

An Integrated Knowledge Base for European Dependability Research.®

Hugh Glaser, Ian Millard et al.

Electronics & Computer Science
University of Southampton

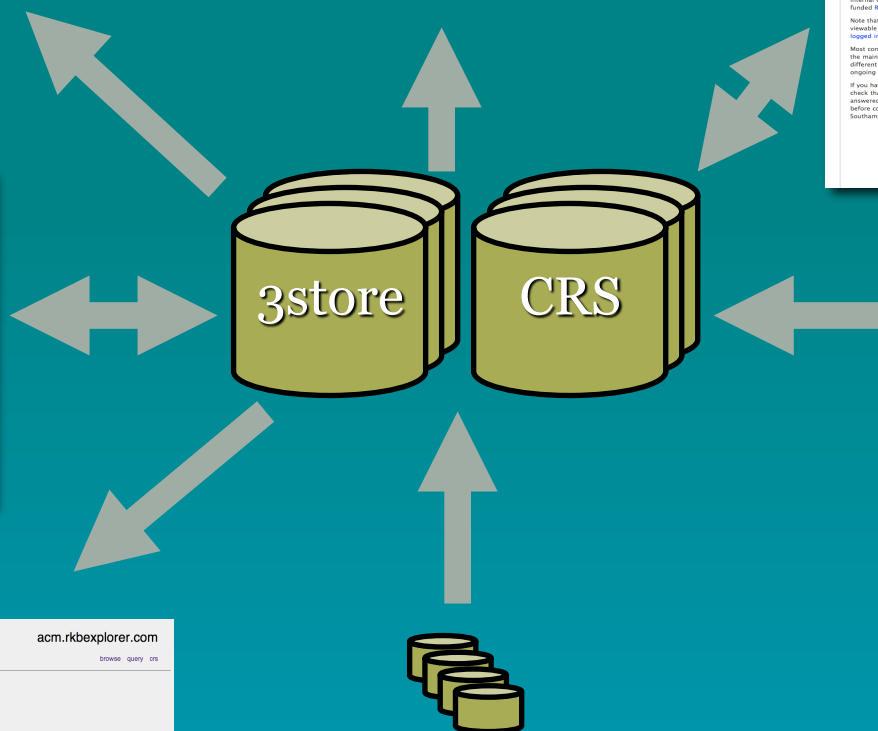
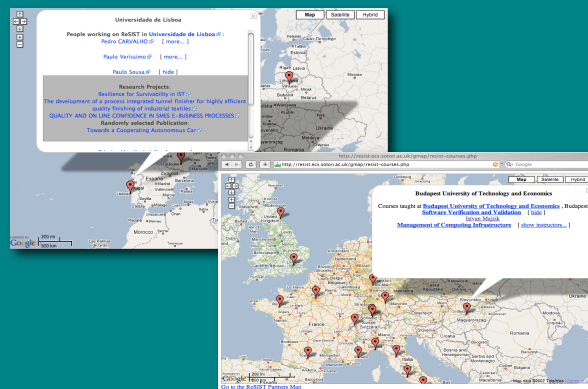
Newcastle University, 7th. October 2008



Overview

- A knowledge-enabled infrastructure to support
 - The ReSIST Project
 - Resilience-Explicit Computing
- A User Interface – the RKBExplorer
- Other components
- Sources
- Some vision
- Discussion

UNIVERSITY OF
Southampton
School of Electronics
and Computer Science



www.rkexplorer.com/explorer/

people mechanisms publications **projects** search

recently viewed assist help contact

ReStiff Resilience for Survivability in IST

Maintenance

Details

Name: ReStiff Resilience for Survivability in IST

Linked Data: [Resilience LIF](#)

7 7

People

Resilience Mechanisms

Publications

Projects

ReStiff RING Editorial Board

ReStiff Training and Dissemination Committee

ReStiff Executive Board

ReStiff Resilience-Digital Computing

[illegible][illegible]

Ontologies, etc,

Citeseer, CORDIS, DBLP,
Partners, UN LoCode, ...

