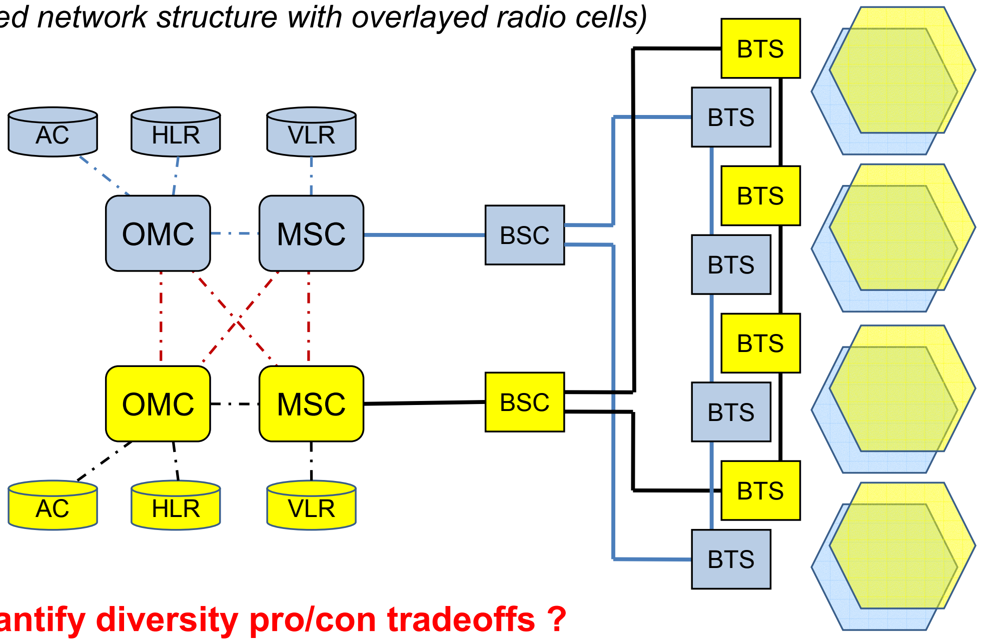
Time related
- *expansion*
- *evolution*
- *. . .*

Compatibility
(backward & forward)

A different focus/role for standards ?

Architectures with explicit redundancy

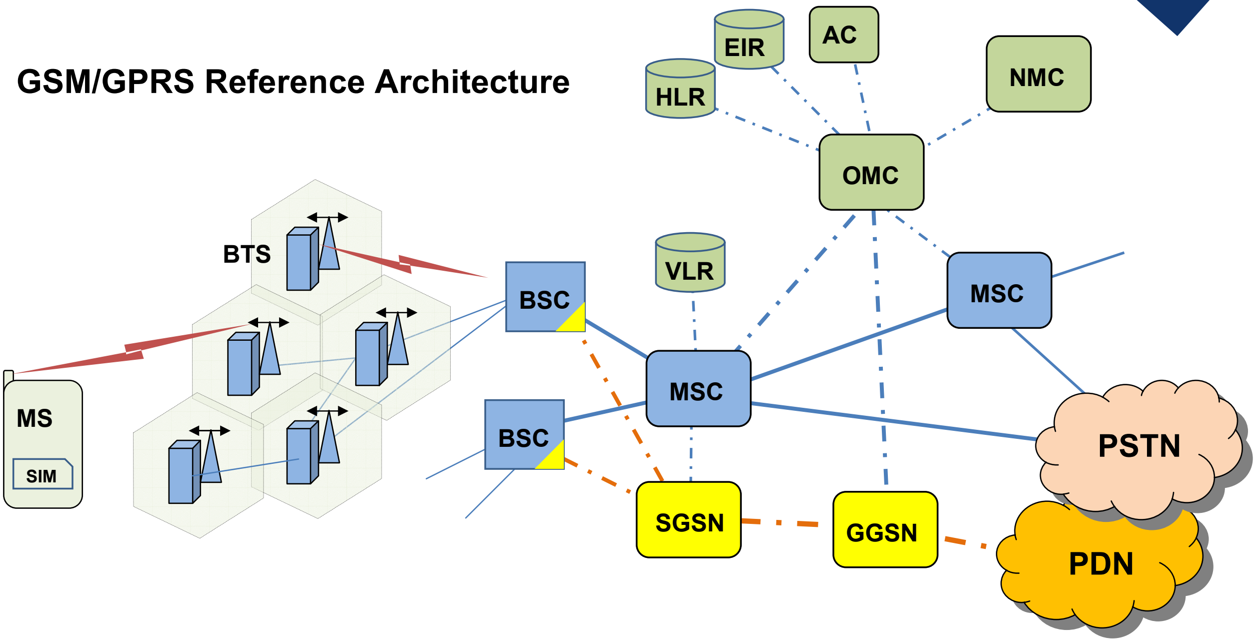
Suggested fully redundant GSM-R architecture
(Fully duplicated network structure with overlayed radio cells)



Can we quantify diversity pro/con tradeoffs ?

Architectures without explicit redundancy

GSM/GPRS Reference Architecture



Time related diversity is unavoidable in complex, long lasting systems

10/22/2007

Resilient Systems
Current Research and Future Directions

ReSIST workshop, Rome
October 18, 2007

ICT Programme
Security research

Yves Paindaveine
Security Unit
DG Information Society and Media

Outline

- Research in Resilience: from Research to Applied Research
  - (recent) past achievements
  - 1st FP7 Calls, ICT and

    SECURITY

- Future directions: Towards Resilient Infrastructures
  - Next call(s)

From Research to Applied Research

6th FP “Towards a global dependability and security framework”

Key Objectives & Breakthroughs

- build on EU technical and scientific excellence on security, dependability and resilience
- meet EU demands for privacy and trust
- strengthen the interplay between research and policy

