Automotive – Safety & Security 2017

Paul Chomicz

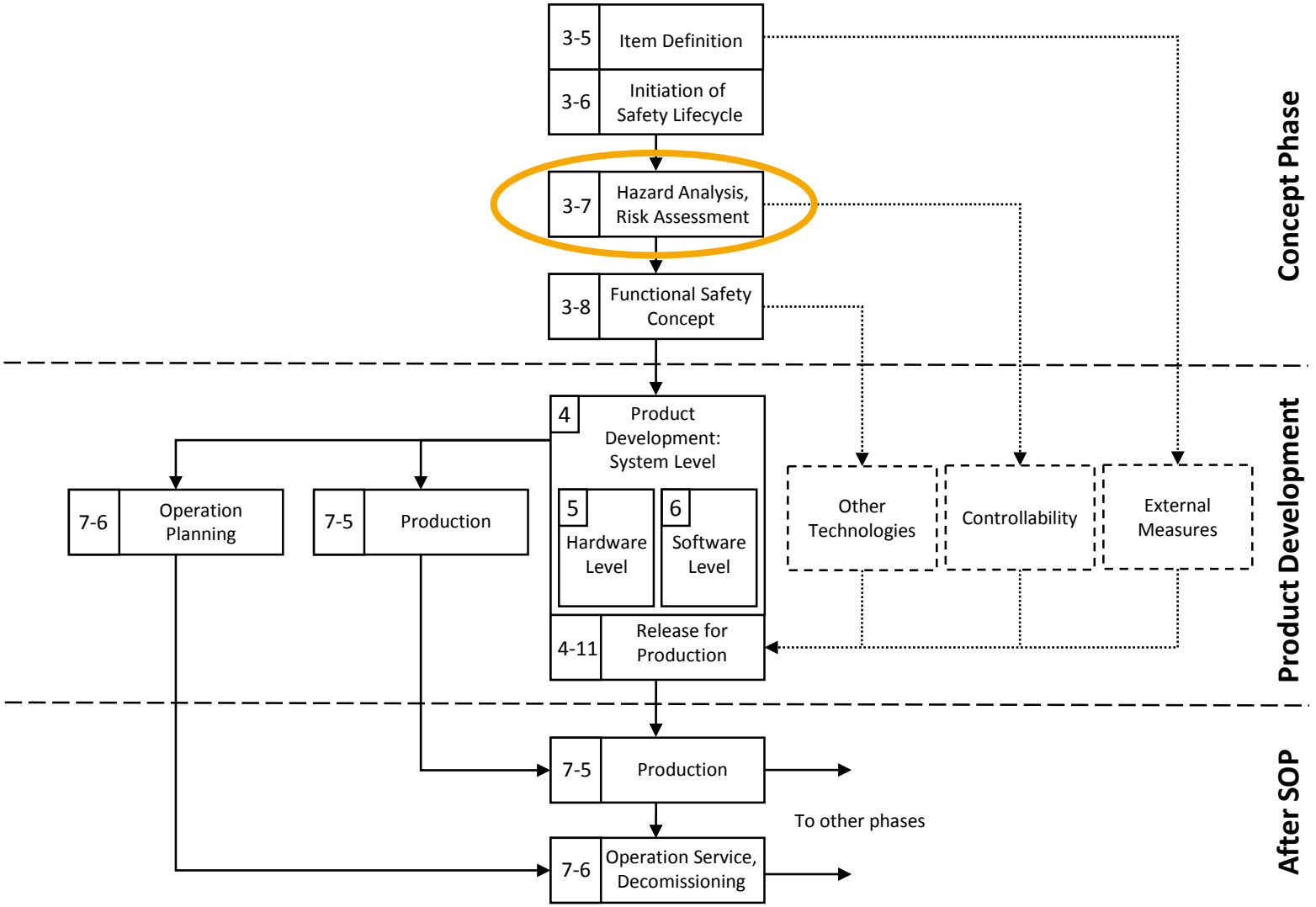
31.05.2017

Towards the Use of Controlled Natural Languages in Hazard Analysis and Risk Assessment

Informatik 11
Embedded Software

RWTH AACHEN UNIVERSITY

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

Vehicle Speed	Malfunction	Hazard	S	E	C	ASIL
<10km/h	Charging of battery pack beyond allowable energy storage	Overcharge causes thermal event	S3	E3	C1	A
>10km/h, <50 km/h	Charging of battery pack beyond allowable energy storage	Overcharge causes thermal event	S3	E3	C2	B
> 50 km/h	Charging of battery pack beyond allowable energy storage	Overcharge causes thermal event	S3	E3	C3	C

Taylor, W.; Krithivasan, G.; Nelson, J.J., "System safety and ISO 26262 compliance for automotive lithium-ion batteries," *Product Compliance Engineering (ISPCE), 2012 IEEE Symposium on* , pp. 1-6, 5-7 Nov. 2012

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

Fuchs, Norbert E., Kaarel Kaljurand, and Tobias Kuhn. “Attempto Controlled English for Knowledge Representation.,” *Reasoning Web*, pp. 104-124, Springer Berlin Heidelberg. 2008.

