Controlled Natural Language
B. Davis et al. (Eds.)

doi:10.3233/978-1-61499-904-1-41

Controlled Natural Languages for Hazard Analysis and Risk Assessment

Paul CHOMICZ [a], Armin MÜLLER-LERWE [b], Götz-Philipp WEGNER [b], Rainer BUSCH [b], and Stefan KOWALEWSKI [a]
[a] *RWTH Aachen University, Lehrstuhl Informatik 11 – Embedded Software*
[b] *Ford Research & Innovation Center Aachen*

Abstract. The hazard analysis and risk assessment (HARA) is a safety activity, which is performed during the concept phase of the functional safety standard ISO 26262. The results of this activity are usually documented by using a natural language. On the one hand, natural languages are expressive and powerful, but on the other hand, they are also ambiguous and complex. The usage of controlled natural languages (CNLs) is a means to reduce the drawbacks of natural languages. In this paper, we introduce controlled natural languages for the rationales of the three risk parameters: severity, exposure, and controllability to extend our set of CNLs for the HARA. In the first place, the application of controlled languages leads to more harmonized descriptions and rationales. Subsequently, an automatic processing based on these languages shall be implemented to enable the detection of inconsistencies across different HARA documentations.

Keywords. Controlled Natural Language, Hazard Analysis and Risk Assessment, Functional Safety, ISO 26262, Controllability, Exposure, Severity, Rationale, Risk Parameter

1. Introduction

The ISO 26262 is an international standard for functional safety of electrical or electronic systems within road vehicles that was published in 2011 [1]. One of the first activities according to the safety lifecycle of the ISO 26262 is the hazard analysis and risk assessment (HARA) [2].

The HARA is divided into three steps. It starts with the identification of all hazards that could be caused by a potential malfunctioning behavior. Then, all relevant operational situations and operation modes are determined in which the identified hazards could possibly occur. The combination of a certain hazard and the situation in which the hazard could occur is called hazardous event. The second step is the assessment of the hazardous event regarding its risk. It comprises the determination of the risk parameters: severity, exposure, and controllability. The rating of the severity reflects the estimated potential harm caused by the hazardous event. The exposure describes the probability of being in the corresponding situation, and the controllability reflects the ability of the driver or other traffic participants to avoid the potential harm. The last step is the assignment of the automotive safety integrity level (ASIL) and the definition of a safety goal. Based on the ratings for severity, exposure, and controllability, a corresponding ASIL will be assigned to the hazardous event. The ASIL specifies the necessary level of risk reduction with ASIL A being the lowest and ASIL D the highest level. Additionally, the class quality management (QM) can be assigned. It states that no safety requirements have to be managed under the ISO 26262 safety lifecycle for this hazardous event. For every hazardous event with an ASIL assigned to it, a safety goal has to be defined. The safety goal is a top-level safety requirement defining how to prevent or mitigate the risk of the hazardous event [2].

The ISO 26262 standard defines the three risk parameters in a qualitative way that leaves room for interpretation. As a consequence and based on the fact that new systems share the same actuators causing the same malfunctions and similar hazards, it is challenging to ensure consistency of the risk assessments along with their rationales between HARAs developed by different teams.

To describe and record the identified hazardous events and the rationales for the risk classifications, a natural language is usually used. Natural languages are complex and ambiguous. Therefore, it might be the case that same or similar hazardous events or risk parameter rationales could be described using different wordings and phrases. This makes it more difficult to verify the consistency across several HARAs.

Our approach to tackle these problems is to apply controlled natural languages (CNLs) for the documentation. A CNL is based on a natural language and restricts the grammar or the vocabulary of it [3]. Therefore, it is a subset of a natural language. The restrictions intend to reduce or eliminate ambiguity and to improve machine processing [4]. The usage of controlled natural languages for the hazard analysis and risk assessment shall reduce the possibility to write similar or same hazardous events or rationales with different wordings and phrases. Furthermore, the languages might be used to enable an automatic check to detect inconsistencies between different HARAs.