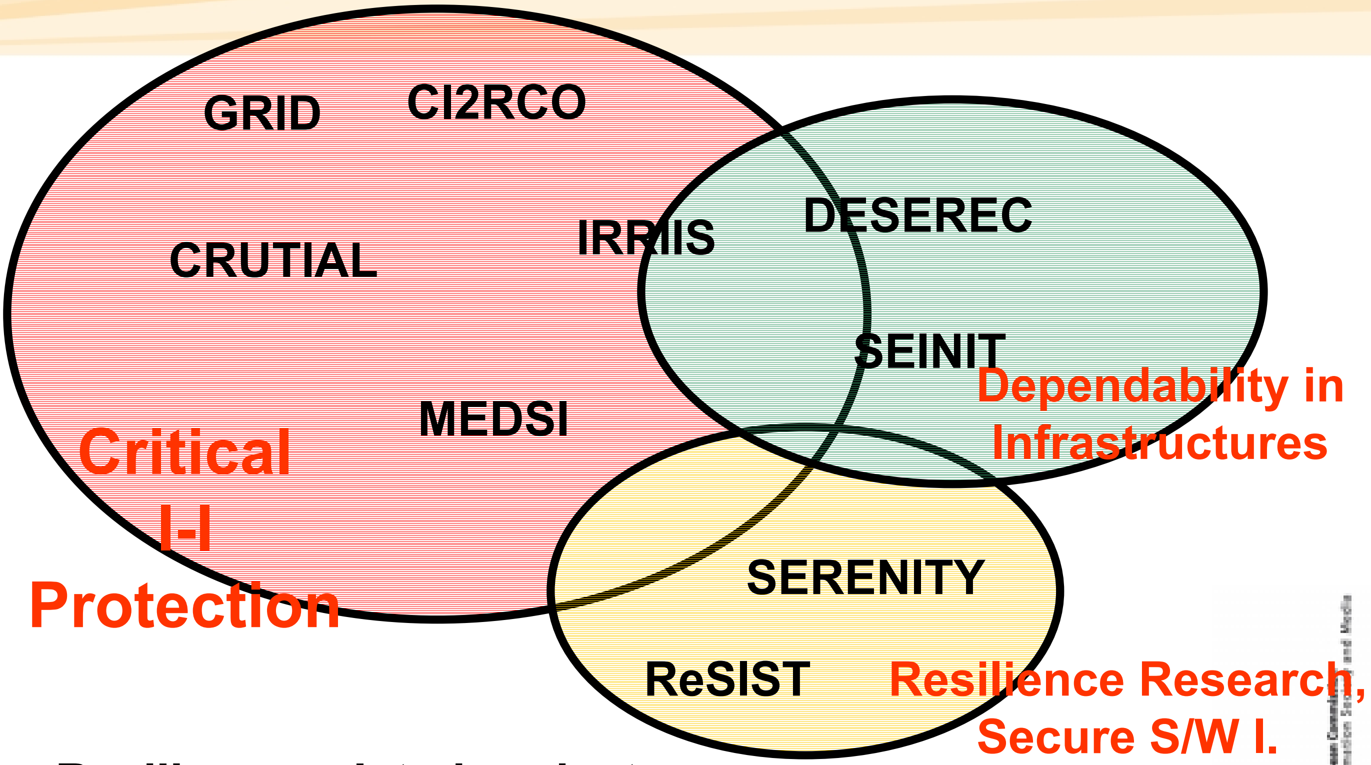
Budget ~ 145 M¤

Research Focus:

- security and dependability challenges arising from complexity, ubiquity and autonomy
- resilience, self-healing, mobility, dynamic content and volatile environments
- Multi-modal and secure application of Biometrics
- Identification, authentication, privacy, Trusted Computing, digital asset management
- Trust in the net: malware, viruses, cyber crime

Choices
Security
Flexibility

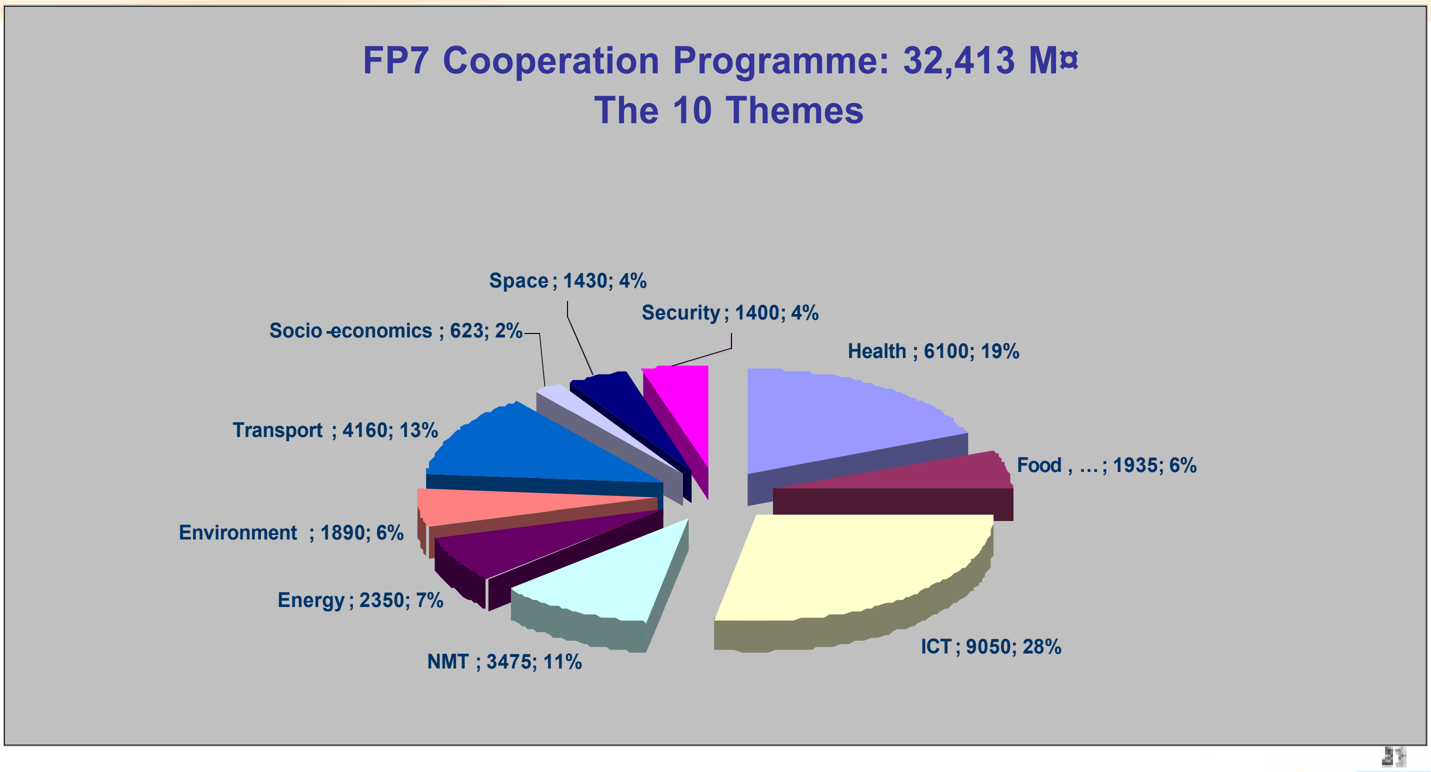
From Research to Applied Research Past Achievements (FP6)



