IPA/SEC's Efforts for Dependable Software

September 9, 2013

Yuzo Nakamura
Software Reliability Enhancement Center (SEC)
Information-technology Promotion Agency (IPA), Japan
Changes in SEC's High Priority Goals

<table>
<thead>
<tr>
<th>First Phase</th>
<th>Second Phase</th>
<th>Third Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>'04</td>
<td>'07</td>
<td>'13</td>
</tr>
<tr>
<td>...</td>
<td>'08</td>
<td>'14</td>
</tr>
<tr>
<td></td>
<td>'09</td>
<td>'15</td>
</tr>
<tr>
<td></td>
<td>'10</td>
<td>'16</td>
</tr>
<tr>
<td></td>
<td>'11</td>
<td>'17</td>
</tr>
<tr>
<td></td>
<td>'12</td>
<td></td>
</tr>
</tbody>
</table>

(Third Phase Plan)

Improvement of Software Reliability

Improvement of Software Development Capability

Vendors

Small and Medium-sized User Companies

Users (General Public)
Major Infrastructure Service Providers
Efforts for Reliable Enterprise Software

GQM+Strategies®

"How to Ensure the required quality through participation of management"

"Guide to deal with Change of Environments"

"Common frame 2013"

"High-Resilience System Infrastructure Introduction Guide"

"Non-Functional Requirements Grade"

"Functional Requirements Consensus Building Guide"

<CoBRA estimate tool> development and release

"Process Improvement Navigation Guide" series

"Visualization of IT projects" series

"Recommendation for Qualitative Quality Prediction, Continued"

*GQM+Strategies® is a registered trademark of the Fraunhofer Institute for Experimental Software Engineering, Germany and the Fraunhofer USA Center for Experimental Software Engineering, Maryland.

Software Reliability Enhancement Center

Efforts for Reliable Embedded Software

ESMR (Project management guide)

Management process guidebooks

Engineering process guidebooks
Efforts for Reliable Integrated Software

Enhancement of Quality Explanation Capabilities
Guideline for implementing software quality explanation scheme

Enhancement of Upstream Process
Rigorous specification descriptions with formal methods, Promotion of MBSE, etc.

Different kinds of systems are connected
Integrated Software
Diversified use forms, Unexpected uses
Fast propagation of failures, more serious failures

Enhancement of Organizational Efforts
Survey on failures that occurred in other countries,
Survey on the software industry in Japan, etc.

Efforts for Reliable Embedded Software

Efforts for Reliable Enterprise Software
Efforts for Dependable Software

- **Environmental Changes**: Society is becoming ever more reliant on software reliability
  - Further enhancements of increasingly complex products/systems
  - These products/systems are interconnected and serve as part of a larger social infrastructure
  - An increase in the role (importance) of software for society

- **Efforts in Third Phase Plan**
  - **Concept**
    - In addition to the existing activities targeted at development vendors, we will expand these activities to general users, and the major infrastructure service providers who have a significant influence on them.
  - **Third Phase Plan**: Promotion of efforts for the improvement of reliability in information processing systems that support society - particularly in major infrastructure areas -
    - Measuring of information system failures in the field of critical infrastructure
    - Visualization of software reliability from a user's viewpoint
Software Reliability from a User's Viewpoint

Software Characteristics
With reference to software intensive products/systems:

- Software is intangible, users are not usually aware of its presence.
- Once a failure or accident occurs, users will have serious doubts about the future reliability of the software. It is very difficult to remedy the users' doubts after the fact.

Importance of the Software Quality Explanation

- Quality must be explained objectively. For example, the following must be covered:
  - Intended users, purpose, utilization situations, constraints
  - Quality and quality goals of the software required for its use
  - Design, implementation, operation and maintenance required to achieve the quality goals
  - Verification to demonstrate the achievement of the quality goals
- In addition, by having a third party expert to evaluate the quality explanation, we will be able to understand the explanation objectively.

* Although evaluation by the expert will be focused on the software, other areas will also be evaluated.
Development of Guideline for Scheme Implementation

- The necessity of a "Guideline for Implementing Software Quality Explanation Scheme"
  - Implementation of a scheme in which a third party expert evaluates the quality of software intensive products/systems, and the results of the evaluation are presented to the users.
  - Because the required quality level, evaluation methods, etc. vary depending on the product/system area, the scheme must be implementable for each area.
  ⇒ SEC developed a guideline for implementing this scheme which should be applied for each area

- Guideline Provisions
  - Securing fairness (for fair management of the scheme)
    - Securing independence between the third party evaluating products/systems, and their suppliers
    - Review of the scheme by external parties who are not involved within the scheme
  - Securing integrity (integrity of the scheme implemented for each area)
    - Scheme requirements that are not dependent on the relevant products/systems (organizations, responsibility, operations, information management, release, etc.)
    - Development of review criteria covering the relevant quality requirements and technologies for each area
Introduction of Bugs in the Upstream Process
- Problems caused by vague specifications or an ambiguous design, etc.

Realization of the "Rigorous Specification Description" based on formal methods
- A formal description removes ambiguity, enables machine processing and creates further possibilities
- A description and verification of rigorous specifications becomes possible by using formal specification description language and tools. In addition, the introduction of formal methods contributes to the promotion of communication among stakeholders during system development

Source: "A survey on the software industry" issued by IPA
 Dependability Assurance Framework For SSCD

■ Safety-Sensitive Consumer Devices (SSCD)
  - Industrial products such as automobiles, service robots, medical devices, clinical systems, and smart houses used by general consumers

■ Characteristics of SSCD
  - Open, dynamic, used in a diversified manner and requires a high level of dependability
  - They are becoming more sophisticated and complex

<table>
<thead>
<tr>
<th></th>
<th>Factory machineries</th>
<th>SSCD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number produced</td>
<td>Moderate numbers</td>
<td>Huge numbers</td>
</tr>
<tr>
<td>Users</td>
<td>Experts</td>
<td>General users</td>
</tr>
<tr>
<td>Cost</td>
<td>High</td>
<td>Low to moderate</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Rigorous, Strongly managed</td>
<td>By Users &amp; Service stations (weakly managed)</td>
</tr>
<tr>
<td>Environment</td>
<td>Factory environment (stable, controlled)</td>
<td>User environment (Open, dynamic and diverse)</td>
</tr>
</tbody>
</table>
Dependability Assurance Framework For SSCD

- Awareness of existing standards (e.g. functional safety)
  - SSCD must not only be safe, but also endure continued use (=dependability).
  - To support an environment of diverse users, a **process of quickly and repeatedly verifying control software**, while using systems engineering and model-based development, is required so that all use-cases of all users can be covered.

⇒ By standardizing these processes and simultaneously implementing various tools based on a common methodology, the costs for manufacturing dependable SSCD should be reduced.

- To achieve the above, we propose a **Dependability Assurance Framework (DAF)** for securing dependability. The components of DAF are 1. to 3.
  1. **Dependability Conceptual Models (DCMs)** define the factors of dependability
  2. Templates to be used to construct **Dependability Assurance Cases (DACs)** for SSCDs
  3. **Dependability Process Models (DPMs)** define rapid and iterative processes for engineering dependable SSCDs

IPA/SEC's Efforts for Dependable Software

Thanks For Listening

Contact Information

Yuzo Nakamura
Email: yu-naka@ipa.go.jp

Customer Relations
Email: sec-pr@ipa.go.jp

Web: https://www.ipa.go.jp/ (Japanese)
Web: https://www.ipa.go.jp/index-e.html (English)

Software Reliability Enhancement Center (SEC)
Information-technology Promotion Agency (IPA), Japan