Modeling of Risk Assessment for Service Robots

Safety Intelligence Research Group (SIRG),
National Institute of Advanced Industrial Science and Technology (AIST)

Yoshihiro Nakabo
Contents

• Objective: Safe Robots
• International safety standards (ISO/IEC)
• Proposal
  – Object oriented approach to robot safety
  – Models for risk identification
  – Model for overall risk assessment
• Conclusion
Next generation service robots

• For Business: Cleaning, Welfare, Security, Guidance
• Home: House keeping, Hobby, Security

• Service robot
  = close proximity with human
  -> Safety issue should be clarified
Next generation industrial robots

• Power assisting robot: already used in some motor companies
• Next generation cell production robots
Safety of next generation robots

• Socially accepted safety technology required (unless almost zero risk for unknown new products)

• Previously:
  – Industrial robots -> separation of human and robots
  – Service robots -> no fundamental principles

• Recently:
  – “Collaborative operation” included in International Standard for safety of industrial robots (ISO10218)
  – New ISO standardization in progress for service robots
  – “Safety guidelines for next-generation robots” in Japan
ISO/IEC Guide 51 determines hierarchical structure

**type-A standards (basic safety standards)**
- ISO 12100: Safety of machinery — Basic concepts, general principles for design —
- ISO 14121: Safety of machinery — Risk assessment —

**type-B standards (generic safety standards)**
- ISO 13849: System safety
- ISO 13855: Safety distances
- IEC 61508: Functional safety
- IEC 61496: Safety sensors

**type-C standards (machine safety standards)**
- Machine tools, Chemical plants, Electric lifts
- Industrial robots, Earth-moving machinery, Press machine
ISO12100 Safety of Machinery

- **Safety:** freedom from unacceptable risk
- **Risk:** combination of the probability of the occurrence of harm and the severity of that harm
- **Harm:** physical injury or damage to the health of people, or property or the environment

(from ISO12100)
ISO12100 Safety of Machinery

- Communication with users

- Protective measures taken by the 
  user,
  including those based on the 
  information for use provided by the designer

- Organization
  - safe working procedures
  - supervision
  - permit-to-work systems

- Provision and use of additional safeguards

- Use of personal protective equipment

- Training, etc.

Residual risk after all protective measures have been taken

from ISO12100
ISO 14121 Risk Assessment

• Risk assessment:
Systematic analysis and evaluation of the risks associated with machinery.

• Should be executed by safety assessors, robot designers and engineers

• Details are explained latter…
IEC 61508 Functional Safety

- The V Model: software safety integrity and the development lifecycle

from IEC61508-3
Example of recommended technologies

- Depends on SIL (Safety Integrity Level)
- Validation for safety requirements

Example:

<table>
<thead>
<tr>
<th>Technique/Measure</th>
<th>Ref.</th>
<th>SIL1</th>
<th>SIL2</th>
<th>SIL3</th>
<th>SIL4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Computer-aided specification tools</td>
<td>B.2.4</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>2a Semi-formal methods</td>
<td>Table B.7</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>2b Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z</td>
<td>C.2.4</td>
<td>---</td>
<td>R</td>
<td>R</td>
<td>HR</td>
</tr>
</tbody>
</table>

NOTE 1 - The software safety requirements specification will always require a description of the problem in natural language and any necessary mathematical notation that reflects the application.

NOTE 2 - The table reflects additional requirements for specifying the software safety requirements clearly and precisely.

* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.

from IEC61508-3
Problems

• Many individual processes and large amount of documentation
• Frequent communication between users, designers and safety assessors
• Waterfall instead of Agile

• Could be solved by modeling and CAD related tool assistance
Proposal

• Object Oriented modeling for robot safety
  – Definitions of safety, risk and other terms
  – Include processes for risk assessment, risk reduction and evaluation
  – Construct framework through UML profiling

• Accelerate development of safe service robots
• Change process from waterfall to agile
Risk reduction process

Concepts for safety of machinery:

- No zero risk
- Start from risk assessment (determining requirements)
- Three step risk reduction
- Judge residue risk
- Safeguards = Functional safety

Risk assessment

Is residue risk acceptable?