Resilience-related projects

7th EU Framework Programme for RTD 2007-2013

Total 50,521 M€

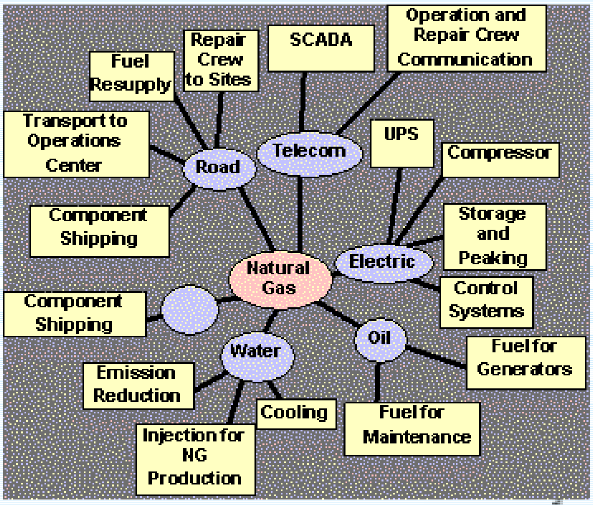


FP7 Cooperation Programme: 32,413 M¤
The 10 Themes

Strengthening Competitiveness through Co-operation

Towards Resilient Critical Infrastructures Challenges Ahead

- Technology development
- Liberalisation, Deregulation
- Global, Cross border CI’s
  - ➔ Different policy & regulatory frameworks
  - ➔ Different protection measures and technologies
- Openness & Interconnection
  - ➔ Interdependencies
  - ➔ Large scale, multi layer systems
  - ➔ Complexity, Chaotic Behavior
  - ➔ New Vulnerabilities, Cyber-threats
- Law enforcement, Crisis Management
- Not designed as integrated systems, as they are operating today



Fuel Resupply

Repair Crew to Sites

SCADA

Operation and Repair Crew Communication

Transport to Operations Center

Road

Telecom

UPS

Compressor

Component Shipping

Storage and Peaking

Natural Gas

Electric

Component Shipping

Control Systems

Water

Oil

Fuel for Generators

Emission Reduction

Cooling

Fuel for Maintenance

Injection for NG Production

Resilient Critical Infrastructures
The EC Context

Policy

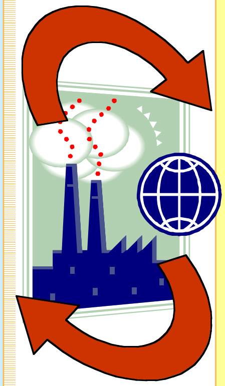
2004: EU program on CIP (EPCIP) and CI Warning Info Network (CIWIN)

2006: Communication and Directive on EPCIP – sectoral approach

2007: Communication on Protecting Europe's Critical Energy and Transport Infrastructure

2007: INFSO consultation process for policy initiative in ICT CIIP sector

ARECI study on Electronic Infrastructures



Research

IST-FP6 (2002-2006)
9 RTD projects, 36M¤ EU funding

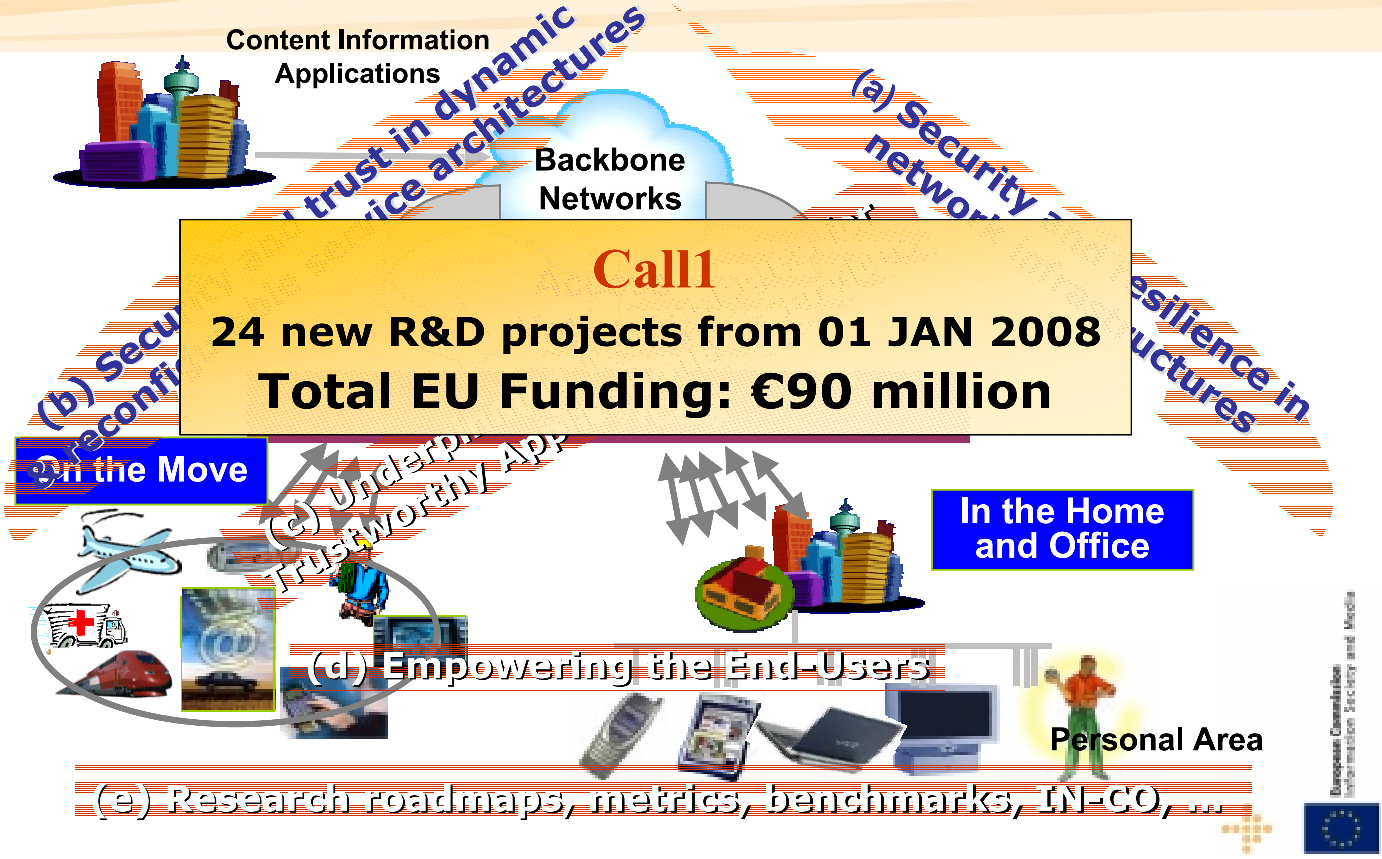
PASR (2004-2006)
5 projects for about 11,5M¤ – total cost

FP7 ICT Call 1 (Apr 2007)
Focused on security and trust in Networks and Services, and underpinning technologies

FP7 ICT-SEC (Nov 2007)
ICT-Security Research Joint Call on Critical Infrastructure Protection

7th EU Research Framework Programme (2007-2013)

"Secure, dependable & trusted infrastructures"