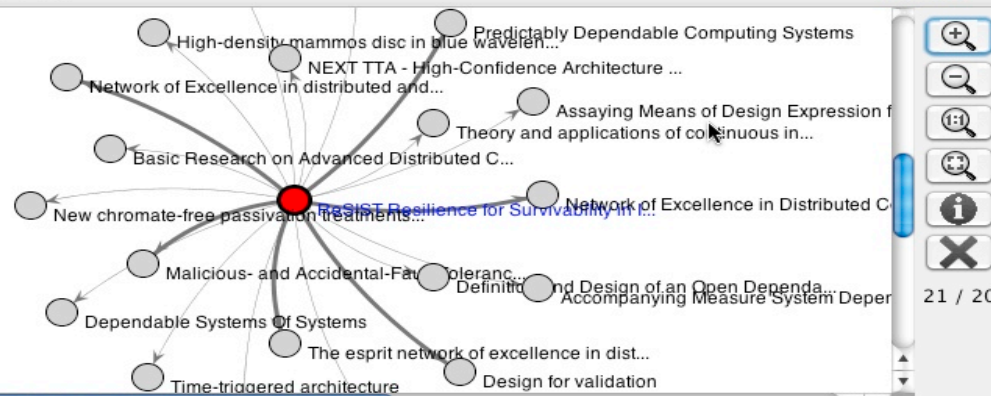


people research areas publications **projects** search

recently viewed reset help

Resilience for Survivability in IST

Maximize



Detail

Title:
Resilience for Survivability in IST

Other Names:
ReSIST Resilience for Survivability in IST

Funding:
4500000

Project Leader:
[Jean-Claude Laprie](#)

Leading Organisation:
Centre National de la recherche Scientifique

People

[Jean-Claude Laprie](#)

[Aad van Moorsel](#)

[Abdelmajid Khelil](#)

[Achour Mostefaou](#)

[Adnan Noon Mian](#)

[Afriz Jaffri](#)

[Agnan de Bonneval](#)

[Alberto Pasquini](#)

Research Areas

Information processing, information systems

Development Failure

Dependability And Security Analysis

Dependability And Security Provision

Publications

Revised version in Predictably dependable computing systems

ASSERT Automated proof based system and software engineering for real-time applications