Related Work – Attempto Controlled English (ACE) (2/2)

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

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

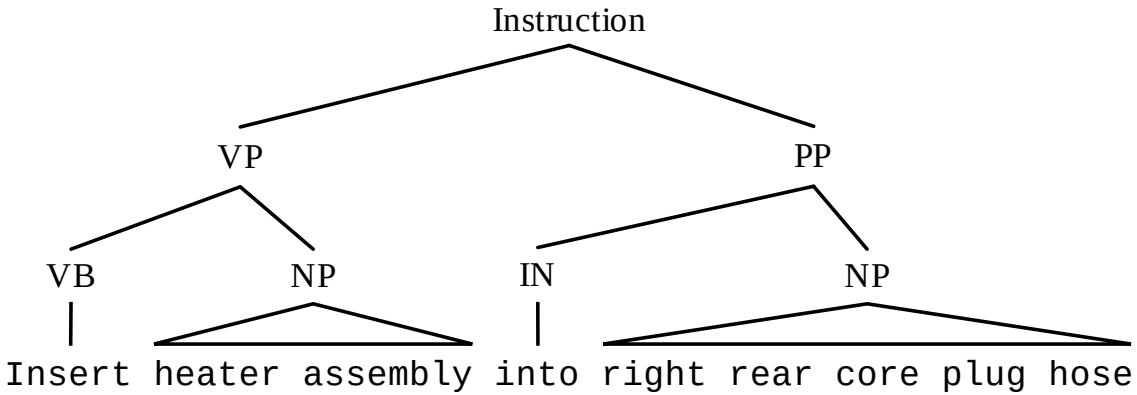
Does a customer insert a card?

Who inserts a card?

Fuchs, Norbert E., Kaarel Kaljurand, and Tobias Kuhn. “Attempto Controlled English for Knowledge Representation,” *Reasoning Web*, pp. 104-124, Springer Berlin Heidelberg. 2008.