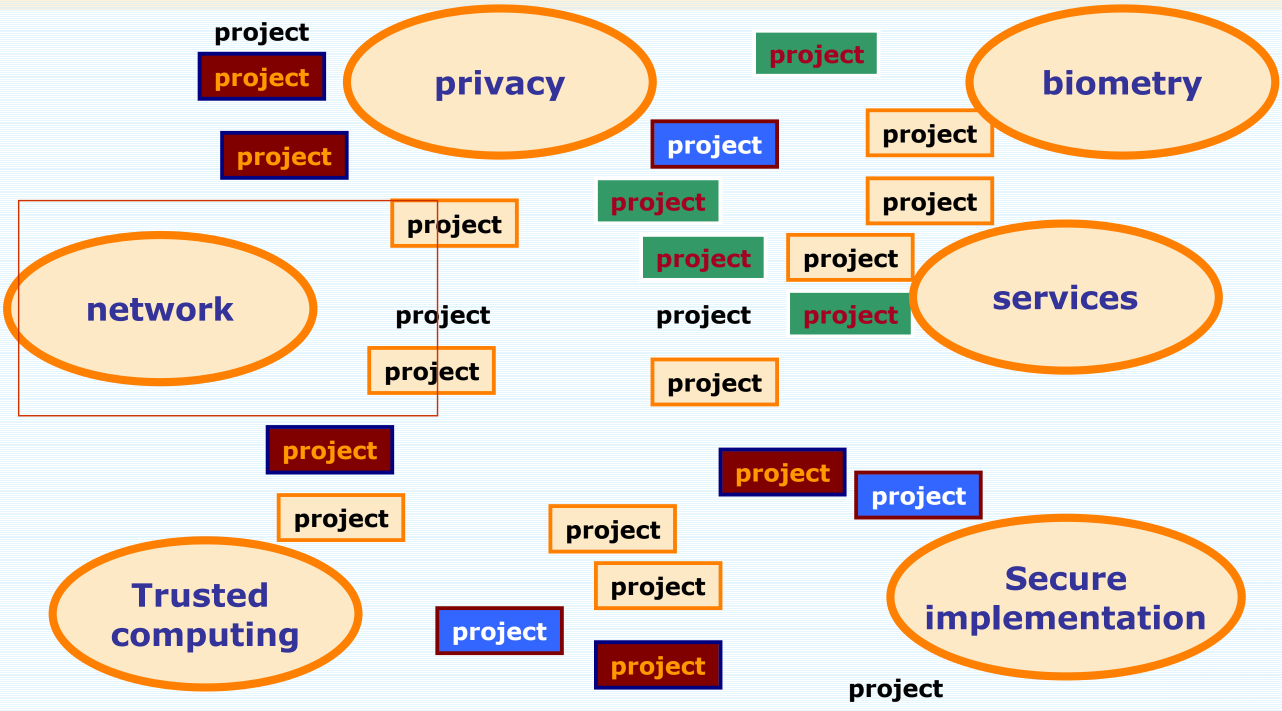


Call1

24 new R&D projects from 01 JAN 2008

Total EU Funding: €90 million

Research in FP7, call 1
Projects under negotiation, funding: 90 M€
PROVISIONAL



Critical Infrastructures Protection
Ongoing PASR work

- Vital Infrastructures Threats and Assurance
- Transport Infrastructures Protection System
- Open Robust Infrastructures
- Protection of Air Transportation and Infrastructure
- On-line monitoring of drinking water

Work in DG RTD: ETP SmartGrids

… the role of ICT (Information and Communication Technology) in adapting electricity networks to real time actions and managing distributed control in the network will be a critical contribution

Development will be taken beyond systems to determine integrated ICT solutions for both transmission and distribution networks.

… new solutions will be developed for data access, transfer and management between all parties in the liberalised sector …

European Commission
Information Society and Media

Towards the Joint Call on CIP

Holistic view on
security and resilience of CI's,
including non-technical aspects

System technology, organisation and management, governance, business, users, legal, regulatory

➡ **Overall resilience and security**

European Commission
Information Society and Media

Towards the Joint Call on CIP

- Two perspectives
  - Technology building blocks for resilient critical networks, communication and control
  - Capability building for security of citizens

Joint Call between Security and ICT Themes on Protection of Critical Infrastructures

Objectives

- Create more secure and dependable Critical Infrastructures (CI's)

  ➔Protect CI's against deliberate acts of terrorism, natural disasters, negligence, mismanagements, accidents, computer hacking, criminal activity and malicious behaviour
- Develop new technical solutions that support and refine the EPCIP policy options and legislative processes

Joint Call between Security and ICT Themes
Critical Infrastructure Protection (3)

Focus of the ICT Theme – Budget: 20 m€

Technology building blocks for creating secure, resilient, responsive and always available information infrastructures linking critical infrastructures (CI's)

a) mastering interactions and complexity of LCCI; preventing against cascading effects; providing recovery and continuity (self-adapted and self-healing); quantifying dependability and resilience of interdependencies

b) Designing and developing distributed information and process control systems; systemic risk analysis and security configuration; dynamic assurance frameworks; security forensics

c) Longer term visions and roadmaps; metrics and benchmarks -> certification and standardisation; international cooperation; coordination with other programmes or initiatives

Joint Call between Security and ICT Themes
Protection of Critical Infrastructures (4)

Focus of the Security Theme – Budget: 20 m€

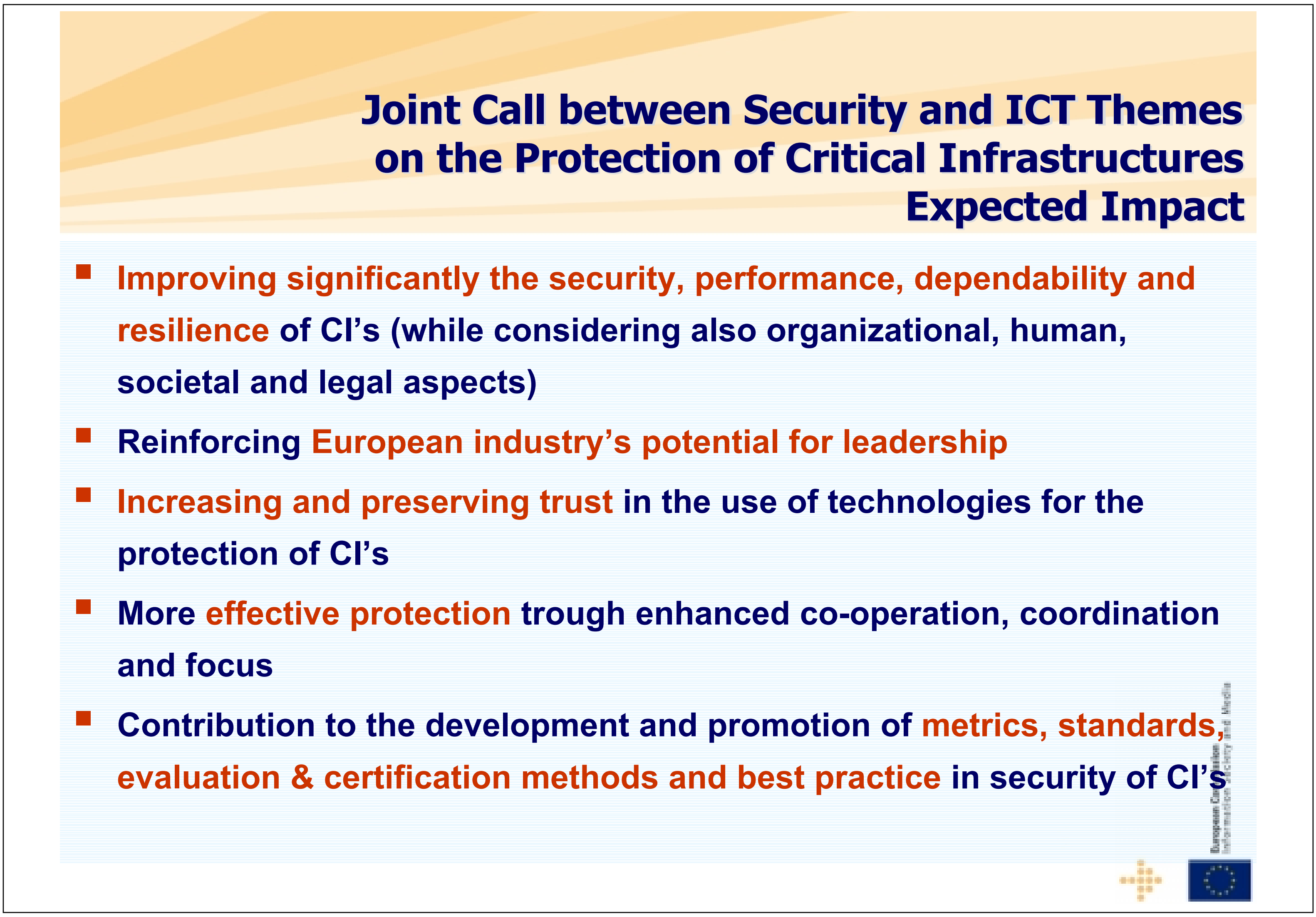
Technology building blocks for secure, resilient and always available transport & energy infrastructures that survive malicious attacks or accidental failures and guarantee continuous provision of services