Guide de la sûreté de fonctionnement

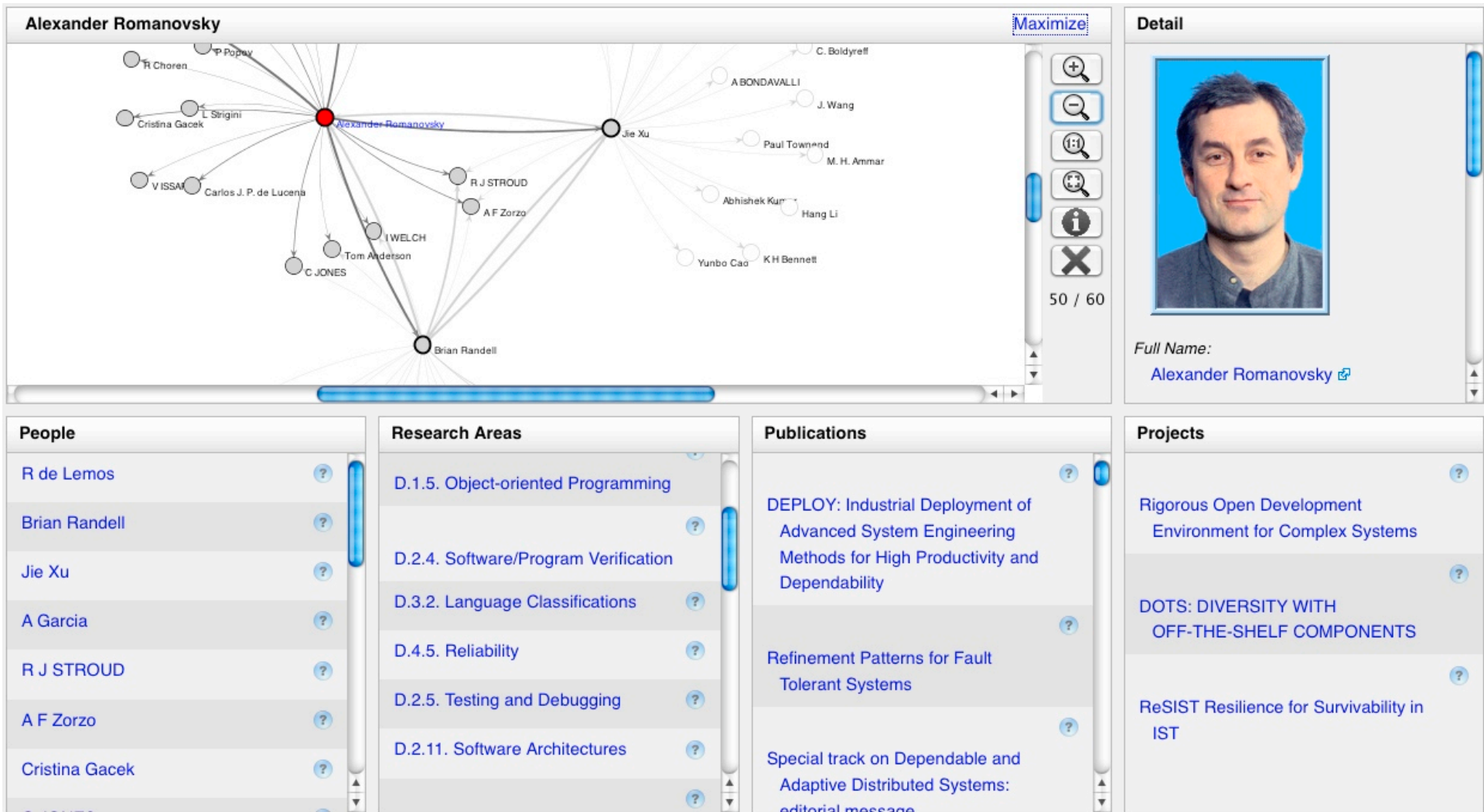
Projects

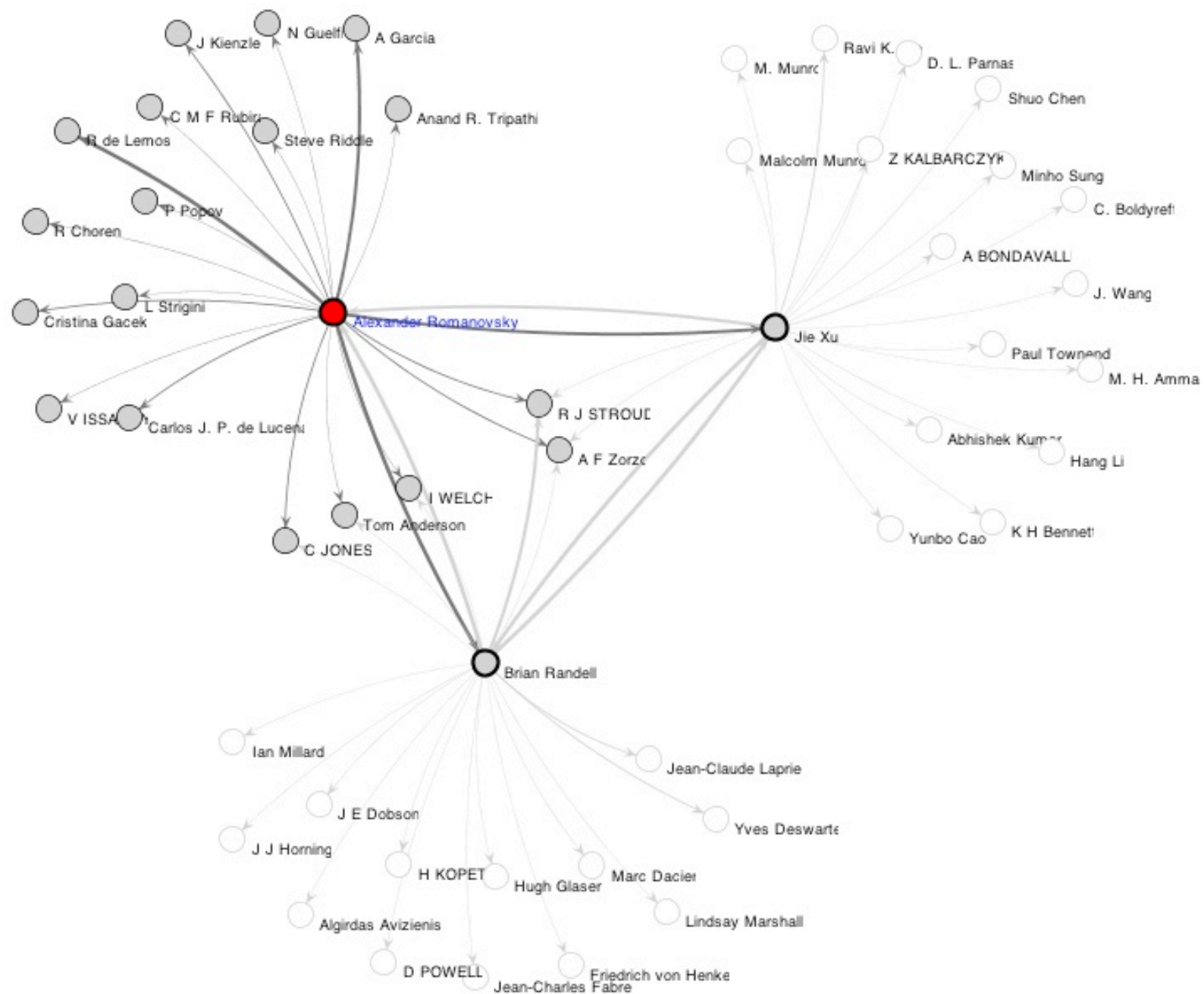
Malicious- and Accidental-Fault Tolerance for Internet Applications

The esprit network of excellence in distributed computing systems architectures

Design for validation

Network of Excellence in





[Alexander Romanovsky](#) is related to [R de Lemos](#)

They are linked by 33 relations.

Publications

They have co-authored 32 papers:

- [Coordinated Atomic Actions in Modelling Objects Cooperation](#)
- [Exception Handling in a Cooperative Object-Oriented Approach](#)
- [Integrating COTS Software Components into Dependable Software Architectures](#)

[\(29 more\)](#)

Affiliations

They are both affiliated to [NEWCASTLE UNIVERSITY](#).

This is a page that gives a simple demonstration showing papers which have been deemed related through textual analysis by IAI Saarbrücken. Up to the top 20 are listed for each paper, when they meet a simple thresholding:

1 – very strong – 0.9 – strongly – 0.7 – related – 0.6 – ignored – 0

The 1980 paper **Exception Handling and Software-Fault Tolerance** [\[browse\]](#)

is very strongly related to

- [\[browse\]](#) 2003 "Automatic detection and masking of non-atomic exception handling" [\[PDF\]](#)
- [\[browse\]](#) 1989 "Formal Verification of Programs with Exceptions"
- [\[browse\]](#) 1983 "Programming Reliable and Robust Software in ADA"

is strongly related to

- [\[browse\]](#) 1998 "Improving software robustness with dependability cases" [\[PDF\]](#)
- [\[browse\]](#) 1999 "Wrapping windows NT software for robustness" [\[PDF\]](#)
- [\[browse\]](#) 1981 "Exception Handling and Error Recovery Techniques in Modular Systems - An Application to the Isaure System"
- [\[browse\]](#) 2003 "Deadlock resolution via exceptions for dependable Java applications" [\[PDF\]](#)
- [\[browse\]](#) 2002 "Robust software - no more excuses" [\[PDF\]](#)

