CNL 2018 : Sixth International Workshop on Controlled Natural Language

Paul Chomicz, Armin Müller-Lerwe, Götz-Philipp Wegner, Rainer Busch, and Stefan Kowalewski

27.08.2018

Controlled Natural Languages for Hazard Analysis and Risk Assessment

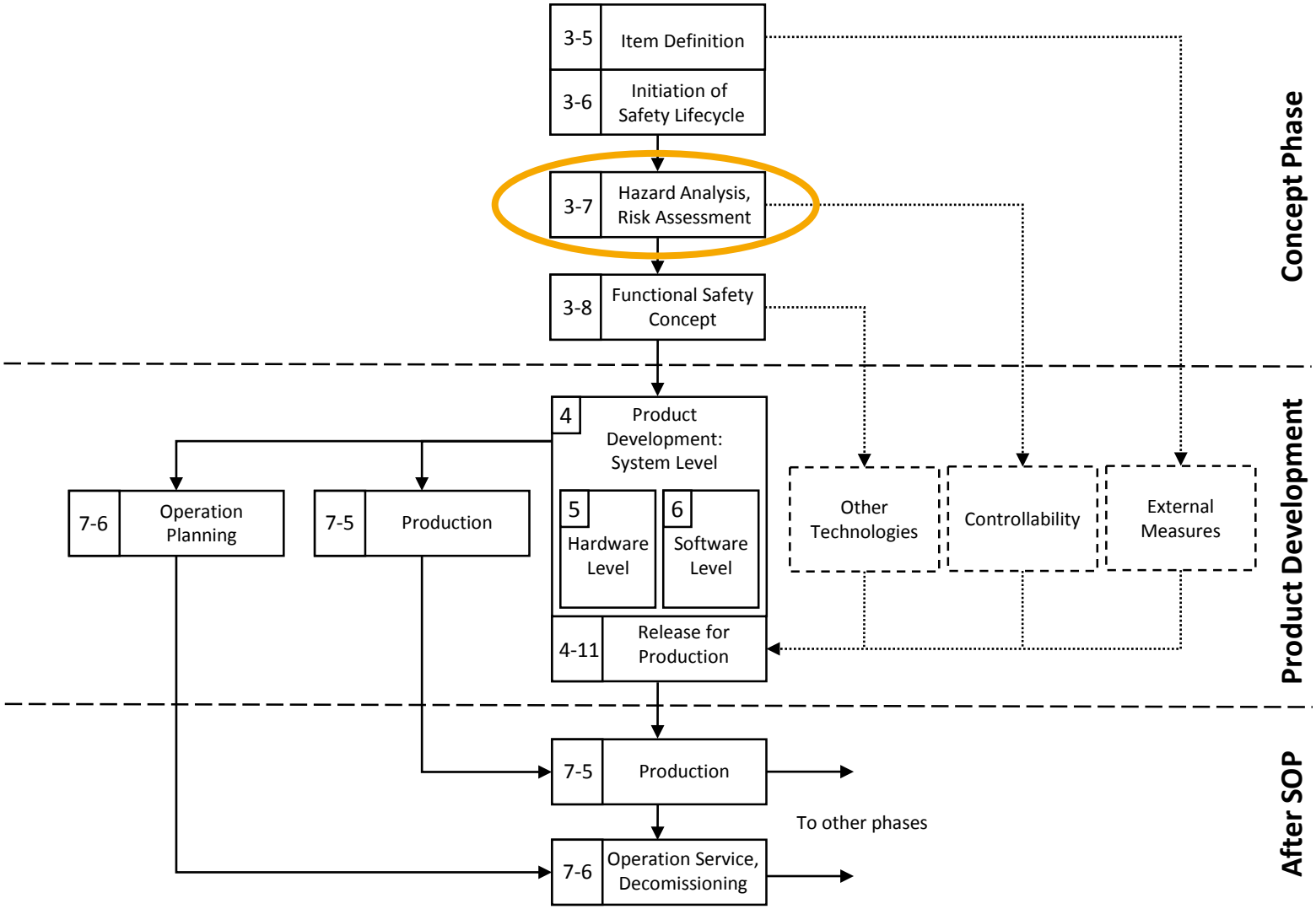
Informatik 11
Embedded Software

RWTH AACHEN UNIVERSITY

Outline

- ISO 26262
  - Hazard Analysis and Risk Assessment
- Hazard Analysis and Risk Assessment at Ford
- Controlled Natural Languages for Hazard Analysis and Risk Assessment
- Conclusion and Outlook

