MODEL-BASED RISK ANALYSIS OF HUMAN-ROBOT INTERACTIONS AND SAFETY ARGUMENT CONSTRUCTION

Quynh Anh DO HOANG
Jérémie GUIOCHET
Mohamed KAÂNICHE
David POWELL

qdohoang@laas.fr

Model-based Safety Assessment Workshop
ISAE Campus de Rangueil – Toulouse March 15,16 2011
Summary

• Human-robot interaction: MIRAS project
• Model-based risk analysis: HAZOP-UML
• Safety argument construction using GSN
A Rehabilitation Robot: The MIRAS Robot
The MIRAS project:
A robotic strolling assistance

• GOAL
  • Assists patient in standing up, walking and sitting down
  • For people suffering from gait and orientation problems

• MEANS
  • Motorised base and moving handlebar
  • Sensors to detect patient’s position and health condition

MIRAS: Multimodal Interactive Robot for Assistance in Strolling
Building a safe system...

• Building a zero-risk system...
  • Totally correct specification
    • All hazardous situations predicted
    • All hazardous situations correctly handled
  • Totally correct design and implementation

• ... is actually impossible
  • Justified confidence that the specification covers the most hazardous situations
  • Justified confidence that the design includes adequate protection techniques
  • Justified confidence that the system is correctly implemented
Building a safe system…

- **Safety**: absence of unacceptable risk [ISO-Guide51]

- **Risk management**: systematic application of management policies, procedures and practices to the task of analysing, evaluating, controlling and monitoring risk [ISO 14971]
Risk management process

- ISO/IEC Guides 51 &73
- ISO/FDIS 14971
Risk management process

Argumentation process

- **Safety case**: A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment. [1]


Systematic model-based approach
Model-based risk assessment

- Adapt the classical risk management process by using **UML** (Unified Modelling Language) to model the system, including the user

- **Why UML?**
  - *De facto* standard
  - Use case, sequence diagram and statechart are easily understandable by non-experts (transdisciplinary models)
  - Diagrams can also be used for development process
  - Models include the user
Unified Modeling Language

- **Use cases**
  - Describe the intended use of the robot
  - Completed with conditions
Unified Modeling Language

- **Sequence diagrams**
  - Describe nominal scenarios corresponding to the use cases
  - Messages are either actions (self-messages) or interactions
Unified Modeling Language

- **Statechart**
  - Describe different system’s state
  - Completed with conditions
UML Models

HAZOP Guidewords

<table>
<thead>
<tr>
<th>Guideword</th>
<th>Signification</th>
</tr>
</thead>
<tbody>
<tr>
<td>No / None</td>
<td>Complete negation of the design</td>
</tr>
<tr>
<td>More than</td>
<td>Quantitative increase</td>
</tr>
<tr>
<td>Less than</td>
<td>Quantitative decrease</td>
</tr>
<tr>
<td>As well as</td>
<td>All the design intention is achieved together with additions</td>
</tr>
<tr>
<td>Part of</td>
<td>Only some of the design intention is achieved</td>
</tr>
<tr>
<td>Reverse</td>
<td>The logical opposite of the design intention is achieved</td>
</tr>
<tr>
<td>Other than</td>
<td>Complete substitution</td>
</tr>
<tr>
<td>Attribute</td>
<td>Guideword</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Predecessors / successors during interaction</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Other than</td>
</tr>
<tr>
<td></td>
<td>As well as</td>
</tr>
<tr>
<td></td>
<td>More than</td>
</tr>
<tr>
<td></td>
<td>Less than</td>
</tr>
<tr>
<td></td>
<td>Before</td>
</tr>
<tr>
<td></td>
<td>After</td>
</tr>
<tr>
<td></td>
<td>Part of</td>
</tr>
<tr>
<td></td>
<td>Reverse</td>
</tr>
<tr>
<td>Message timing</td>
<td>As well as</td>
</tr>
<tr>
<td></td>
<td>Early</td>
</tr>
<tr>
<td></td>
<td>Later</td>
</tr>
<tr>
<td>Sender / receiver objects</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Other than</td>
</tr>
<tr>
<td></td>
<td>As well as</td>
</tr>
<tr>
<td></td>
<td>Reverse</td>
</tr>
<tr>
<td></td>
<td>More</td>
</tr>
<tr>
<td></td>
<td>Less</td>
</tr>
</tbody>
</table>

**Entity = Sequence Diagram**

```
1: Catch handles
2: Starts standing up

2.1: Detection and activation of standing up mode

loop
1: Patient is standing up

2: Standing up course monitoring

2.2: Detection of the end of standing up

2.3: Switch to strolling mode
```
### Example of HAZOP-UML application