is related to

- [\[browse\]](#) 1995 "Fault tolerance in concurrent object-oriented software through coordinated error recovery" [\[PDF\]](#)
- [\[browse\]](#) 2004 "Implementing simple replication protocols using CORBA portable interceptors and Java serialization" [\[PDF\]](#)
- [\[browse\]](#) 1984 "Fault Tolerance Using Communicating Sequential Processes"
- [\[browse\]](#) 2001 "Middleware support for voting and data fusion" [\[PDF\]](#)

**RESILIENCE FOR SURVIVABILITY IN IST
KNOWLEDGE BASE**[Wiki](#)[RKB Browser](#)[Query RKB](#)[Course Metadata](#)

ReSIST / Welcome

Welcome to the ReSIST Wiki, which is the internal communication mechanism for the EU funded [ReSIST "Network of Excellence"](#).

Note that virtually all pages are private, and viewable only to ReSIST members who have [logged in](#).

Most content can be found by firstly browsing the main [ReSIST page](#), which details the different research areas in which activities are ongoing as part of the project.

If you have any questions or problems, please check that they have not previously been answered in the [frequently asked questions](#), before contacting [Ian Millard](#) or [Hugh Glaser](#) at Southampton.

Quick Links

[\[edit\]](#)

- [Frequently asked questions](#)
- [ReSIST project page](#)
- [Recent changes to the wiki](#)
- [Upload new file / View uploaded files](#)
- [ReSIST members / photos / locations](#)
- [Calendar of Events](#)
- [Browse](#), [query](#), or find out more about the [Resilience Knowledge Base](#)

Editing tools

- » [View Page](#)
- » [Discuss this page](#)
- » [Edit this page](#)
- » [History](#)
- » [Protect](#)
- » [Delete](#)
- » [Move](#)
- » [Watch this page](#)

Personal tools

- » [hugh glaser](#)
- » [My talk](#)
- » [Preferences](#)
- » [My watchlist](#)
- » [My contributions](#)
- » [Log out](#)

Search

Toolbox

- » [What links here](#)
- » [Related changes](#)
- » [Upload file](#)
- » [Special pages](#)

ReSIST :: Courses

http://resist.ecs.soton.ac.uk/courseware/edit/04dc6312

Google

**RESILIENCE FOR SURVIVABILITY IN IST
KNOWLEDGE BASE**

WikiRKB BrowserQuery RKB**Course Metadata**

ReSIST / Courses / Editing 'Advanced seminars on Distributed Systems'

Step 1 of 4: Information regarding the organisation of the course
(For questions, problems or feedback filling out this form, please [email us](#).)

Name of the course

Advanced seminars on Distributed Systems

Taught at
(CTRL+Click to select multiple values)

Universita degli studi di Roma, La Sapienza

Universitat ULM

Universite De Toulouse 1

Universite de Rennes 1

University of Naples

University of Toulouse III

[\[Add new item\]](#)

Currently being taught

<Select Currently being taught>

Description

The course focuses on recent advances on distributed systems. A set of topic is selected and studied through the help of original papers and, practically, most known distributed system platforms are selected and analyzed.

Language(s) of the course
(CTRL+Click to select multiple values)

English

Esperanto

Estonian

Finnish

French

Gaelic

Select Author(s)
(CTRL+Click to select multiple values)

Roberto Baldoni

Roberto Beraldi

Roberto Bonato

Robin Bloomfield

Ruta Marcinkeviciene

Sadie Creese

[\[Add new item\]](#)

ReSIST / Resilience-Explicit Computing Mechanisms

Name of the resilience mechanism N-Version Programming/1/1
(A title to identify your mechanism)

Submitted by [Zoe Andrews](#)
(The person(s) identified here shall be the point of contact for any queries relating to data entered into this form about this mechanism)

