

MSc Curriculum in Resilient Computing*

Luca Simoncini

University of Pisa, Italy

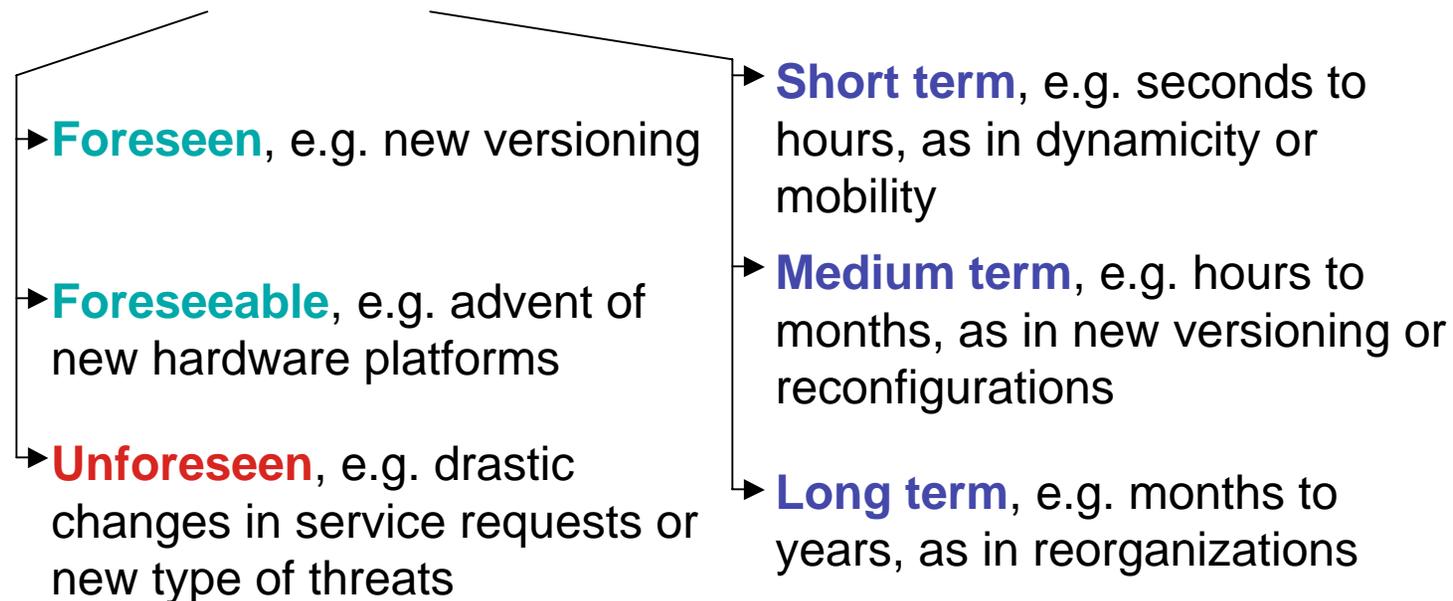
* Co-operative work in the frame of EU NoE ReSIST
<http://www.resist-noe.org/>



Why a curriculum on Resilient Computing

Resilience (for computing systems and information infrastructures): the persistence of service delivery that can justifiably be trusted, when facing changes (functional, environmental or technological)

Changes:



Computing in the future



Table 1. Examples of Pervasive Computing

• Wearable Computers	• Smart Classrooms
• Wearable Keyboards	• Enhanced Learning Environments
• Smart Homes	• Telematics
• Active Badges	• GPS-equipped Automobiles
• Active RFID tags	

Table 2. Two Alternate Futures

Future Given Current Trends	Trustworthy Future
Spam	Hassle-free systems
Identity theft	User-controlled privacy
Network outages	Self-aware networks
Malware	Self-adjusting networks
Frequent manual intervention	Self-healing networks
Unchecked abuses of laws and rights	Balanced regulation and law enforcement

Four Grand Challenges:

1. Eliminate Epidemic Attacks by 2014
2. Enable Trusted Systems for Important Societal Applications
3. Develop Accurate Risk Analysis for Cyber-security
4. Secure the Ubiquitous Computing Environments of the Future

Some examples of recent resilience problems

➤ **“Over the past five years, high profile IT difficulties have affected the [UK’s] Child Support Agency, Passport Office, Criminal Records Bureau, Inland Revenue, National Air Traffic Services and the Department of Work and Pensions, among others”**

S. Pearce. Government IT Projects, Report 200, Parliamentary Office of Science and Technology, 7 Millbank, London, 2003.

➤ **The French Insurer’s Association estimates the yearly cost of computer failures to be 2 B Euros, of which slightly more than half is due to malicious faults (e.g. by hackers and corrupt insiders)**