The remainder of this paper is structured as follows. The next section describes related work and previous work that was made to achieve a controlled natural language for the hazardous event descriptions. Afterwards, the formalization process along with the resulting CNLs for the rationales of the three risk parameters severity, exposure, and controllability are presented. The paper concludes with an evaluation of the created languages and an outlook on future work.

2. Related Work

In a previous work [5], we have already developed a controlled natural language for the description of hazardous events. Along with means to perform a situation analysis [6], the CNL can be used to record the outcomes of the first step of the hazard analysis and risk assessment in a more formal way than only using a natural language.

The grammar of the controlled natural language for the description of hazardous events only allows to write the description in a bullet-point manner. Noun phrases (NPs) are used to describe an event, a situation, or a characteristic of a system. The headword of the phrase is a noun, and it can contain additional adnominals. Certain prepositions (IN) and conjunctions are used to connect several noun phrases to create more complex descriptions. The usage of pronouns, clauses, and verbs is prohibited to further reduce the complexity. In the depicted example in Fig. 1, two simple noun phrases are connected with a preposition resulting in a noun phrase and a prepositional phrase (PP) [13].

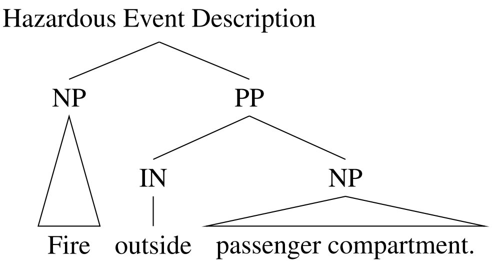

Figure 1. Hazardous event description written in the CNL [5]

The developed controlled natural language is based on a representative set of already finished HARAs that were documented using the English language. In a bottom-up and iterative approach, the documents were analyzed to find a common structure for the descriptions. From this common structure the CNL was created. The newly created language was applied in two ways. Firstly, it was used to describe all hazardous events which already exist in the HARAs that were analyzed. A large portion (51.9 %) of the existing descriptions was already compliant to the controlled language. The other portion could be translated by domain experts into semantically equivalent descriptions that are in line with the language. Secondly, the CNL was prototypically utilized to three newly created HARAs at the Ford Research & Innovation Center Aachen. After extending the vocabulary with domain-specific terms, all hazardous events could be described using the new language.

Several controlled natural languages have been developed for various domains and purposes [4,7]. Among these, a great number has been designed for requirements engineering like [8] or [9]. Requirements are rather specifying in contrast to the hazardous events and the risk parameter rationales which have a rather descriptive and justifying character.

Such kind of languages have been developed or used for technical documentations, like Caterpillar Technical English [10] or Bull Controlled English [11]. These languages usually consist of a simplified set of rules and a controlled vocabulary to improve understandability and translatability. During the creation of the new controlled natural languages for the hazard analysis and risk assessment, the presented best-practice features and the models for developing a new controlled natural language for technical documents were considered and applied [12].

3. Formalization Process

For the formalization of the rationales, the same process was applied as for the formalization of the hazardous event descriptions [5]. In two iterations, different sets of HARAs were analyzed to find a common structure for each rationale. At first, the single rationales were extracted from the documents, and duplicates were removed. Then, the rationales were analyzed in detail by determining word frequency statistics, the used parts of speech, and sentence structure statistics based on the part of speech tagging. All operations, like the part of speech tagging, were performed computer-assisted and double-checked manually.

The severity rationales have a similar structure as the hazardous event descriptions [5]. Therefore, the structure can be divided into two categories. The first category contains rationales written in a bullet-point manner, and for the second category, full sentences were used to formulate the rationales. In the first iteration, 166 different severity rationales were extracted from the given documents. The biggest part of the rationales belongs to the first category (59 %). Only a small portion (9.7 %) uses full sentences for the rationales. The remaining rationales were written in a mixed version of using full sentences and bullet-points (31.3 %).

In the second iteration, 114 additional severity rationales were extracted. For both iterations, the same documents were used as for the formalization of the hazardous event descriptions [5]. In this set, the portion of bullet-point rationales is bigger (62.9 %), and again, only a few were written using full sentences (14.9 %). The categorization was performed manually in both iterations.