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



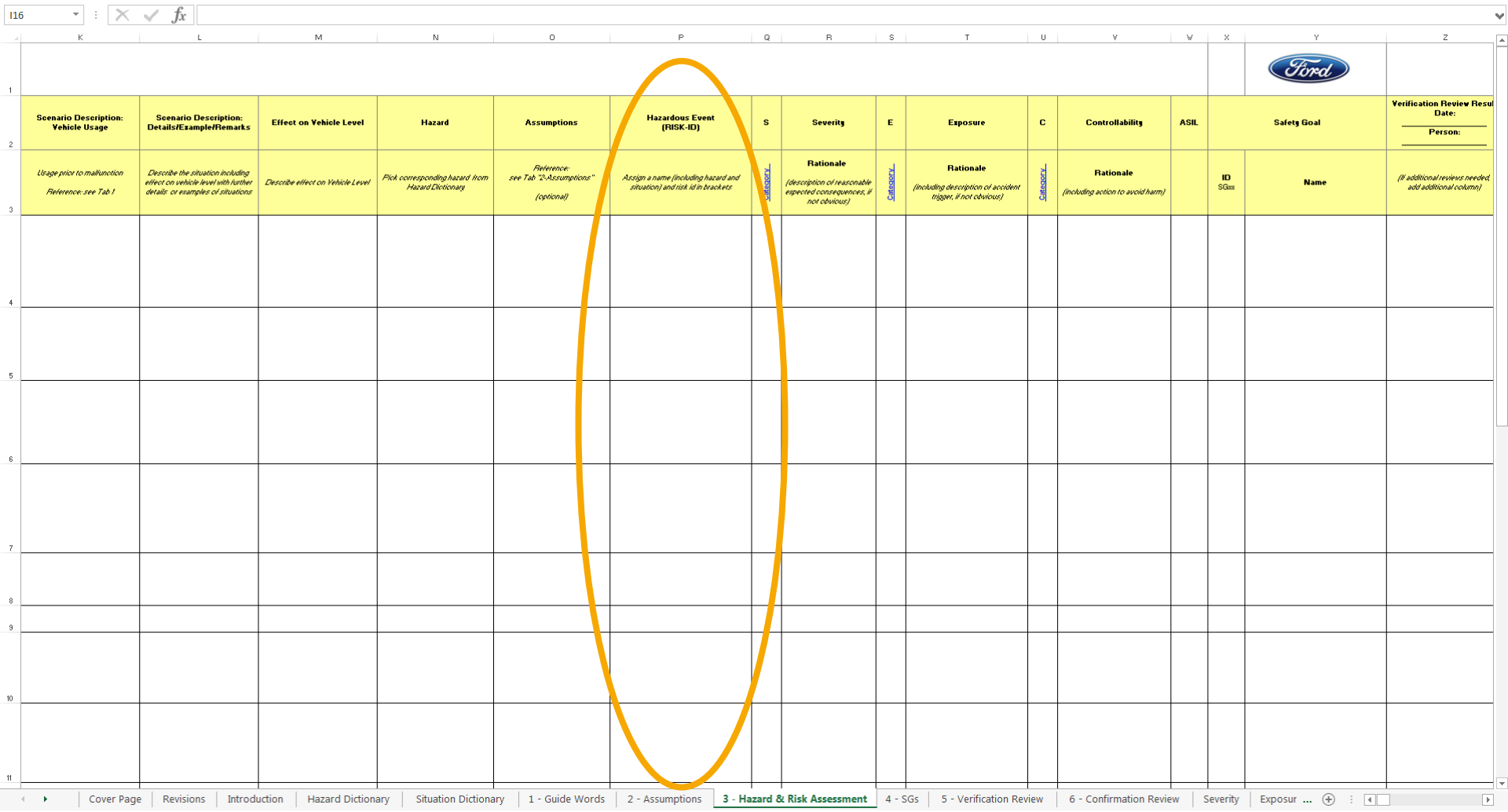
N. Rychtyckyj. “An Assessment of Machine Translation for Vehicle Assembly Process Planning at Ford Motor Company,” *Conference of the Association for Machine Translation in the Americas*, pp. 207-215, Springer Berlin Heidelberg. 2002.

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

Tobias Kuhn. “A Survey and Classification of Controlled Natural Languages,” *Computational Linguistics 40*, no. 1, pp. 121-170, 2014.

Ford's Hazard Analysis and Risk Assessment Tooling



Scenario Description: Vehicle Usage	Scenario Description: Details/Example/Remarks	Effect on Vehicle Level	Hazard	Assumptions	Hazardous Event (RISK-ID)	S	Severity	E	Exposure	C	Controllability	ASIL	Safety Goal		Verification Review Result Date: Person:
Usage prior to malfunction Reference: see Tab 1	*Describe the situation including effect on vehicle level with further details or examples of situations*	*Describe effect on Vehicle Level*	*Pick corresponding hazard from Hazard Dictionary*	*Reference: see Tab "2-Assumptions" (optional)*	*Assign a name (including hazard and situation) and risk id in brackets*	Category	Rationale *(description of reasonable expected consequences, if not obvious)*	Category	Rationale *(including description of accident trigger, if not obvious)*	Category	Rationale *(including action to avoid harm)*		ID SGxx	Name	*(If additional reviews needed, add additional column)*

Cover Page | Revisions | Introduction | Hazard Dictionary | Situation Dictionary | 1 - Guide Words | 2 - Assumptions | 3 - Hazard & Risk Assessment | 4 - SGs | 5 - Verification Review | 6 - Confirmation Review | Severity | Exposur ...

Analysis Process (1/3)

- Iterative and bottom-up approach

		9 HARA documents		7 HARA documents		total	
Hazardous Events	BP	208	67.8 %	93	81.7 %	301	72.1 %
	S		21.6 %		12.9 %		18.9 %
	M		10.6 %		5.4 %		9.0 %

