Diversity: Directions for research

presented by Lorenzo Strigini

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


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
Outline

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

Laudata sii, Diversità 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:

<table>
<thead>
<tr>
<th>from</th>
<th>towards</th>
</tr>
</thead>
<tbody>
<tr>
<td>small-scale diversity</td>
<td>large-scale diversity</td>
</tr>
<tr>
<td>dealing with unintended faults</td>
<td>dealing with malice as well</td>
</tr>
<tr>
<td>systems made of hardware and software</td>
<td>systems including people</td>
</tr>
<tr>
<td>closely controlled (&quot;designed&quot;) diversity</td>
<td>more &quot;spontaneous&quot; diversity</td>
</tr>
</tbody>
</table>
The landscape of open problems

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