Towards the Use of Controlled Natural Languages in Hazard Analysis and Risk Assessment
Introduction – ISO 26262

ISO 26262 Road Vehicles – Functional Safety (2011)
Introduction – Hazard Analysis and Risk Assessment (1/2)

► Situation analysis and hazard identification

► Hazardous Event Classification
  - Determination of the Severity (S)
  - Probability of Exposure (E)
  - Controllability (C)

► Automotive Safety Integrity Level (ASIL) determination

<table>
<thead>
<tr>
<th>Vehicle Speed</th>
<th>Malfunction</th>
<th>Hazard</th>
<th>S</th>
<th>E</th>
<th>C</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10km/h</td>
<td>Charging of battery pack beyond allowable energy storage</td>
<td>Overcharge causes thermal event</td>
<td>S3</td>
<td>E3</td>
<td>C1</td>
<td>A</td>
</tr>
<tr>
<td>&gt;10km/h, &lt;50 km/h</td>
<td>Charging of battery pack beyond allowable energy storage</td>
<td>Overcharge causes thermal event</td>
<td>S3</td>
<td>E3</td>
<td>C2</td>
<td>B</td>
</tr>
<tr>
<td>&gt; 50 km/h</td>
<td>Charging of battery pack beyond allowable energy storage</td>
<td>Overcharge causes thermal event</td>
<td>S3</td>
<td>E3</td>
<td>C3</td>
<td>C</td>
</tr>
</tbody>
</table>

Introduction – Hazard Analysis and Risk Assessment (2/2)

► Problems:
  - Determination of the risk parameters
  - Risk parameters defined in a qualitative way
  - Documentation

► Documentation – Natural language
  - Similar hazardous events are often described using different wordings and phrases
  - Similar hazardous events might be classified differently
  - Difficult to check consistency

► Goal: Consistent hazardous event ratings across all hazard analyses and risk assessments
Related Work – Controlled Natural Languages

► Controlled natural languages (CNLs)
  ▪ Subset of a natural language
  ▪ Restrictions on
    • Grammar
    • Vocabulary
  ▪ Objectives
    • Reduce ambiguity and complexity
    • Improve readability and automatic processing

► Many examples from various domains
  ▪ Knowledge representation
  ▪ Requirements engineering
  ▪ Aviation
  ▪ Biomedicine
  ▪ ...
Related Work – Attempto Controlled English (ACE) (1/2)

- CNL for knowledge representation and query language

- Objectives:
  - Automatic and unambiguous translation into first-order logic

- Vocabulary
  - Functions words (conjunctions, prepositions, ...) and predefined phrases (there is, it is false that, ...)
  - Content words (nouns, verbs, adjectives, and adverbs)
    - Basic lexicon (~ 100,000 entries)

- Grammar
  - Sequence of declarative sentences
  - Questions

A customer inserts a card that is valid and opens an account.

A customer inserts the card.
A card is valid.
The customer opens an account.

A customer inserts a card that is valid and that opens an account.

Does a customer insert a card?
Who inserts a card?

Related Work – Standard Language (SLANG)

► CNL for writing of process build instructions

► Objectives
  ▪ Reduce ambiguity and lack of consistency
  ▪ Generation of required elements and labor times
  ▪ Automatic translation

► Sentence written in imperative form
  ▪ Sentence → VerbPhrase PrepositionalPhrase*

► Number of verbs is limited and each verb describes a single particular action

Related Work – Summary

Why not using an existing controlled natural language?

- General-purpose language
  - Not optimized for a domain-specific problem
  - In general, usage is possible but more complex

- Domain-purpose language
  - Too domain-specific
  - Usually not applicable for other domains/purposes

## Ford’s Hazard Analysis and Risk Assessment Tooling

<table>
<thead>
<tr>
<th>Scenario Description: Vehicle Usage</th>
<th>Scenario Description: Detailed sample worksheet</th>
<th>Effect on Vehicle Level</th>
<th>Hazard</th>
<th>Assumptions</th>
<th>Hazardous Event (PEM-DE)</th>
<th>G</th>
<th>Severity</th>
<th>E</th>
<th>Exposer</th>
<th>C</th>
<th>Controllability</th>
<th>ASIL</th>
<th>Safety Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph prior to malfunction (Refer to Appendix)</td>
<td>Describe the situation including relevant technical details or examples of similar events</td>
<td>Describe relevant vehicle level</td>
<td>Pick corresponding hazard from Hazard Dictionary</td>
<td>Reference see Tab: &quot;Assumptions&quot; (optional)</td>
<td>Assign a name (including hazard and threat and risk driver)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Rationale
- (description of reasonable expected consequences, if not obvious)
- (including description of accident, if applicable)