No

Risk reduction

Step 1. Intrinsic safety

Step 2. Safe guard

Step 3. Information for use

Yes
Risk assessment process

1. Determination of the limits of the machinery
2. Hazard identification
3. Risk estimation
4. Risk evaluation
5. Is residue risk acceptable?
   - Yes
   - No
   - Risk reduction

Risk analysis

Risk assessment
Limits of machinery

Consideration of necessary phases and tasks
Extraction of those concerned with each phase or task

Operation manual

Consideration of definition of object operation

Use case diagram

Study operation scenario

Activity diagram

Detailed design document

Study the structural model of machine

Class diagram of machine

Create scenario (activity diagram) for each use case
Example of hazards

<table>
<thead>
<tr>
<th>Type of group</th>
<th>Examples of hazards</th>
<th>Potential consequences</th>
</tr>
</thead>
</table>
| Mechanical hazards  | - Acceleration, deceleration (kinetic energy)  
                    | - Angular parts      |
|                     | - Approach of a moving element to a fixed parts|
|                     | - Cutting parts     |
|                     | - Falling objects   |
| Electrical hazards  | - Arc               |
|                     |                     | - Burn                |

- Example of hazards listed in ISO 14121
- Any combination of origin and potential consequences should be considered
- Hazards classified by group type
Example of typical hazards

- Subset of the hazard table

from ISO14121
• UML diagram can be used for modeling ISO hazard description (includes humans and environment as elements of risk)
Example of hazardous situations

- All phases of machine life cycle should be taken into account
- Each phase consists of separate tasks

Listed life cycle:
- Transport
- Assembly and installation, Commissioning
- Setup, Teaching/programming and/or process changeover
- Operation
- Cleaning, Maintenance
- Fault finding/Troubleshooting
- Decommissioning, Dismantling

<table>
<thead>
<tr>
<th>Phase of machine life cycle</th>
<th>Examples of tasks</th>
</tr>
</thead>
</table>
| Transport                   | - Lifting  
  - Loading  
  - Packing  
  - Transportation           |
| Assembly and installation   | - Adjustments of the machine and its components  
  - Assembly of the machine  |
| Commissioning               |                                                        |
| Setting                      | - Adjustment and setting of protective device and other components |
| Teaching/programming and/or process changeover |                                                        |
Hazard identification by:

- Extracting risks from activity diagrams and class diagram of object machine
- Considering potential consequences and origin of hazards

Process to be continued until all risks identified
Rest of Processes in Risk Assessment

• Risk estimation (quantitative analysis)
  – Severity of harm
  – Probability of occurrence
    • Exposure of person to the hazards
    • Occurrence of hazardous events
    • Possibility of avoiding or limiting the harm
• Risk evaluation (if the risk has been adequately reduced)
• Documentation
UML model of risk assessment

- Listed in ISO 14121
- UML diagrams
- Outside scope of presentation

Documents ➔ Risk assessment process ➔ Lifecycle ➔ Use case diagram ➔ Actor ➔ Activity diagram

Risk assessment process ➔ Use case diagram ➔ Actor ➔ Activity diagram

Origin of hazards ➔ Risk assessment data ➔ Risk estimation basis

Machinery (Class diagram) ➔ Tasks ➔ Hazardous parts of machinery ➔ Hazardous situations in tasks ➔ Potential consequence

Risk estimation basis:
- Red class
- Yellow class
- Green class

Risk assessment data:
- Occurrence
- Exposure
- Severity
- Possibility of avoidance

Risk assessment process:
- Risk estimation basis
Conclusion

• Proposed an object oriented modeling of ISO based risk assessment
• All processes and safety related concepts can be modeled by using UML models
• Standardization of proposed UML should be useful for the propagation of known safety principles, development of CAD-based risk assessment and design of safety related robot modules
• Future work will be focused on developing UML profile, implementing risk estimation and evaluation