Author of mechanism [Algirdas Avizienis](#)
(Click on the "add new item" link to search for, and add, authors of this mechanism. These people should have a good understanding of the mechanism and may be the same as those identified in the previous question)

Associated projects [<None>](#)
(Click on the "add new item" link to search for, and add, projects that are associated with this mechanism. Possible associations include projects that: funded research on the mechanism; address similar aims; or use similar techniques)

Mechanism Objectives To utilise design diversity and voting in order to tolerate software faults
(Summary of the purpose of your mechanism in a sentence or two)

Detailed Description The information here applies to the specific variant of the mechanism NVP/1/1, described in "Definition and Analysis of Hardware- and Software-Fault Tolerant Architectures". The specific variant considered, NVP/1/1, has three diverse implementations of a software module. For a more general overview of the mechanism please see "The N-Version Approach to Fault-Tolerant Software".
(Either enter a detailed description of the mechanism here, should be detailed enough for the reader to be able to re-create the mechanism, or reference a paper with such text in below)

Detailed Description Publication [Definition and Analysis of Hardware- and Software-Fault-Tolerant Architectures](#)
(If applicable (see above), click on the "add

Editing "N-Version Programming/1/1"

Step 5 of 7: Resilience metadata - how the mechanism helps a system's resilience

(For questions, problems or feedback filling out this form, please [email us](#) )

Failure Modes

(Select the ways in which your mechanism can fail to function as intended. To help you to decide what the appropriate failure modes are you could treat your mechanism as a black box and think about the kinds of failures you expect to observe from it. The terms in this list are taken from the ReSIST ontology on security and dependability.)

(CTRL+Click to select multiple values)

Consistent Failures
Content And Timing Failure
Content Failure
Early Timing Failure
Erratic Failure
False Alarm

Threats Addressed

(Select the threats to resilience that your mechanism aims to address, ie the faults it aims to remove, the errors it aims to compensate for and the failures it aims to prevent. The terms in this list are taken from the ReSIST ontology on security and dependability.)

(CTRL+Click to select multiple values)

Accidental Fault
Budget Failure
Catastrophic Error
Catastrophic Failure
Commission Fault
Complete Development Failure

Resilience Metadata

In this question you are asked to think about the effect your mechanism has on the resilience of a system. If you were to compare your mechanism to a different mechanism addressing a similar aim, what data would you use to choose which was fit for a specific purpose? This question allows you to define such metrics and associate a value with them for your mechanism. New resilience metadata metrics and values can be added to this list by clicking on the "add new item" link. Existing metadata instances can be deleted or edited by clicking the cross or the pencil next to them respectively. Note that when you edit some metadata a new version is saved as well as the old one, which can then be deleted.)

Time-dependent probability $P(t)$ of undetected failure
POFOD (Undetected) * application software's execution
rate * t Probability  

Time-dependent probability $P(t)$ of failure POFOD *
application software's execution rate * t Probability  

Time-dependent probability $P(t)$ of detected failure  

http://resist.ecs.soton.ac.uk/gmap/resist-courses.php

http://resist.ecs.soton.ac.uk/gmap/resist-courses.php

Google



[Go to the ReSIST Partners Map](#)

Some Underlying Sources

acm.rkbexplorer.com

budapest.rkbexplorer.com

citeseer.rkbexplorer.com

cordis.rkbexplorer.com

courseware.rkbexplorer.com

darmstadt.rkbexplorer.com

dblp.rkbexplorer.com

deepblue.rkbexplorer.com

deploy.rkbexplorer.com

eurecom.rkbexplorer.com

ft.rkbexplorer.com

ibm.rkbexplorer.com

ieee.rkbexplorer.com

irit.rkbexplorer.com

italy.rkbexplorer.com

kaunas.rkbexplorer.com

kisti.rkbexplorer.com

laas.rkbexplorer.com

lisbon.rkbexplorer.com

newcastle.rkbexplorer.com

nsf.rkbexplorer.com

pisa.rkbexplorer.com

resex.rkbexplorer.com

roma.rkbexplorer.com

southampton.rkbexplorer.com

ulm.rkbexplorer.com

unlocode.rkbexplorer.com

wiki.rkbexplorer.com

Range from a few 100 to more than 10,000,000 “facts”