<table>
<thead>
<tr>
<th>Project: PHRIENDS</th>
<th>Date: June-01-2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAZOP number: UC4/SD4</td>
<td>Prepared by: Ofaina Taofifena</td>
</tr>
<tr>
<td>Entity: Sequence Diagram 4 (sd4) “Take an object from the user's hand”</td>
<td>Revised by: Jérémie Guiochet</td>
</tr>
<tr>
<td></td>
<td>Approved by:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Element (attribute)</th>
<th>Guide word</th>
<th>Deviation</th>
<th>a. Use Case Effect</th>
<th>Severity</th>
<th>b. Real World Effect</th>
<th>Possible Causes</th>
<th>Integrity level Requirements</th>
<th>New Safety Requirements</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive and interpret order (pred/succ)</td>
<td>More than / as well as</td>
<td>The robot receives several different orders</td>
<td>a. Wrong order taken into account</td>
<td>Moderate</td>
<td>b. Wrong task, bad synchronization between robot and user, could result in collision</td>
<td>Failure of H/W for order reception</td>
<td>H/W for order reception should be SIL1</td>
<td>User education and training</td>
<td>Means for communication between robot and user needs to be defined for the PHRIENDS use case (speech, graphical HMI, vision, etc.)</td>
</tr>
<tr>
<td>Put the object in the gripper (pred/succ)</td>
<td>Before</td>
<td>Since the gripper is open the user can give the object to the robot before the latter is ready</td>
<td>a. Bad synchronization between user and robot can cause collision</td>
<td>Severe</td>
<td>b. The object can fall / The arm and human can collide</td>
<td>Human error</td>
<td>None</td>
<td>The robot should keep the gripper closed until the arm movement is finished</td>
<td>The procedure in the seq. diag. is as follows: the robot opens its gripper then the robot arm moves towards the user hand. Only then the user can place the object in the robot gripper. A safer procedure is: the robot should keep the gripper closed until arm movement is finished -&gt; modify sequence diagram</td>
</tr>
</tbody>
</table>
Results in the MIRAS project

• First iteration of the process
  • 11 use cases, 12 sequence diagrams
  • 297 interpreted deviations
  • 13 hazards identified
  • 29 recommendations for design modifications
  ➔ New specification and design of the robot

• Second iteration of the process on the new UML model
  • 1 modified use case, 4 new use cases, 4 new sequence diagrams
  • 215 interpreted deviations
  • 1 new hazard identified
  • 28 new recommendations for design modifications
## Hazard list

<table>
<thead>
<tr>
<th>HN</th>
<th>Description</th>
<th>PHA</th>
<th>Use Case Diagram</th>
<th>Sequence Diagram</th>
<th>Statechart</th>
</tr>
</thead>
<tbody>
<tr>
<td>HN1</td>
<td>Incorrect posture of patient during movement</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>HN2</td>
<td>Patient fall during robot use</td>
<td>29</td>
<td>27</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>HN3</td>
<td>Robot shutdown during use : patient is not assisted</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>HN4</td>
<td>Patient fall without alarm or with a late alarm</td>
<td>11</td>
<td>13</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>HN5</td>
<td>Physiological problem of the patient without alarm or with a late alarm</td>
<td>15</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HN6</td>
<td>Patient fall caused by the robot</td>
<td>10</td>
<td>51</td>
<td>37</td>
<td>10</td>
</tr>
<tr>
<td>HN7</td>
<td>Failure to switch to safe mode when a problem is detected, the robot keeps moving</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HN8</td>
<td>Robot parts catching patient or clothes</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>HN9</td>
<td>Collision between the robot (or robot part) and the patient</td>
<td>2</td>
<td>14</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>HN10</td>
<td>Collision between the robot and a person other than the patient</td>
<td>5</td>
<td>14</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>HN11</td>
<td>Disturbance of medical staff during an intervention</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HN12</td>
<td>Patient loses her balance</td>
<td>11</td>
<td>1</td>
<td>70</td>
<td>1</td>
</tr>
<tr>
<td>HN13</td>
<td>Patient fatigue</td>
<td>12</td>
<td>1</td>
<td>53</td>
<td>21</td>
</tr>
<tr>
<td>HN14</td>
<td>Patient injury caused by sudden movements of robot while carrying the patient</td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
Safety case construction using GSN

- **Goal Structuring Notation**
  - A graphical notation developed at University of York
  - Mostly used in safety cases

- **Argument elements**
  - Requirement
  - Claim
  - Evidence
  - Context
Goal Structuring Notation

"To show how goals are broken down into sub-goals, and eventually supported by evidence (solutions) whilst making clear the strategies adopted, the rationale for the approach (assumptions, justifications) and the context in which goals are stated." [2]