ISO 26262



ISO 26262 Road Vehicles – Functional Safety (2011)

Hazard Analysis and Risk Assessment – HARA (1/2)

- Situation analysis
  - Hazardous event
- Classification
  - Severity of potential harm (S)
  - Probability of Exposure (E)
  - Controllability (C)
- Automotive Safety Integrity Level (ASIL) and Safety Goal (SG) determination

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

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

- Problems:
  - Determination of the risk parameters
  - Risk parameters defined in a qualitative way
    - C1 – Simply controllable
    - C2 – Normally controllable
  - Documentation
- Documentation – Natural language
  - Similar hazardous events are often described using different wordings and phrases
  - Similar hazardous events might be classified differently

HARA @ Ford (1/2)

Excel

Hazardous Event (RISK-ID)	S	Severity	E	Exposure	C	Controllability	ASIL	Safety Goal	
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**

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 ...

HARA @ Ford (2/2)

- New functions use the same actuators
- Malfunctions could cause similar hazards
- Difficult to check consistency, since different functions are developed by different teams
- Goal: Consistent hazardous event ratings across all hazard analyses and risk assessments

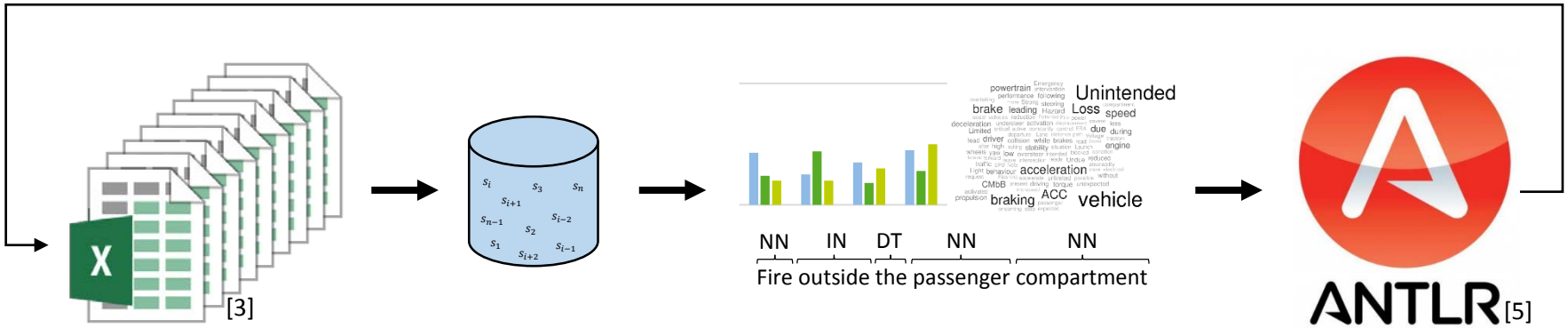
Previous Work

Hazardous Event	Severity		Exposure		Controllability		ASIL
	S	Rationale	E	Rationale	C	Rationale	
CNL	S0 S1 S2 S3		E0 E1 E2 E3 E4		C0 C1 C2 C3		QM A B C D

- Controlled Natural Language for the description of hazardous events
- Development according to today's presented CNLs