More Semantic Web/Linked Data issues

- The system supports state of the art facilities:
 - Browsing
 - Resolvable URIs
 - SPARQL endpoint
 - CRS (Coreferent knowledge)
 - RDF publishing
 - Semantic Sitemap
 - On a separate domain

Supporting resilience

- People, Publication, Projects, Research Areas
- Resilience-related topics
- Resilience-Explicit Computing
- Educational Resources

- In the future
 - Automating discovery of issues and solutions
 - Design time
 - Run time

Finding mechanisms that are appropriate for Hardware and Aerospace

```
SELECT DISTINCT ?mechanismURI ?mechanismName ?metadataName ?metadataValue WHERE {  
  ?mechanismURI rdf:type resex:Resilience-Mechanism .  
  ?mechanismURI resex:applies-to-technology akt:Hardware-Platform .  
  ?mechanismURI resex:has-application-domain acm:J.2.0 .  
  ?mechanismURI rdfs:label ?mechanismName .  
}
```

Result	Binding	Value
1	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-267972cd
	?mechanismName	N-Self-Checking Programming/1/1
2	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-e679bd05
	?mechanismName	N-Version Programming/1/1
3	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-7425f52f
	?mechanismName	Recovery Blocks/1/1

Inspecting metadata, number of variants

```
SELECT DISTINCT ?mechanismURI ?mechanismName ?metadataName ?metadataValue WHERE {  
  ?mechanismURI rdf:type resex:Resilience-Mechanism .  
  ?mechanismURI resex:applies-to-technology akt:Hardware-Platform .  
  ?mechanismURI resex:has-application-domain acm:J.2.0 .  
  ?mechanismURI rdfs:label ?mechanismName .  
  ?mechanismURI resex:has-resilience-metadata ?metadata .  
    ?metadata resex:metadata-type id:resilience-metadata-type-231c8583  
    ?metadata resex:metadata-type ?mt . ?mt rdfs:label ?metadataName .  
    ?metadata resex:has-value ?metadataValue  
}
```

Result	Binding	Value
1	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-7425f52f
	?mechanismName	Recovery Blocks/1/1
	?metadataName	Number of variants
	?metadataValue	2
2	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-e679bd05
	?mechanismName	N-Version Programming/1/1
	?metadataName	Number of variants
	?metadataValue	3
3	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-267972cd
	?mechanismName	N-Self-Checking Programming/1/1
	?metadataName	Number of variants
	?metadataValue	4

Inspecting metadata, average cost of implementing fault tolerant system -vs- cost of implementing non fault tolerant system

```
SELECT DISTINCT ?mechanismURI ?mechanismName ?metadataName ?metadataValue WHERE {  
  ?mechanismURI rdf:type resex:Resilience-Mechanism .  
  ?mechanismURI resex:applies-to-technology akt:Hardware-Platform .  
  ?mechanismURI resex:has-application-domain acm:J.2.0 .  
  ?mechanismURI rdfs:label ?mechanismName .  
  ?mechanismURI resex:has-resilience-metadata ?metadata .  
    ?metadata resex:metadata-type id:resilience-metadata-type-de1eddf9 .  
    ?metadata resex:metadata-type ?mt . ?mt rdfs:label ?metadataName .  
    ?metadata resex:has-value ?metadataValue  
}
```

Result	Binding	Value
1	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-e679bd05
	?mechanismName	N-Version Programming/1/1
	?metadataName	Av CFT/CNFT
	?metadataValue	2.25
2	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-267972cd
	?mechanismName	N-Self-Checking Programming/1/1
	?metadataName	Av CFT/CNFT
	?metadataValue	3.01
3	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-7425f52f
	?mechanismName	Recovery Blocks/1/1
	?metadataName	Av CFT/CNFT
	?metadataValue	1.75