<https://www.clusif.asso.fr/fr/production/sinistralite/index.asp>

➤ **“At 03.25hrs on Sunday 28 September 2003, the Italian power system experienced a power failure across all of Italy because of an inadequate SCADA (supervisory control and data acquisition) systems... The electricity supply to Rome was not restored until late afternoon and the remainder by late evening”**

Report of Joint Energy Security of Supply Working Group - http://www.dti.gov.uk/energy/jess/blackout_note.pdf

➤ **“Nearly 10 million people in the US suffered from some kind of on-line fraud last year ... the total cost was \$1.2bn”**

Stated by Gartner at RSA Conference, February 2005 - <http://www.vnunet.com/news/1161375>

➤ **“Law enforcement agencies in the United States and overseas recently disrupted an on-line organised crime ring that spanned eight U.S. states and six countries ... 7 million credit card numbers had been stolen by the crime ring, costing consumers and credit card companies around \$4.3 million”**

Ralph Basham, Director of the U.S. Secret Service - <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=7667789>

➤ **“Mobile devices such as PDAs and cell phones are the new frontier for viruses, spam and other security threats ... 70 percent of all email traffic on the Internet is spam ... The number of known viruses grew by 28,327 in 2004 (for a running total of 112,438 known viruses) an increase of 25 percent from 2003”**

IBM 2004 Global Business Security Index Report - <http://www.ibm.com/news/be/en/2005/02/09.html>

➤ **“On 17 Mar 2005 the UK's National Hi-Tech Crime Unit reported a (foiled) attempt to steal £220m from the London offices of the Japanese bank Sumitomo Mitsui, by criminals who attempted to transfer the money electronically after hacking into the bank's systems”**

BBC News <http://news.bbc.co.uk/1/hi/uk/4356661.stm>

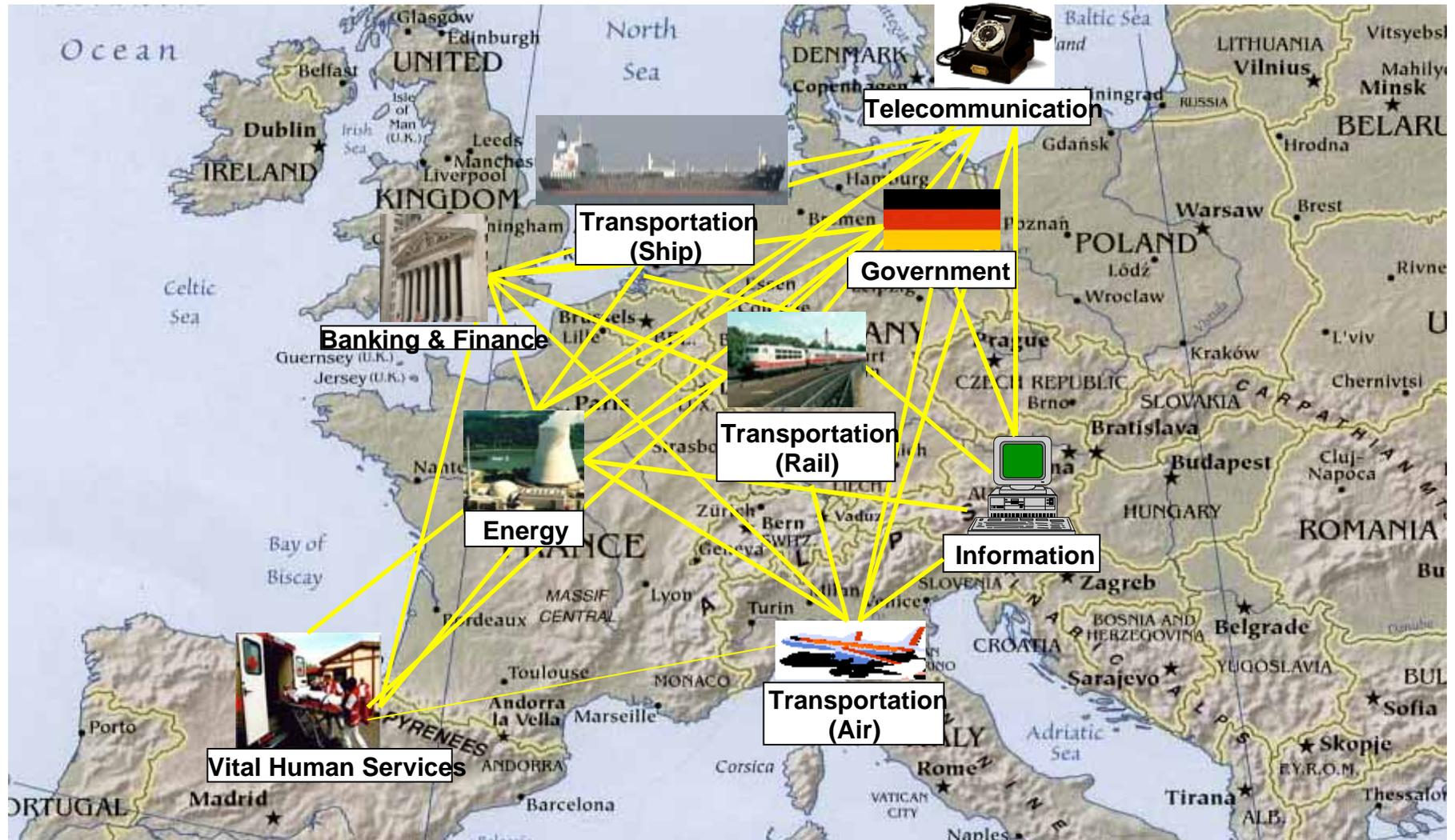
What about software ?