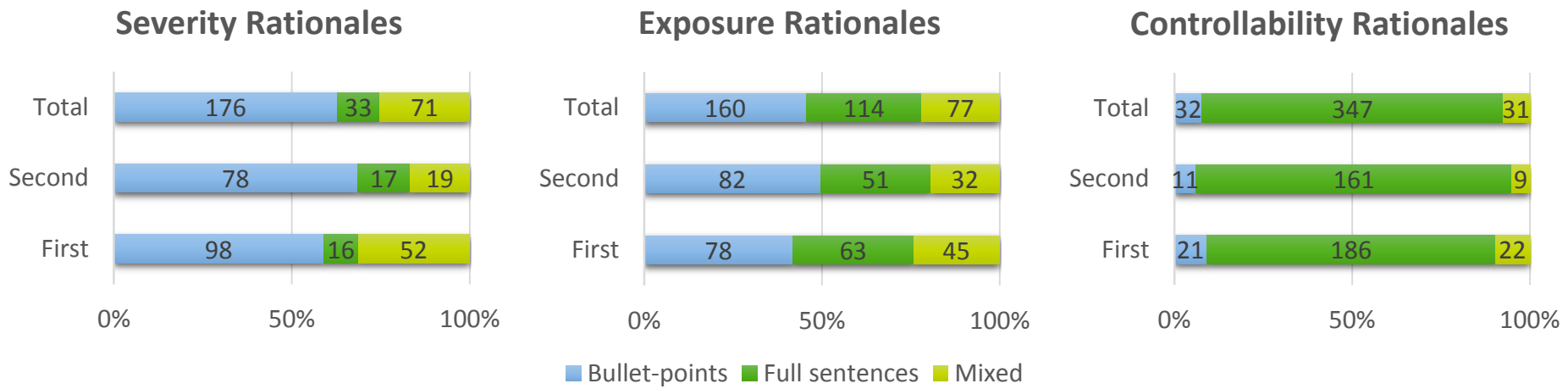
Chomicz, P., Müller-Lerwe, A., Wegner, G., Busch, R., and Kowalewski, S., "Towards the Use of Controlled Natural Languages in Hazard Analysis and Risk Assessment", in *Proc. Automotive - Safety & Security 2017*, pp. 163-174.

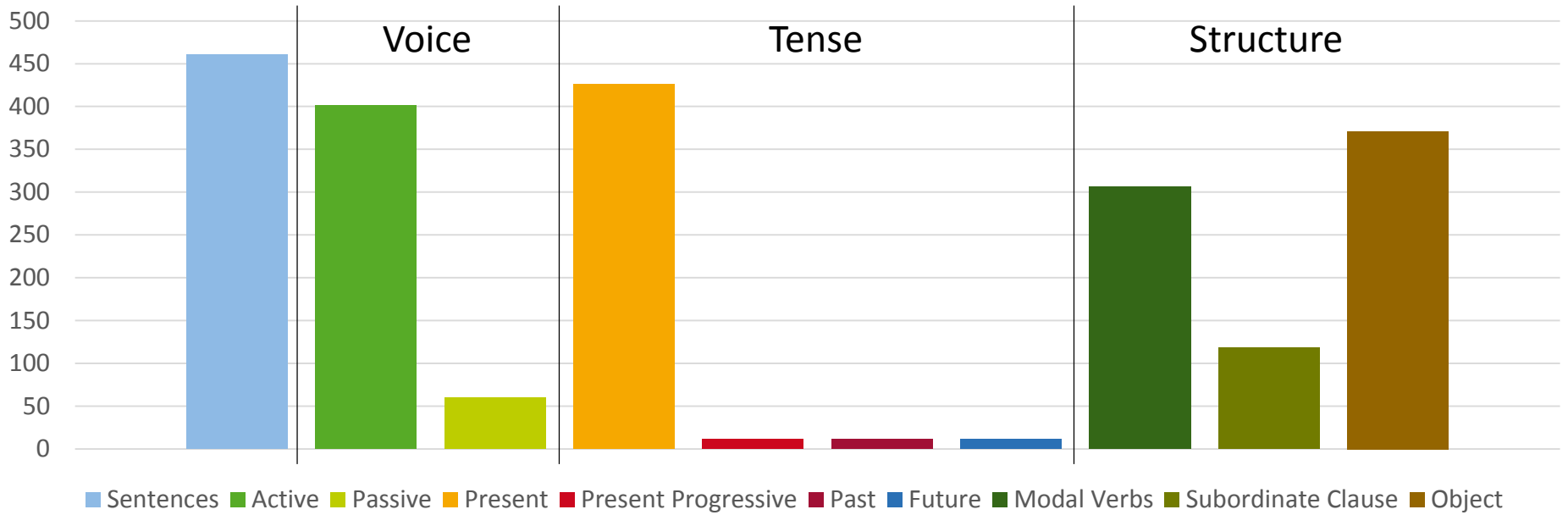
Formalization (1/2)