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>(Additional columns needed, and additional columns)</th>
</tr>
</thead>
</table>

---

Towards the Use of Controlled Natural Languages in Hazard Analysis and Risk Assessment
Paul Chomicz | 31.05.2017
### Analysis Process (1/3)

**Iterative and bottom-up approach**

<table>
<thead>
<tr>
<th>Hazardous Events</th>
<th>9 HARA documents</th>
<th>7 HARA documents</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BP</td>
<td>BP</td>
<td>BP</td>
</tr>
<tr>
<td></td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>208</td>
<td>67.8 %</td>
<td>81.7 %</td>
</tr>
<tr>
<td></td>
<td>93</td>
<td>21.6 %</td>
<td>12.9 %</td>
</tr>
<tr>
<td></td>
<td>10.6 %</td>
<td>10.6 %</td>
<td>5.4 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>9 HARA documents</th>
<th>7 HARA documents</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7 HARA documents</td>
<td>7 HARA documents</td>
<td>7 HARA documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The system is active at high speed and may not detect objects in relevant distance (due to sensor performance).

The driver is not alerted to a credible threat.

Unintended and unlimited AEB brake activation leading to loss of vehicle steerability due to blocked wheels without ABS.

Fire outside passenger compartment.
Analysis Process (2/3)

Most frequently used words and phrases in hazardous event descriptions:

- unintended
- vehicle(s)
- no hazard
- loss of
- the
- in
- due to
- braking
- behaviour
- acceleration; and
- brake(s); driver(s); is; yaw
- a; speed; unexpected
- driving; propulsion; with

Graph showing the frequency of these terms.
Synonyms and similar words and phrases in hazardous event descriptions:

- unintended
- unexpected
- undue
- undesired
- not expected
- unintended yaw behaviour
- unexpected yaw behaviour
- braking
- brake
- brakes
- behaviour
- behavior
Formalization (1/2)

► Restrictions on grammar and vocabulary

► Descriptions in bullet-point manner

► Reduction of complexity
  - No verbs!
  - No grammatical tenses!
  - No pronouns!
  - No clauses!

► Reduction of ambiguity
  - Restricted vocabulary without synonyms
Formalization (2/2)

NP -> Determiner? Adverb* Adjective* Noun+

PP -> Preposition NP

HE -> NP PP*

Hazardous Event Description

NP

PP

IN

NP

Fire outside passenger compartment.
Evaluation (1/2)

<table>
<thead>
<tr>
<th>Hazardous Events</th>
<th>9 HARA documents</th>
<th>7 HARA documents</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>208</td>
<td>93</td>
<td>301</td>
</tr>
<tr>
<td>BP</td>
<td>67.8 %</td>
<td>81.7 %</td>
<td>72.1 %</td>
</tr>
<tr>
<td>S</td>
<td>21.6 %</td>
<td>12.9 %</td>
<td>18.9 %</td>
</tr>
<tr>
<td>M</td>
<td>10.6 %</td>
<td>5.4 %</td>
<td>9.0 %</td>
</tr>
</tbody>
</table>

- 156 out of 217 already in line with the CNL (71.9 %)
- 48 hazardous events translated into a correct form by replacing synonyms (22.1 %)
- Other descriptions also translated into semantically equivalent descriptions conform to the CNL
The system is active at high speed and may not detect objects in relevant distance (due to sensor performance).

Active system at high speed and undetected objects in relevant distance by the system due to sensor performance.
Conclusion

► Controlled natural languages based on given HARAs
  - Common structure
  - Restricted vocabulary

► Reduction of complexity and ambiguity

► Common structure simplifies the search for existing same or similar hazardous events

► Tooling essential
  - Correctness
  - Input support
Outlook

► Formalization of the rationales for the risk parameters
  ▪ Severity
  ▪ Exposure
  ▪ Controllability

► Implementation of the concept in a prototype tool

► Case study based on prototype tool
  ▪ Further examination and improvement of the concept
  ▪ Gather more user experience
  ▪ Show benefits of the concept