Self-healing systems – What are they?

Tiina Niklander
Seminar introduction, 2007
Earlier version: AMICT, Aug 2006

Overview

SELF-MANAGEMENT

SELF-CONFIGURING  SELF-ADAPTIVE
SELF-OPTIMIZING  SELF-PROTECTING
SELF-HEALING  SELF-ORGANIZING

Autonomic Computing Initiative by IBM, 2001

Self-* (selfware)

• Self-configuring
• Self-healing
• Self-optimising
• Self-protecting
• Self-aware
• Self-monitor
• Self-adjust
• Self-adaptive

• Self-governing
• Self-managed
• Self-controlling
• Self-repairing
• Self-organising
• Self-evolving
• Self-reconfiguration
• Self-maintenance

Eight Goals for a System

1. System must know itself
2. System must be able to reconfigure itself within its operational environment
3. System must preemptively optimise itself
4. System must detect and respond to its own faults as they develop
5. System must detect and respond to intrusions and attacks
6. System must know its context of use
7. System must live in an open world
8. System must actively shrink the gap between user/business goals and IT solutions

Autonomic Computing

• Basic model: closed control loops
  – Based on Process Control Theory
• Controller continuously compares the actual and expected behavior and makes needed adjustments

SEE: Any control-theory books
Autonomic Control Loop

**Analyze**
- Collect, combine, find trends, correlations
  - From system elements, users, environment, agents, ...

**Act**
- Modify behavior, inform users

**Decide**
- Use uncertain reasoning, policies, rules, ...

Elements of Self-Healing 1/2

<table>
<thead>
<tr>
<th>Fault model</th>
<th>Fault duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fault manifestation</td>
</tr>
<tr>
<td></td>
<td>Fault source</td>
</tr>
<tr>
<td></td>
<td>Granularity</td>
</tr>
<tr>
<td></td>
<td>Fault profile expectations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault Detection</td>
</tr>
<tr>
<td>Degradation</td>
</tr>
<tr>
<td>Fault response</td>
</tr>
<tr>
<td>Fault recovery</td>
</tr>
<tr>
<td>Time constants</td>
</tr>
<tr>
<td>Assurance</td>
</tr>
</tbody>
</table>

Fault models

- Each aspect describes a characteristic of the fault.
  - Duration: Is the fault permanent?
  - Manifestation: What does the fault do to the system?
  - Source: Where does the fault come from?
  - Granularity: Is the fault global or local?
  - Occurrence expectation: How often will the fault occur?

System Response

- Each aspect describes a characteristic of reacting to faults.
  - Detection: How does a system detect faults?
  - Degradation: Will the system tolerate running in a degraded state?
  - Response: What does a system do when the fault occurs?
  - Recovery: Once a fault occurs, can the system return to a healthy state?
  - Time: How much time does the system have to respond to a fault?
  - Assurance: What assurances does a system have to maintain while handling a fault?

Elements of Self-Healing 2/2

<table>
<thead>
<tr>
<th>System completeness</th>
<th>Architectural completeness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System self-knowledge</td>
</tr>
<tr>
<td></td>
<td>System evolution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design context</th>
<th>Abstraction level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Component homogeneity</td>
</tr>
<tr>
<td></td>
<td>Behavioral predetermined</td>
</tr>
<tr>
<td></td>
<td>User involvement in healing</td>
</tr>
<tr>
<td></td>
<td>System linearity</td>
</tr>
<tr>
<td></td>
<td>System scope</td>
</tr>
</tbody>
</table>

System Completeness

- Each aspect describes how system implementation affects self-healing.
  - Architecture completeness: How does the system deal with incomplete and unknown parts?
  - Designer knowledge: How do developers deal with unavoidable abstractions?
  - System self-knowledge: What does the system need to know about its components perform self-healing?
  - System evolution: How does the system cope with changing components and environments?
Design Context

- Each aspect describes how system design affects self-healing.
  - Abstraction level: What abstraction level performs self-healing?
  - Component homogeneity: Are the system’s distributed components homogeneous?
  - Behavioral predetermination: Is the system non-deterministic?
  - User involvement: Does a user do some of the healing?
  - System linearity: Is the system constructed out of composable components?
  - System scope: Does the size of the system affect self-healing possibilities?