Application to MIRAS

Goal1
The MIRAS robot is at least as safe as a classical rollator

Context1
The robot follows these standards:
- EU Machinery Directive 98/37/EC
- EN ISO 11199-2:2005 (Part 2: Rollators)
- International Standard ISO/IEC 60601-1,2,4,6,8
- EN ISO 14971:2007 Medical Devices — Application Of Risk Management To Medical Devices

Context2
New hazards found in robotic rollator use:
- HN6 : patient falls caused by the robot
- HN9/HN10 : collision between the robot (or robot part) and a person
- HN8 : robot parts catching patient or clothes
- HN1a : incorrect posture of patient during movement (due to robot)
- HN3 : robot shutdown during use: patient is not assisted
- HN7: failure to switch to safe mode when a problem is detected, the robot keeps moving
- HN11 : disturbance of medical staff during an intervention

Context3
Risk assessment is performed on robot without seat

Strategy1
New risks induced by robotic rollator are correctly mitigated

Strategy2
Risks induced by classical rollator use are either correctly mitigated or not increased

Context4
Hazards found in classical rollator use:
- HN4 : patient fall without alarm or with a late alarm
- HN5 : physiological problem of the patient without alarm or with a late alarm
- HN1b : incorrect posture of patient during movement
- HN12 : patient loses her balance
- HN2 : patient fall during robot use
Development of a strategy

Context 4
Hazards found in classical rollator use:
- HN4: patient fall without alarm or with a late alarm
- HN5: physiological problem of the patient without alarm or with a late alarm
- HN1b: incorrect posture of patient during movement
- HN12: patient loses her balance
- HN2: patient fall during robot use

Strategy 2
Risks induced by classical rollator use are either correctly mitigated or not increased

Goal 8
Incorrect posture (HN1), patient fall (HN4) & physiological problem (HN5) without alarm risks are mitigated with an alarm system and a safe mode

Goal 9
Patient imbalance (HN12) risk is managed by a compensation system which is acceptably dependable

Goal 10
Patient fall during robot use (HN2) risk will not increase
How did we treat HN12?

• What is HN12?
  • The patient loses her balance

• MIRAS assistance
  • Moves back or forward to help patient to find her balance

• What is the hazard?
  • Loss of balance not detected in time
  • Improper compensation
Development of a goal

Context6
HN12 acceptable rate $\lambda_{HN12}$ is $10^{-4}$ per hour (for example)

Goal9
Patient imbalance (HN12) risk is managed by a compensation system which is acceptably dependable

Strategy3
Argument over acceptability of compensation system

Goal9.1
Design faults are properly managed

Solution26
Rigorous development process (61508 SIL requirement...)

Goal9.2
Compensation system failure rate due to physical faults is acceptable ($\lambda < \lambda_{\text{max}}$)

Solution27
Failure rate evaluation process (FTA, fault injection...)

Goal9.3
System compensation efficiency following patient imbalance is acceptable ($c > c_{\text{min}}$)

Solution28
Testing system under different patient imbalance scenarios

Justification2
$\lambda_{\text{max}}$ and $c_{\text{min}}$ given by Markov model
Markov model

\[ \lambda : \text{system failure rate} \]
\[ \alpha : \text{loss of balance rate} \]
\[ \mu : \text{compensation rate} \]
\[ c : \text{system compensation efficiency} \]

\[ \lambda_{HN12} \approx \lambda + (1 - c)\alpha \]

\[ \lambda \approx 10^{-4} \text{ per hour} \]
\[ \alpha \approx 4 \times 10^{-2} \text{ per hour} \]
\[ \mu \approx 60 \text{ per hour} \]
\[ (1 \text{ fall per day}) \]
\[ (\text{compensation in 1 minute}) \]
Which values of $c_{\text{min}}$ and $\lambda_{\text{max}}$?

$$\lambda \approx \lambda_{\text{HN12}} - (1 - c) \cdot \alpha$$

$\alpha \approx 4 \times 10^{-2}$ per hour

Feasible region

System compensation efficiency $c$

System failure rate $\lambda$

- $\lambda_{\text{HN12}} = 1.00 \times 10^{-4}$
- $\lambda_{\text{HN12}} = 4.00 \times 10^{-5}$
UML models

- Use case diagram
- Sequence diagram
- Statechart

HAZOP → Hazards → GSN

Risk analysis

Quantitative models

Argumentation
Thank you for your attention!
MODEL-BASED RISK ANALYSIS OF HUMAN-ROBOT INTERACTIONS AND SAFETY ARGUMENT CONSTRUCTION

Quynh Anh DO HOANG
Jérémie GUIOCHET
Mohamed KAÂNICHE
David POWELL
qdohoang@laas.fr

Model-based Safety Assessment Workshop
ISAE Campus de Rangueil – Toulouse March 15,16 2011