a) ICT-SEC-2007-1.0-01: integrated frameworks/methodologies for global analysis of risks; contingency management based on emergency plans

b) ICT-SEC-2007-1.0-02: Modelling & simulation including scenario building to support training of crisis managers

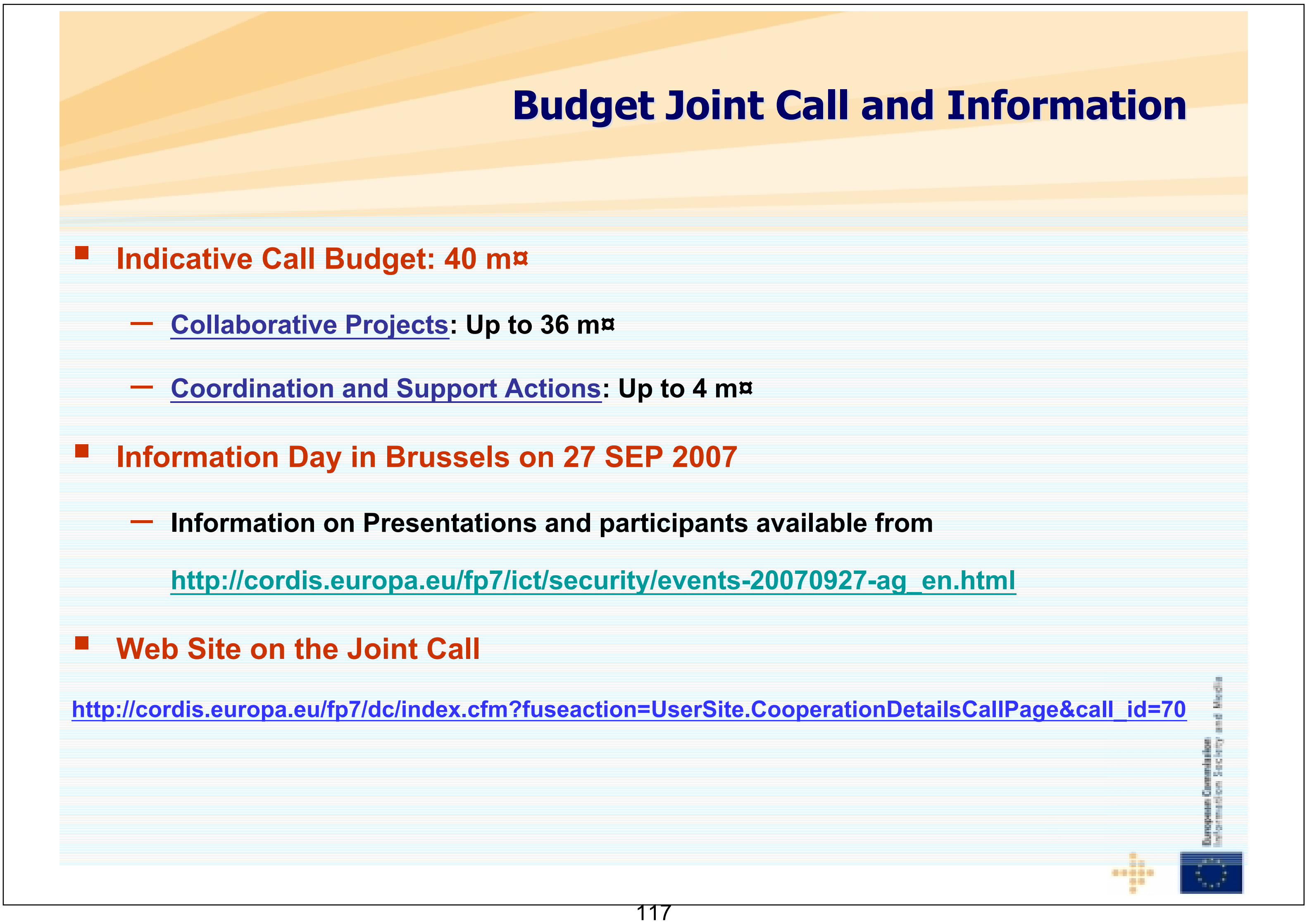
c) ICT-SEC-2007-1.0-03: Tools for the integration of smart surveillance to build high-level situation awareness

d) ICT-SEC-2007-1.0-04: Novel technologies for personal digital support systems as part of emergency management; first responders in crisis



Joint Call between Security and ICT Themes on the Protection of Critical Infrastructures Expected Impact

- Improving significantly the security, performance, dependability and resilience of CI’s (while considering also organizational, human, societal and legal aspects)
- Reinforcing European industry’s potential for leadership
- Increasing and preserving trust in the use of technologies for the protection of CI’s
- More effective protection trough enhanced co-operation, coordination and focus
- Contribution to the development and promotion of metrics, standards, evaluation & certification methods and best practice in security of CI’s



Budget Joint Call and Information

- Indicative Call Budget: 40 m¤
  - Collaborative Projects: Up to 36 m¤
  - Coordination and Support Actions: Up to 4 m¤
- Information Day in Brussels on 27 SEP 2007
  - Information on Presentations and participants available from http://cordis.europa.eu/fp7/ict/security/events-20070927-ag_en.html
- Web Site on the Joint Call

http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=70

Further Information & Contact

- *Call information*
  - → CORDIS call page and work programme, evaluation forms: http://cordis.europa.eu/fp7/calls/