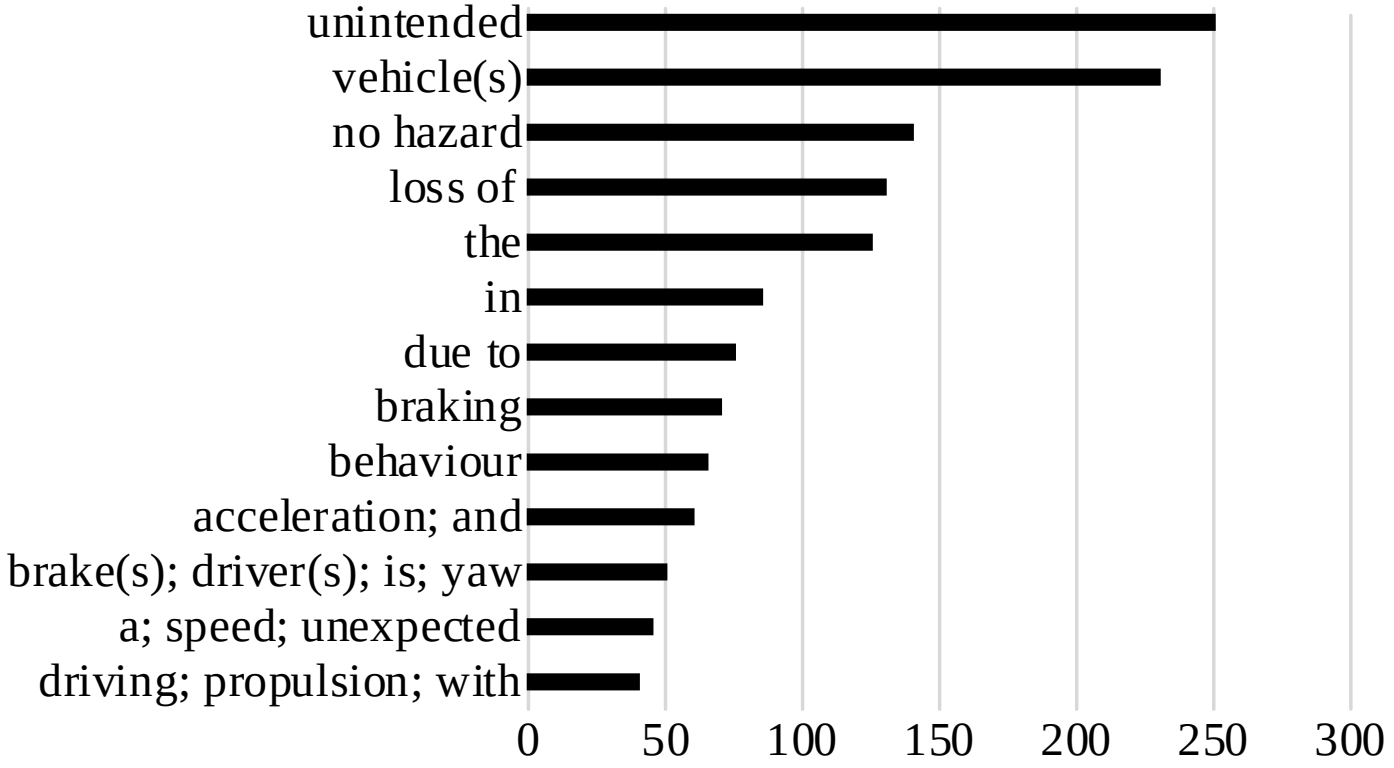
The driver is not alerted to a credible threat.