- In 1995, The Standish Group reported that the average US software project **overran its budgeted time by 190%**, **its budgeted costs by 222%**, and **delivered only 60%** of the planned functionality. Only **16%** of projects were **delivered at the estimated time and cost**, and **31%** of projects were **cancelled before delivery**, with larger companies performing much worse than smaller ones. Later Standish Group surveys show an improving trend, but success rates are still low
- A UK survey, published in the 2001 Annual Review of the British Computer Society showed a similar picture. **Of more than 500 development projects, only 3 (three!!!) met the survey's criteria for success.**
- In 2002, the **annual cost of poor quality software to the US economy was estimated at \$ 60B [NIST, 2002]**

Risks, novel problems and need for integration

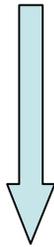
Class of Applications	Present or Potential Risks	Novel Problems	Need for Integration
Critical Utility Infrastructures (e.g. power distribution)	Black-outs (e.g. Italy 29/09/2003)	-Escalating and Cascading failures - Human Interaction	- New fault types - Interdependencies - Resilience for survivability
E-commerce (e.g. online auctions – eBay)	Frauds (several reported)	-Trusted identity management of dynamic sellers/buyers	- Identity mngmt. - Security - Legal issues
Personal digital devices	Potential catastrophe on a large-scale basis (not yet reported)	- “Common mode” failures affecting a very large number of untrained users at the same time	- Human interface - Public awareness - Societal issues

Complex systems need to be correct and resilient





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



- “Panic inducing” malicious faults
- “Huge multiplicity common mode” accidental faults



Catastrophic failure



Rationale

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

Avionics, railway signalling, nuclear control, etc.

Transaction processing, back-end servers, etc.

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

Scalability of Dependability
Beyond rigorous functional design, provision of
Resilience for Survivability,
wrt accidental and malicious threats