- *General sources of help:*
  - → The Commission's FP7 Enquiry service : http://ec.europa.eu/research/enquiries
  - → National Contact Points : http://cordis.europa.eu/fp7/ncp_en.html

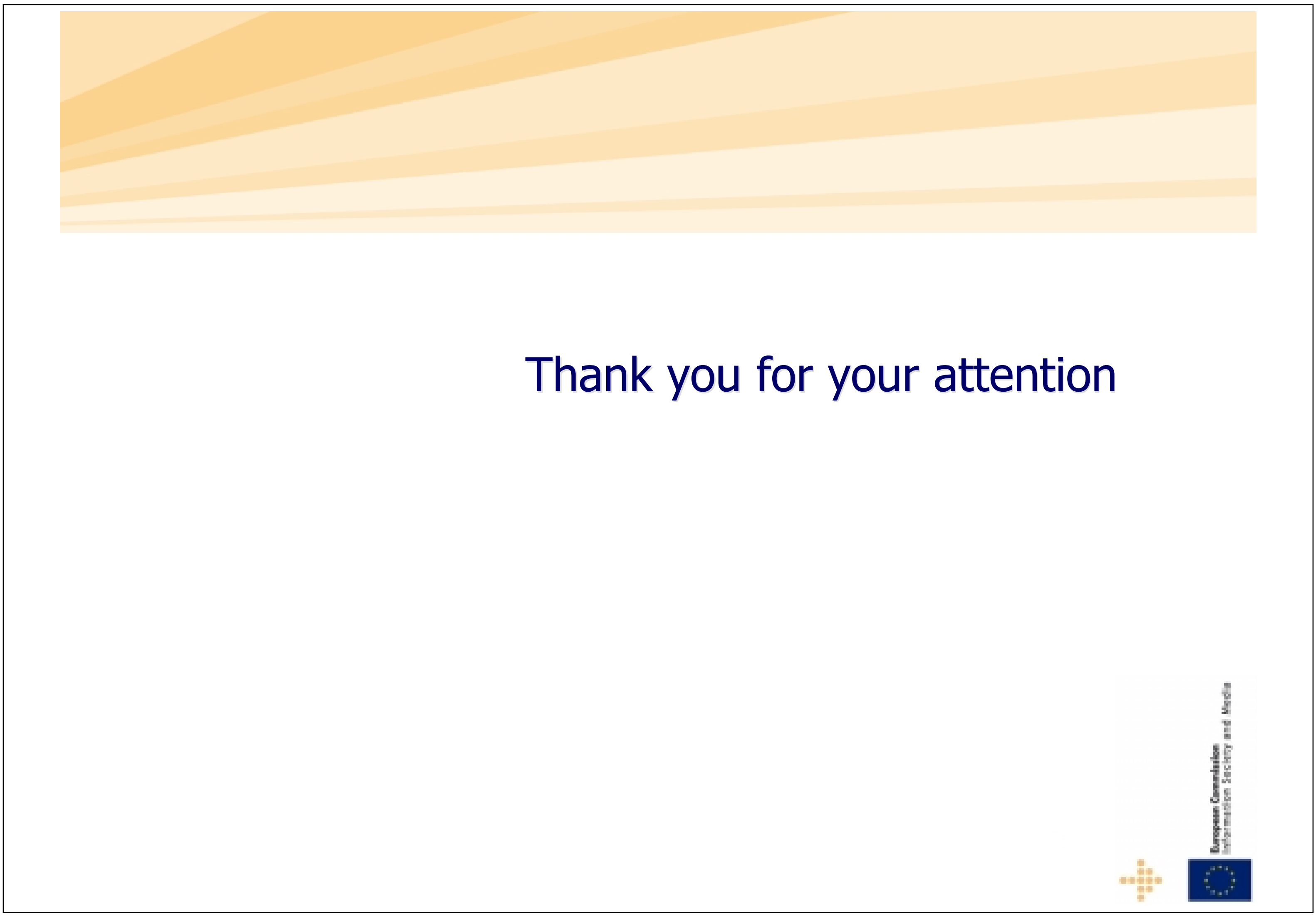
- *Specialised and technical assistance:*
  - → CORDIS help desk : http://cordis.europa.eu/guidance/helpdesk/home_en.html
  - → CORDIS FP7 service : cordis.europa.eu/fp7/participate_en.html
  - → Risk sharing financing facility (European Investment Bank): http://www.eib.org/rsff
  - → EPSS Help desk e-mail: support@epss-fp7.org
  - → IPR helpdesk http://www.ipr-helpdesk.org
  - → ICT Information Desk email: ict@ec.europa.eu
  - → Security Information Desk e-mail: entr-security-research@ec.europa.eu

- Contacts for the Joint Call:
  - → [ICT Theme] Angelo.Marino AT ec.europa.eu,
  - → [Security Theme] Laurent.Cabirol AT ec.europa.eu

Working as an expert on EU projects

Registering as an expert for evaluations and reviews of EU projects:

https://cordis.europa.eu/emmfp7/



Thank you for your attention

5- ReSIST Brochure

ReSIST

Resilience for Survivability in IST

A European Network of Excellence

Information Society Technologies

SIXTH FRAMEWORK PROGRAMME

Partners: LAAS-CNRS (Coordinator)
Budapest University of Technology and Economics
City University, London
Technische Universität Darmstadt
Deep Blue Srl
Institut Eurécom
France Telecom Recherche et Développement
IBM Research GmbH
Université de Rennes 1 – IRISA
Université de Toulouse III – IRIT
Vytautas Magnus University, Kaunas
Fundação da Faculdade de Ciencias da Universidade de Lisboa
University of Newcastle upon Tyne
Università di Pisa
QinetiQ Limited
Università degli studi di Roma "La Sapienza"
Universität Ulm
University of Southampton

http://www.resist-noe.eu

2 October 2007

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.

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. 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 (Figure 1).

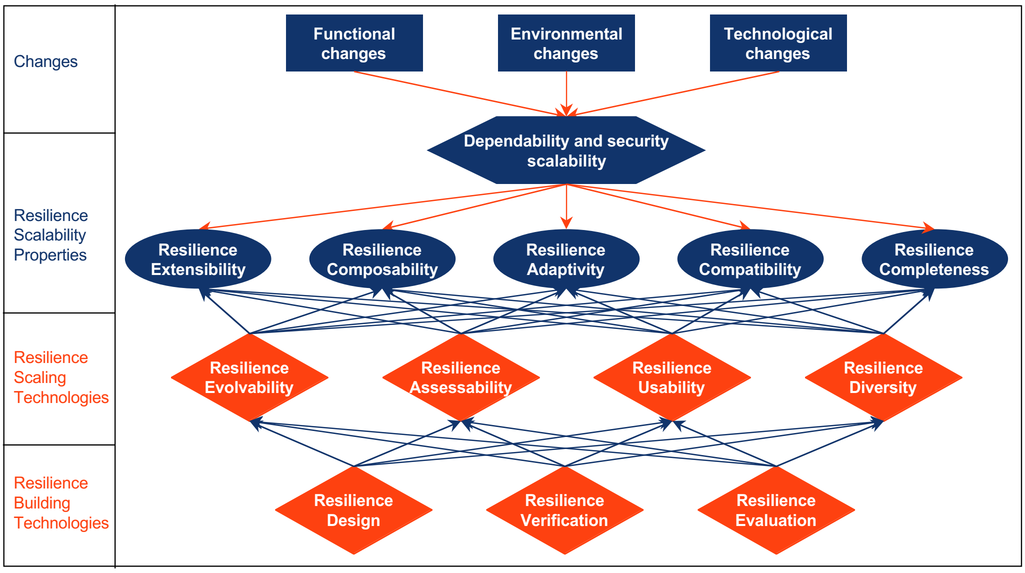


Figure 1 - Scalable resilience

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.