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

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

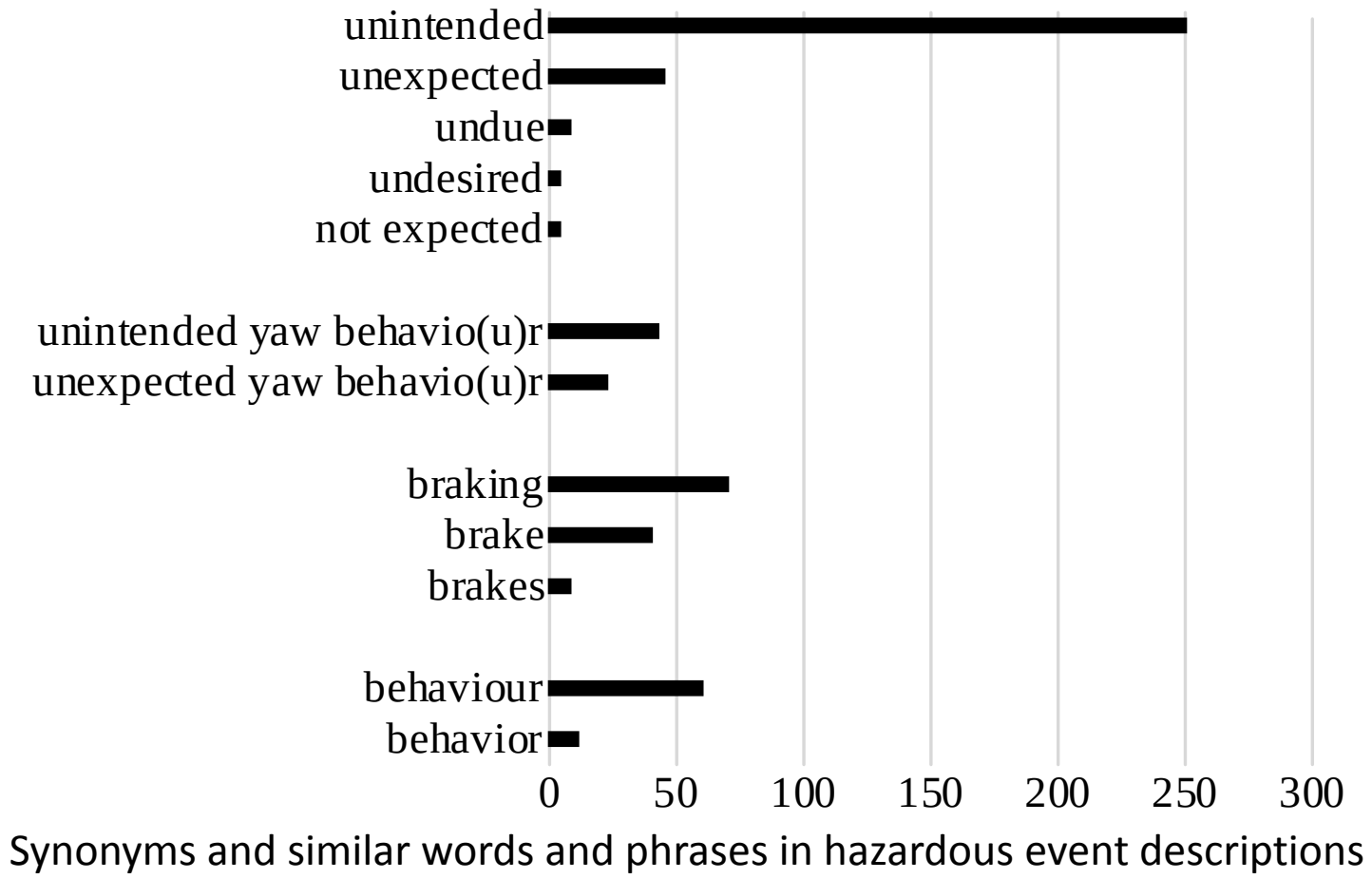
Fire outside passenger compartment

Analysis Process (2/3)



Most frequently used words and phrases in hazardous event descriptions

Analysis Process (3/3)



Formalization (1/2)

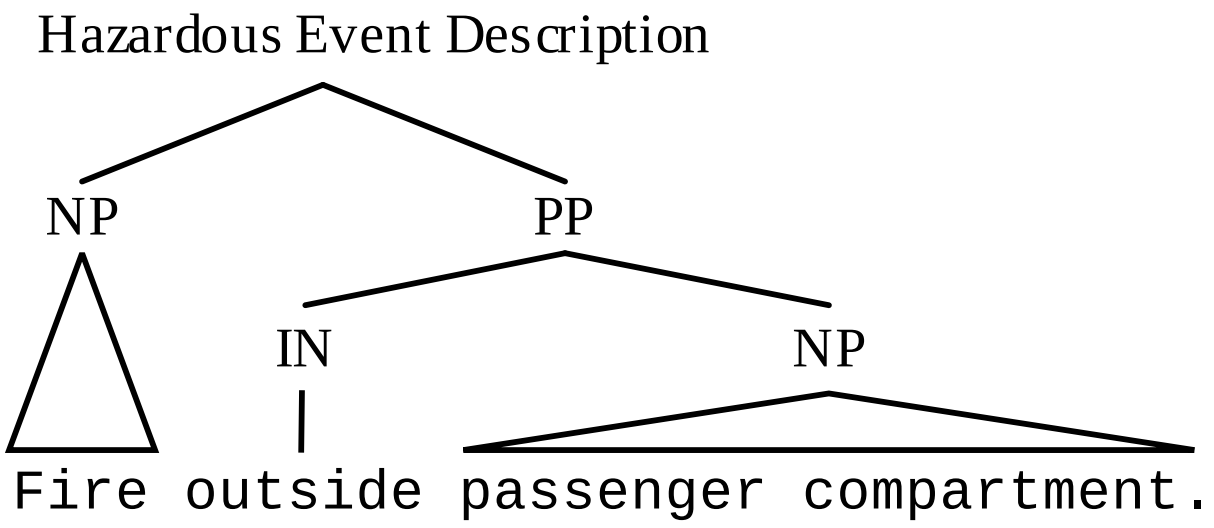
- Restrictions on grammar and vocabulary
- Descriptions in bullet-point manner
- Reduction of complexity
  - No verbs!
  - No grammatical tenses!
  - No pronouns!
  - No clauses!
- Reduction of ambiguity
  - Restricted vocabulary without synonyms