Logic



Partners

Budapest U
City U
Darmstadt U
DeepBlue
Eurecom

France Telecom R&D
IBM Zurich
IRISA
IRIT

LAAS-CNRS (Coord.)
Lisbon U
Newcastle U
Pisa U
QinetiQ

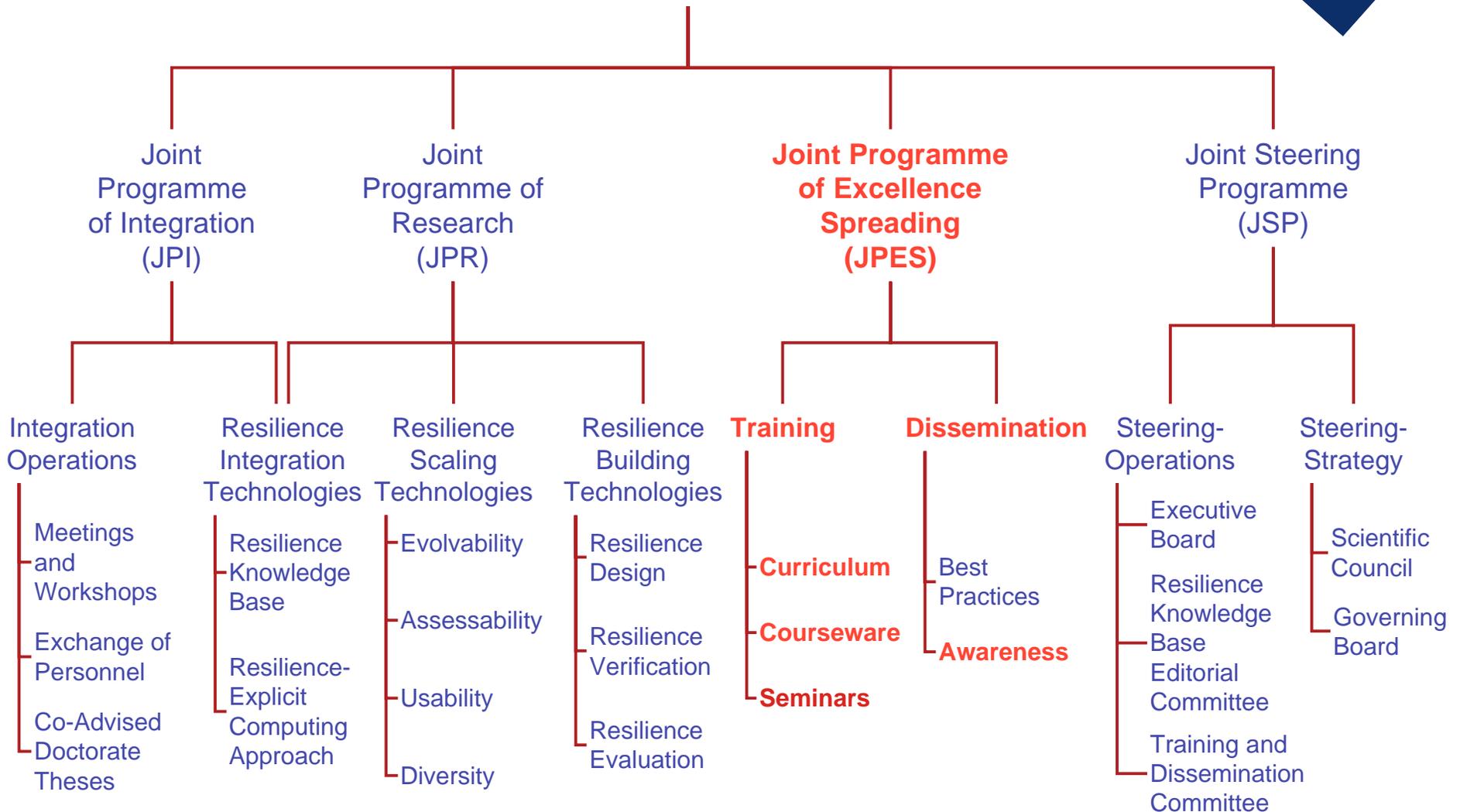
Roma-La Sapienza U
Southampton U
Ulm U
Vytautas Magnus U



Joint Programme of Activities insight



Joint Programme of Activities (JPA)



Curriculum rationale

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

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

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

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

From **Best Practices** → to **Methodical Scientific Approach**

Curriculum aims

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

Curriculum organization

1st Year

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

Courses:

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

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

Courses:

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

1st semester scheduling

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

2nd semester scheduling

Computer Networks Security
Fault and Intrusion-Tolerant Distributed Systems and Algorithms
Dependability Evaluation of Computer Systems
Testing, Verification and Validation
Usability and User Centered Design for Dependable and Usable Socio-technical Systems

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

Courses (common to all application tracks)

- **Management of Projects** (3 ECTS)
- **Fault Tolerant Middleware- based Systems** (3 ECTS)
- **Software Reliability Engineering** (3 ECTS)

Application track: **Telecom.**

Courses (specific for this track):

- **Resilience of Protocols and Architecture** (3 ECTS)
- **Resilience of Mobile Applications** (3 ECTS)

Application track: **Safety critical Systems**

Courses (specific for this track):

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

Application track: **e-Business**

Courses (specific for this track):

- **Resilience of SOA and Web-based Applications** (3 ECTS)
- **Damage Tolerance in Large scale Systems** (3 ECTS)

Common to all Application tracks:

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

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

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

Curriculum Pre-requisites

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

Contributions welcome !

- Review first year courses and their content
- Propose courses and application tracks for second year
- Identify existing support material for all courses

Means for contributing:

- Through the curriculum forum at ReSIST web portal
<http://www.resist-noe.org/>
- Through a dedicated Consultation Panel at:
<http://resist.isti.cnr.it/home.php>

Events of interest:

- **Professoral Seminar**, Newcastle, UK on Sept. 2-4, 2008 to inform on ReSIST findings and discuss with interested academics of the best way of disseminating this knowledge
- **Dedicated WSs** during 2008 on the MSc Curriculum on Resilient Computing

Persons interested to be informed:

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