- Word frequency statistics
- Part-of-speech tagging
- Sentence structure statistics
  - Full sentences
  - Bullet-point phrases

Formalization (2/2)





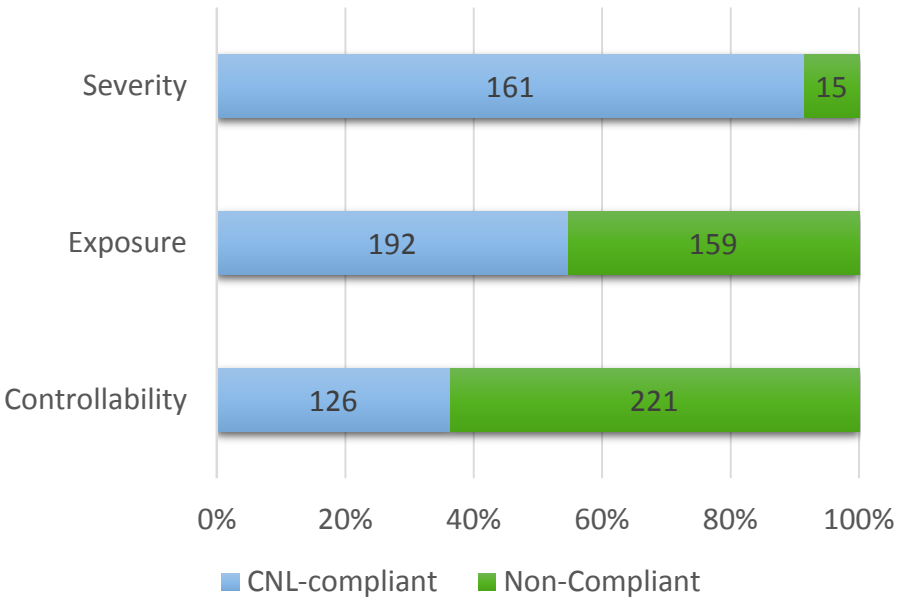
CNLs for HARA

Hazardous Event	Severity		Exposure		Controllability		ASIL
	S	Rationale	E	Rationale	C	Rationale	
BP-CNL	S0 S1 S2 S3	*BP-CNL*	E0 E1 E2 E3 E4	*BP-CNL* *FS-CNL*	C0 C1 C2 C3	*FS-CNL*	QM A B C D

- Bullet-Point CNL
  - Nominal phrases connected with prepositions and conjunctions
  - No verbs
- Full-Sentence CNL
  - Fixed sentence structures
  - No passive voice
  - Only present tense
- Common Vocabulary
  - Domain-specific
  - No pronouns
  - Removed synonyms

Evaluation

- Created CNLs evaluated against provided data to show intended relation



- Prototypical application in HARAs for new systems
  - Steering
  - Fuel cell
  - Powertrain
- Usage required vocabulary extension

Conclusion

- Controlled natural languages based on given HARAs
  - Common structure
  - Restricted vocabulary
- Reduction of complexity and ambiguity
- Common structure simplifies the check for consistency
- Tooling essential
  - Correctness
  - Input support
  - Consistency check

Outlook

- Implementation of the concept in a prototype tool
  - Ontology
  - Semantic analysis
  - Consistency check
- Case study based on prototype tool
  - Further examination and improvement of the concept
  - Gather more user experience
  - Show benefits of the concept

Image References

[1] Ford Motor Company – Global Locations - https://upload.wikimedia.org/wikipedia/commons/thumb/5/52/Ford_Motor_Company_global_locations.png/800px-Ford_Motor_Company_global_locations.png

[2] Map Location - http://jrnychurch.com/wp-content/uploads/2016/08/map__location_large_dot_indicator_navigation-512.png

[3] Excel File Icon - https://cdn.windowsfileviewer.com/images/types/xlsx.png

[4] ANTLR Icon - https://avatars3.githubusercontent.com/u/80584