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
Conversion & Versioning

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

Ontologies, etc,
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]
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

- 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
### Course Information

**Name of the course:** Advanced seminars on Distributed Systems

**Taught at:**
- Universita degli studi di Roma, La Sapienza
- Universitat ULM
- Universite De Toulouse 1
- Universite de Rennes 1
- University of Naples
- University of Toulouse III

**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:**
- English
- Esperanto
- Estonian
- Finnish
- French
- Gaelic

**Select Author(s):**
- Roberto Baldoni
- Roberto Berald
- Roberto Bonato
- Robin Bloomfield
- Ruta Marcinkeviciene
- Sadie Creese
<table>
<thead>
<tr>
<th>Name of the resilience mechanism (A title to identify your mechanism)</th>
<th>N-Version Programming/1/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitted by</td>
<td>Zoe Andrews</td>
</tr>
<tr>
<td>Author of mechanism (Click on the &quot;add new item&quot; 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)</td>
<td>Algirdas Avizienis</td>
</tr>
<tr>
<td>Associated projects (Click on the &quot;add new item&quot; 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)</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Mechanism Objectives (Summary of the purpose of your mechanism in a sentence or two)</td>
<td>To utilise design diversity and voting in order to tolerate software faults</td>
</tr>
<tr>
<td>Detailed Description (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)</td>
<td>The information here applies to the specific variant of the mechanism NVP/1/1, described in &quot;Definition and Analysis of Hardware- and Software-Fault Tolerant Architectures&quot;. 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 &quot;The N-Version Approach to Fault-Tolerant Software&quot;.</td>
</tr>
<tr>
<td>Detailed Description Publication (If applicable (see above), click on the &quot;add</td>
<td></td>
</tr>
</tbody>
</table>

**Definition and Analysis of Hardware- and Software-Fault-Tolerant Architectures**
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.)

CONSISTENT FAILURES
CONSISTENT AND TIMING FAILURE
CONSISTENT FAILURE
EARLY TIMING FAILURE
ERRORIC FAILURE
FALSE ALARM

Threats Addressed
(Select the threats to resilience that your mechanism aims to address, i.e., 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.)

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
Budapest University of Technology and Economics

Courses taught at Budapest University of Technology and Economics, Budapest:

- Software Verification and Validation
- Management of Computing Infrastructure

Istvan Majzik
Some Underlying Sources

<table>
<thead>
<tr>
<th>acm.rkbexplorer.com</th>
<th>italy.rkbexplorer.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>budapest.rkbexplorer.com</td>
<td>kaunas.rkbexplorer.com</td>
</tr>
<tr>
<td>citeseer.rkbexplorer.com</td>
<td>kisti.rkbexplorer.com</td>
</tr>
<tr>
<td>cordis.rkbexplorer.com</td>
<td>laas.rkbexplorer.com</td>
</tr>
<tr>
<td>courseware.rkbexplorer.com</td>
<td>lisbon.rkbexplorer.com</td>
</tr>
<tr>
<td>darmstadt.rkbexplorer.com</td>
<td>newcastle.rkbexplorer.com</td>
</tr>
<tr>
<td>dblp.rkbexplorer.com</td>
<td>nsf.rkbexplorer.com</td>
</tr>
<tr>
<td>deepblue.rkbexplorer.com</td>
<td>pisa.rkbexplorer.com</td>
</tr>
<tr>
<td>deploy.rkbexplorer.com</td>
<td>resex.rkbexplorer.com</td>
</tr>
<tr>
<td>eurecom.rkbexplorer.com</td>
<td>roma.rkbexplorer.com</td>
</tr>
<tr>
<td>ft.rkbexplorer.com</td>
<td>southampton.rkbexplorer.com</td>
</tr>
<tr>
<td>ibm.rkbexplorer.com</td>
<td>ulm.rkbexplorer.com</td>
</tr>
<tr>
<td>ieee.rkbexplorer.com</td>
<td>unlocode.rkbexplorer.com</td>
</tr>
<tr>
<td>irit.rkbexplorer.com</td>
<td>wiki.rkbexplorer.com</td>
</tr>
</tbody>
</table>

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:has-application-domain acm:J.2.0 .
  ?mechanismURI rdfs:label ?mechanismName .
}
Inspecting metadata, number of variants

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

<table>
<thead>
<tr>
<th>Result</th>
<th>Binding</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rkbexplorer.com/id/resilience-mechanism-7425f52f">http://resex.rkbexplorer.com/id/resilience-mechanism-7425f52f</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>Recovery Blocks/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Number of variants</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rkbexplorer.com/id/resilience-mechanism-e679bd05">http://resex.rkbexplorer.com/id/resilience-mechanism-e679bd05</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>N-Version Programming/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Number of variants</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rkbexplorer.com/id/resilience-mechanism-267972cd">http://resex.rkbexplorer.com/id/resilience-mechanism-267972cd</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>N-Self-Checking Programming/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Number of variants</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>4</td>
</tr>
</tbody>
</table>
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:has-application-domain acm:J.2.0 .
  ?mechanismURI rdfs:label ?mechanismName .
    ?metadata resex:has-value ?metadataValue
}
```

<table>
<thead>
<tr>
<th>Result</th>
<th>Binding</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rxbexplorer.com/id/resilience-mechanism-e679bd05">http://resex.rxbexplorer.com/id/resilience-mechanism-e679bd05</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>N-Version Programming/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Av CFT/CNFT</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>2.25</td>
</tr>
<tr>
<td>2</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rxbexplorer.com/id/resilience-mechanism-267972cd">http://resex.rxbexplorer.com/id/resilience-mechanism-267972cd</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>N-Self-Checking Programming/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Av CFT/CNFT</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>3.01</td>
</tr>
<tr>
<td>3</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rxbexplorer.com/id/resilience-mechanism-7425f521">http://resex.rxbexplorer.com/id/resilience-mechanism-7425f521</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>Recovery Blocks/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Av CFT/CNFT</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>1.75</td>
</tr>
</tbody>
</table>
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:has-application-domain acm:J.2.0 .
?mechanismURI rdfs:label ?mechanismName .
  ?metadata resex:metadata-type id:resilience-metadata-type-3443934c .
  ?metadata resex:has-value ?metadataValue
}

<table>
<thead>
<tr>
<th>Result</th>
<th>Binding</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rkbexplorer.com/d/resilience-mechanism-7426f52f">http://resex.rkbexplorer.com/d/resilience-mechanism-7426f52f</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>Recovery Blocks/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Errors op time overheads</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>One variant and acceptance test execution</td>
</tr>
<tr>
<td>2</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rkbexplorer.com/d/resilience-mechanism-267972cd">http://resex.rkbexplorer.com/d/resilience-mechanism-267972cd</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>N-Self-Checking Programming/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Errors op time overheads</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>Possible result switching</td>
</tr>
<tr>
<td>3</td>
<td>?mechanismURI</td>
<td><a href="http://resex.rkbexplorer.com/d/resilience-mechanism-e679bd05">http://resex.rkbexplorer.com/d/resilience-mechanism-e679bd05</a></td>
</tr>
<tr>
<td></td>
<td>?mechanismName</td>
<td>N-Version Programming/1/1</td>
</tr>
<tr>
<td></td>
<td>?metadataName</td>
<td>Errors op time overheads</td>
</tr>
<tr>
<td></td>
<td>?metadataValue</td>
<td>Usually negligibie</td>
</tr>
</tbody>
</table>
http://eprints.ecs.soton.ac.uk/16761