Joint Programme of Activities

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

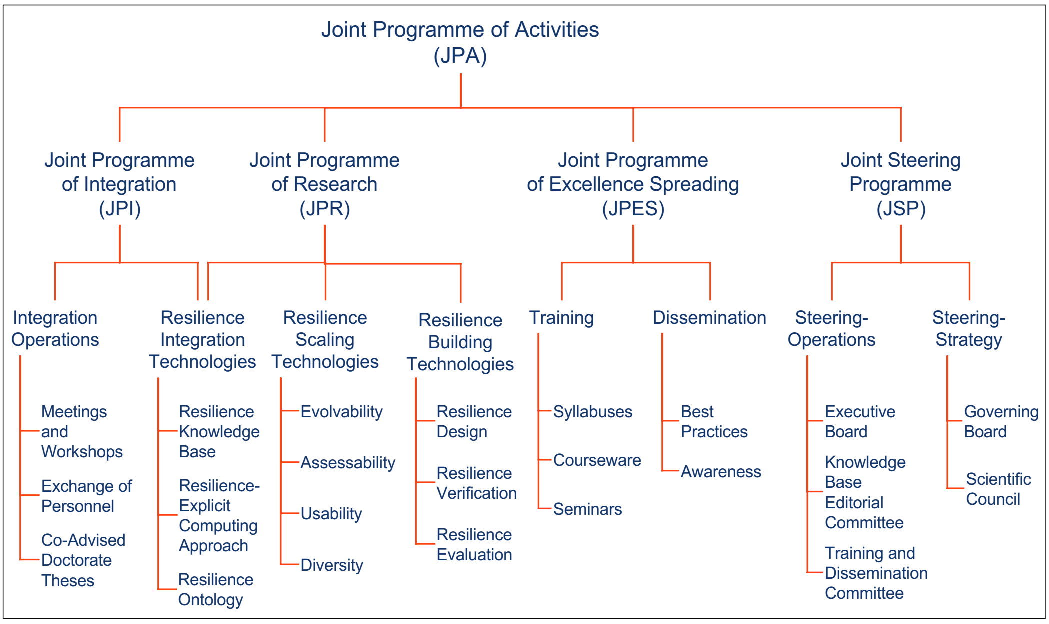

Joint Programme of Activities (JPA)
Joint Programme of Integration (JPI)
Joint Programme of Research (JPR)
Joint Programme of Excellence Spreading (JPES)
Joint Steering Programme (JSP)
Integration Operations
Meetings and Workshops
Exchange of Personnel
Co-Advised Doctorate Theses
Resilience Integration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

Figure 2 - JPA components

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.

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

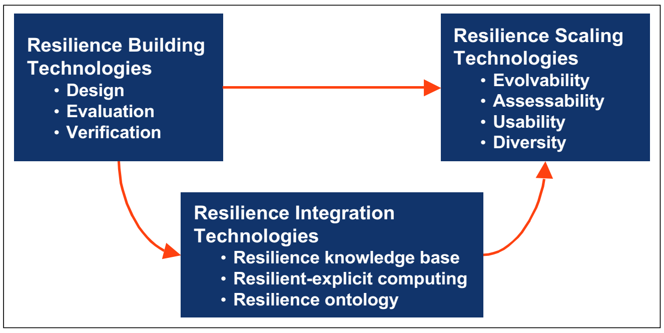

Resilience Building Technologies
• Design
• Evaluation
• Verification
Resilience Scaling Technologies
• Evolvability
• Assessability
• Usability
• Diversity
Resilience Integration Technologies
• Resilience knowledge base
• Resilient-explicit computing
• Resilience ontology

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.

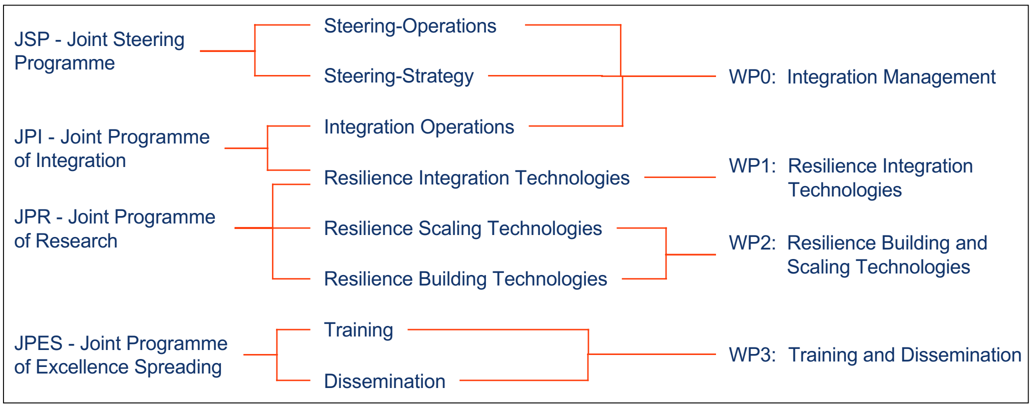

JSP - Joint Steering Programme
JPI - Joint Programme of Integration
JPR - Joint Programme of Research
JPES - Joint Programme of Excellence Spreading
Steering-Operations
Steering-Strategy
Integration Operations
Resilience Integration Technologies
Resilience Scaling Technologies
Resilience Building Technologies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