Formalization (2/2)

```
NP -> Determiner? Adverb* Adjective* Noun+

PP -> Preposition NP

HE -> NP PP*
```

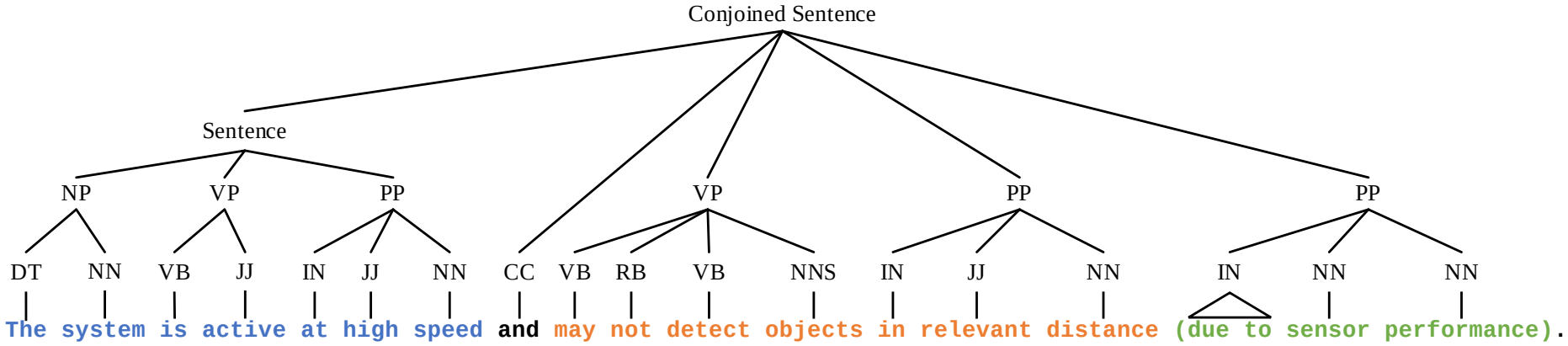


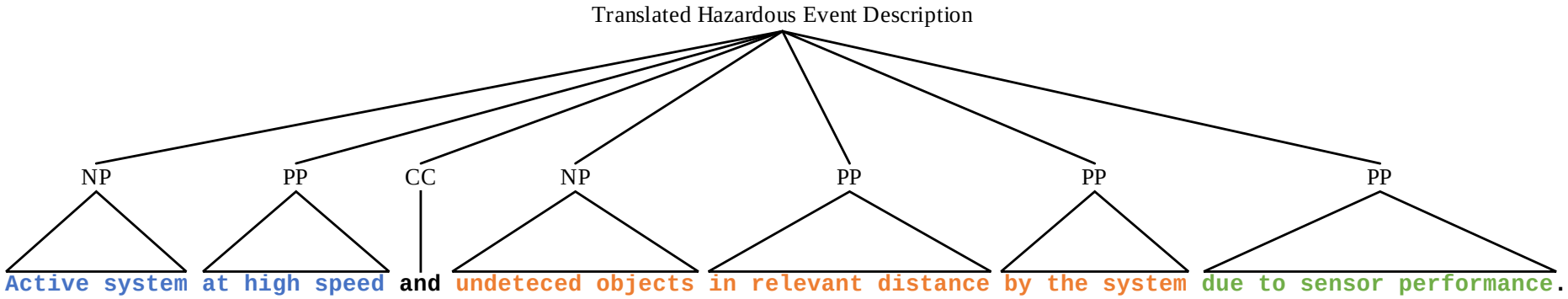
Evaluation (1/2)

		9 HARA documents		7 HARA documents		total	
Hazardous Events	BP	208	67.8 %	93	81.7 %	**301**	**72.1 %**
	S		21.6 %		12.9 %		18.9 %
	M		10.6 %		5.4 %		9.0 %

- 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

Evaluation (2/2)





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