Alternative taxonomy

- Maintenance of health
  - Redundancy, probing, ADL, component relation and regularities, diversity, log-analysis
- Detection of failure, discovery of non-self
  - Missing, monitoring model, notification of aliens
- System recovery back to healthy state
  - Redundancy, repair strategies, repair plan, self-assembly, recovery-oriented computing, replication, gauges, event-based action.


Size of the self-healing unit?

- Component
  - Focus on connectors and component discovery
- Service
  - Service interfaces, Service discovery, restart
- Node
  - Network and interface failures, change to new connection

Architectural approach

- The healing or recovery part often requires reconfiguration and adaptation
- They change the architecture
  - Locate and use alternative component
  - Restart (or rejuvenation or resurrection) the failed component
- Self-healing can be build on reflective middleware

Experiments

- OSAD – model (On-demand Service Assembly and Delivery)
- MARKS – Middleware Adaptability for Resource discovery, Knowledge usability and Self-healing
- PAC – Autonomic Computing in Personal Computing Environment
- Using self-healing components and connectors

Life-cycle of Self-Healing

- OSAD – On-demand Service Assembly and Delivery
- Prototype in JINI environment
- Looking for alternatives only by name

Figure 1. The lifecycle of self-healing behaviour in OSAD model.
MARKS

- Middleware Adaptability for Resource Discovery, Knowledge Usability and Self-healing
- Marks is targeted at embedded and pervasive, small mobile handheld devices.
- New Services: Context, Knowledge Usability and Self-Healing
- Prototype: Dell Axim 30 pocket PC & .NET

Self-healing in MARKS

- Healing manager (of the network) to handle all fault types
  - To isolate faulty device (Fault containment)
  - Select surrogate device or share load among working members
- Resource manager used as repository of information for backup purposes
- Self-healing unit (on each device)
  - One process named rate of change of status
  - For monitoring the device and announcing the conditions

Self-healing component

- For healing:
  - Self-Healing controller
  - Component monitor
  - Reconfiguration manager
  - Repair manager
Reconfiguration decision

- Anomaly detection:
  - Compare observed and expected behavior
- Isolate the 'faulty' object
- Repair or replace the faulty object (and return back to normal operation)

PAC – Personal Autonomic Computing

- Goal: collaboration among personal systems to take a shared responsibility for self-awareness and environment awareness
- Proof of concept: self-healing tool utilizing pulse monitor (heart beat)


PAC

- Autonomic manager
  - Self-adjuster
  - Self-monitor
  - Internal-monitor
  - External-monitor
  - Pulse-monitor (and generator)

Fig. 2. Architecture of a PAC Alarms.

Conclusions

- Self-healing has three roots:
  - Autonomic and self-management world
  - Distributed systems world (especially middleware)
  - Dependable and fault-tolerance world
- The failure recognition and repair decisions might be faster if autonomic
- However: effects of incorrect decisions can be large (and correct them time consuming)

References

- Philip Koopman: Elements of the Self-Healing System Problem Space. In Proceedings of ICSE WADS 03
Additional material


7. IBM Director software rejuvenation. – white paper

Schedule (conference simulation)

- 1. period: Writing the paper
  - 2. meeting: List of references, refinement of the topic
  - 3. meeting: Table of content
  - 4. meeting: draft (to show to Tiina)
  - 5. meeting: Paper ready for review
  - 6. meeting: Review feedback (from two members)
  - Paper ready and submitted before second period

- 2. period: Presentations

Seminar topics for Spring 2007

- Faults / Recovery / Autonomic computing
- Self-adaptive services
- Configuration-level adaptation
- Self-healing architectures
  - Agent-based
  - Components
  - Middleware
- Performance issues
  - Self-optimisation etc.

- Detection and monitoring
- Instrumentation
- Diagnosis (intelligent systems area)
- Repair
  - Dynamic updates
  - Hot-swap & reconfiguration (software/hardware)
  - Remote healing
- Network related
  - Survivable networks
  - Sensor networks
- Software analysis / design for healing