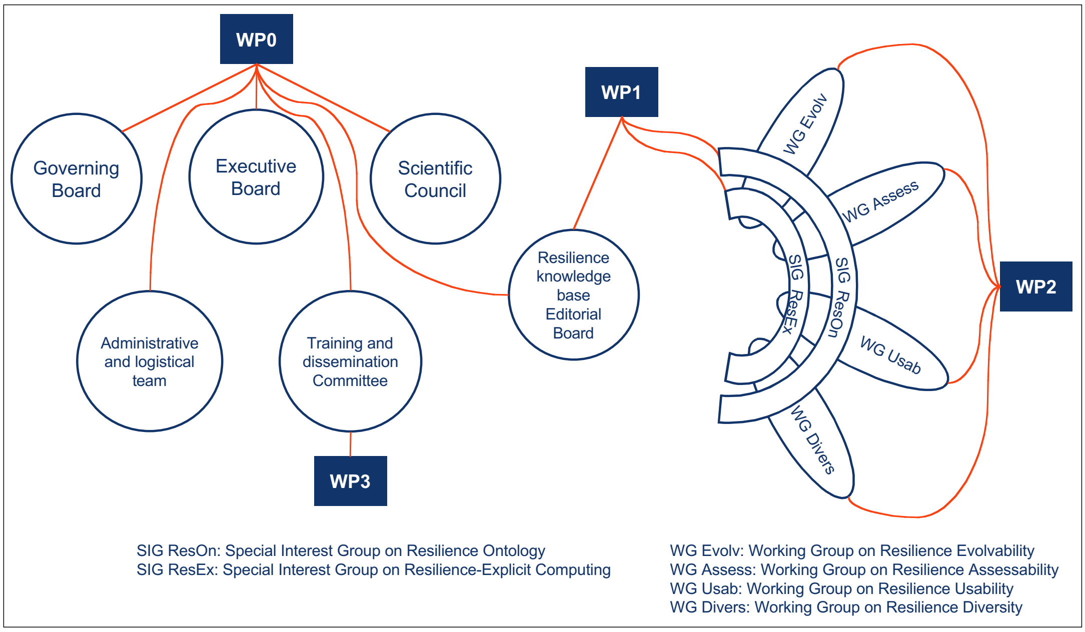

WP0
Governing Board
Executive Board
Scientific Council
Administrative and logistical team
Training and dissemination Committee
WP3
WP1
Resilience knowledge base Editorial Board
WG Evolv
WG Assess
SIG ResOn
SIG ResEx
WG Usab
WG Divers
WP2
SIG ResOn: Special Interest Group on Resilience Ontology
SIG ResEx: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

Results

The major achievements of the ReSIST activity have been the production of a) a State of Knowledge in Resilience-Building Technologies and a Research Agenda in Resilient Computing, and of b) a prototype of the Resilience Knowledge Base.

The work for producing the State of Knowledge in Resilience-Building Technologies has been carried out by five working groups dealing with different aspects of resilience building technologies and the corresponding subdisciplinary areas. The document is therefore made up of five parts, each produced by one of the working groups: architecture, algorithms, socio-technical issues, evaluation, verification.

Each working group then produced its views in terms of research gaps and challenges according to the four resilience-scaling technologies: evolvability, assessability, usability, diversity. The corresponding texts have constituted starting points for newly formed working groups, according to these resilience-scaling technologies. The texts have been reworked, augmented, and supplemented. Syntheses have been produced, where the various gaps and challenges have been clustered. The syntheses and the detailed ‘research gaps and challenges’ texts constitute the ReSIST view of a Research Agenda in Resilient Computing, entitled 'From Resilience-Building to Resilience-Scaling Technologies: Directions'.

Both documents, co-authored by a total of 83 researchers and doctorate students, have been extensively reviewed by the ReSIST members.

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 40 millions basic facts, from three classes of information: a) resilience data captured from each partner’s information resources, b) external sources including the compendium of the 33 editions of the Fault-Tolerant Computing Symposia / Dependable Systems and Networks Conferences, c) two ontologies, on Dependability and Security, and on Systems concepts.

In addition to the above facts, ground work has been performed on:

- The Resilience-Explicit Computing approach, with the production of a document presenting a first edition of both the approach and a first set of resilience mechanisms, including their metadata. The mechanisms have been integrated in the Resilience Knowledge Base.
- The Best Practice Document, its production being prepared by the holding of a workshop gathering 17 industrial experts, from all application fields of information technologies (Università di Roma ‘La Sapienza’, 16-17 October 2007).
- Education, with the production of a draft Curriculum in Resilient Computing, and of a Resilient Computing Courseware outline.

Besides the achievements addressed so far, a number of significant events are worth mentionng:

- Gathering of 101 ReSIST participants to the initial plenary meeting of the network (LAAS, 21-23 March 2006), and of 80 participants to the second plenary meeting (Budapest University of Technology and Economics, 19-21 March 2007).
- Holding of the first Open Workshop (Budapest University of Technology and Economics, 21-22 March 2007), attended by 93 participants, and of the second Open Workshop (Università di Roma ‘La Sapienza’, 18 October 2007).
- 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.
- Holding of the Summer School (in Porquerolles Isaland, France, on 23-28 September 2007), with an attendance of 66 (ReSIST members, doctorate students and industry engineers), out of which 18 external to the network.

Figure 6 shows the contribution of the ReSIST activities, according to components of the Joint Programme of Activities, to the network objectives.

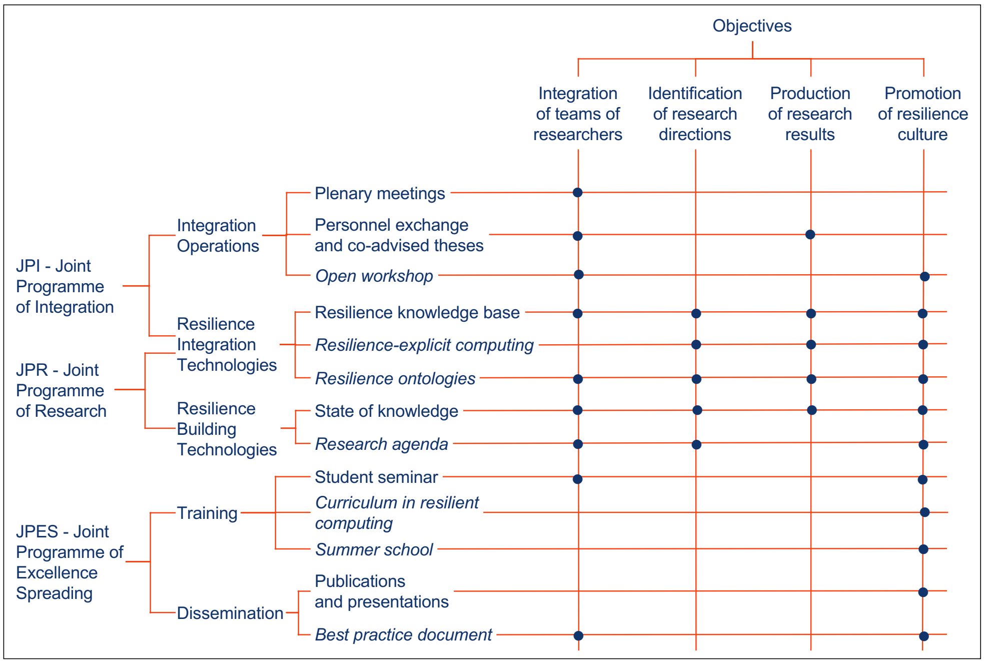

Objectives
Integration of teams of researchers
Identification of research directions
Production of research results
Promotion of resilience culture
JPI - Joint Programme of Integration
JPR - Joint Programme of Research
JPES - Joint Programme of Excellence Spreading
Integration Operations
Resilience Integration Technologies
Resilience Building Technologies
Training
Dissemination
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