Comparison of the operational overheads in determining a fault has occurred

```
SELECT DISTINCT ?mechanismURI ?mechanismName ?metadataName ?metadataValue WHERE {  
  ?mechanismURI rdf:type resex:Resilience-Mechanism .  
  ?mechanismURI resex:applies-to-technology akt:Hardware-Platform .  
  ?mechanismURI resex:has-application-domain acm:J.2.O .  
  ?mechanismURI rdfs:label ?mechanismName .  
  ?mechanismURI resex:has-resilience-metadata ?metadata .  
    ?metadata resex:metadata-type id:resilience-metadata-type-3443934c .  
    ?metadata resex:metadata-type ?mt . ?mt rdfs:label ?metadataName .  
    ?metadata resex:has-value ?metadataValue  
}
```

Result	Binding	Value
1	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-7425f52f
	?mechanismName	Recovery Blocks/1/1
	?metadataName	Errors op time overheads
	?metadataValue	One variant and acceptance test execution
2	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-267972cd
	?mechanismName	N-Self-Checking Programming/1/1
	?metadataName	Errors op time overheads
	?metadataValue	Possible result switching
3	?mechanismURI	http://resex.rkbexplorer.com/id/resilience-mechanism-e679bd05
	?mechanismName	N-Version Programming/1/1
	?metadataName	Errors op time overheads
	?metadataValue	Usually negligible

RKBExplorer.com/explorer/ – Try it!

The screenshot displays the RKBExplorer.com website interface. At the top, the URL <http://www.rkbexplorer.com/explorer/> is visible in the browser's address bar. The website header includes the ReSIST logo and navigation links: [people](#), [research areas](#), [publications](#), [projects](#), and [search](#). A secondary navigation bar contains [recently viewed](#), [reset](#), and [help](#).

The main content area features a network diagram titled "Resilience for Survivability in IST". The diagram shows a central red node connected to several peripheral nodes, including "High-density mammos disc in blue waven...", "Predictably Dependable Computing Systems", "NEXT TTA - High-Confidence Architecture ...", "Assaying Means of Design Expression f...", "Theory and applications of col...", "Basic Research on Advanced Distributed C...", "Network of Excellence in Distributed C...", "New chromate-free passivation treatments...", "Malicious- and Accidental-Fault Toleranc...", "Design of an Open Dependable Accompanying Measure System Depe...", "Dependable Systems of Systems", "The esprit network of excellence in dist...", "Time-triggered architecture", and "Design for validation". A "Maximize" button is located in the top right corner of the diagram area.

To the right of the diagram is a "Detail" panel for the selected project. It contains the following information:

- Title:** Resilience for Survivability in IST
- Other Names:** ReSIST Resilience for Survivability in IST
- Funding:** 4500000
- Project Leader:** Jean-Claude Laprie
- Leading Organisation:** Centre National de la recherche Scientifique

Below the main content area are four panels, each with a list of items and a search icon:

- People:** Jean-Claude Laprie, Aad van Moorsel, Abdelmajid Khelil, Achour Mostefaou, Adnan Noon Mian, Afraz Jaffri, Agnan de Bonneval, Alberto Pasquini.
- Research Areas:** Information processing, information systems; Development Failure; Dependability And Security Analysis; Dependability And Security Provision.
- Publications:** Revised version in Predictably dependable computing systems; ASSERT Automated proof based system and software engineering for real-time applications; Guide de la sûreté de fonctionnement.
- Projects:** Malicious- and Accidental-Fault Tolerance for Internet Applications; The esprit network of excellence in distributed computing systems architectures; Design for validation; Network of Excellence in.

At the bottom of the page, there is a footer with links: [about](#) | [news](#) | [system requirements](#) | [acknowledgements](#) | [contact](#). A small status bar at the very bottom indicates "Applet eu.resist.rkb.RKBExplorer started".

<http://eprints.ecs.soton.ac.uk/16761>