An exemplary set of severity rationales is shown in Table 1 that represents how the rationales are currently described using the English language. The rationales 1 and 3 are written in a bullet-point manner, the rationale 2 is written as a full sentence, and the last rationale is described in a mixed version.

Table 1. Exemplary set of severity rationales

No.	*Severity Rationale*
1	Potential collision with surrounding traffic at low speed.
2	Pedestrian may be overrolled.
3	Potential lane departure due to unexpected yaw behavior. Potential crash into pedestrians or obstacles beside the road or side collision with oncoming traffic.
4	Vehicle may be moved into the path of oncoming traffic. Side collision with velocities greater than 35 kph possible.

Furthermore, we analyzed the exposure rationales and the controllability rationales in the same way and divided the single rationales into the two categories. In total, 351 different exposure rationales were extracted from 16 different HARAs and categorized. Nearly the half (45.6 %) is formulated in bullet-point manner, and a third (32.5 %) is written using full sentences. The remaining 22.9 % are stated in a mixed version. Table 2 shows an exemplary set of exposure rationales.

Table 2. Exemplary set of exposure rationales

No.	*Exposure Rationale*
1	Service situation. Frequency rated.
2	Failure can potentially occur during any driving situation.
3	Launch on a hill on μ-split occurs a few times a year for the great majority of drivers.
4	Stopped at intersection (E4); however lower probability with non-motorist crossing the road (E3), 1-10 % of average operating time.

The results of the analysis of the controllability rationales indicate an even stronger tendency for using full sentences to justify the chosen controllability value. From the 16 HARA documents, overall, 410 different controllability rationales were extracted. Only 7.8 % of the rationales are written in a bullet-point manner. The major part is stated in full sentences (84.6 %). Again, in the remaining rationales, bullet-point phrases and full sentences are used together (7.6 %). The Table 3 contains some controllability rationale examples.

Since the focus has changed on using full sentences, we also analyzed the structure of the sentences in more detail for the exposure rationales and the controllability rationales. For both, the total number of rationales is significantly bigger than the number of severity rationales or hazardous event descriptions. This indicates a bigger variety.

Table 3. Exemplary set of controllability rationales

No.	*Controllability Rationale*
1	Difficult to control for an average driver.
2	Most of drivers will brake/steer to avoid collision.
3	The driver can reduce the acceleration request and/or is able to increase the steer angle.
4	Driver has to steer slightly and/or reduce throttle to control this situation. Situation is slightly better to control than with 2WD.

In the following, only the results of the sentence structure analysis of the controllability rationales are presented. Each sentence was considered separately, and in total 461 different sentences were analyzed. One fourth of the sentences contains at least one subordinate clause (25.6 %). The majority of the sentences is formulated in present tense (92.4 %). Only a small portion used the present progressive, the past tense, or the future tense. In addition to that, much more active voice (88.7 %) is used than passive voice. In 66.4 % of the sentences, modal verbs are used to express obligations or abilities.

Every sentence contains at least a subject and a predicate. In our case, the predicate of a sentence corresponds to the main verb and any auxiliaries (e.g. modal verbs or adverbs) that accompany it [13]. The dependents of the predicate were analyzed separately. In 80.5 % of the sentences, an object follows the predicate. The type of the object (e.g. direct object or prepositional object) was not further determined. Modifiers as the dependent of the predicate are used in 25 % of the analyzed sentences. Additionally, one fourth of the sentences contains an infinitive phrase (26.5 %) [14].

The results of the sentence structure analysis of the exposure rationales are nearly the same. The biggest differences were identified in the usage of modal verbs and infinitive phrases. Only in 20 % of the exposure rationales modal verbs are used and in 7.6 % infinitive phrases. The differences of the other values do not exceed a portion of 10 %.

4. Controlled Natural Languages

As a result of the formalization process, the controlled natural languages for the rationales of the three risk parameters are introduced in this section.

4.1. Severity Rationale

The severity parameter gives an estimation on the potential harm or damage that could be caused by the hazard in a specific operational situation. The structure of the rationales is similar to the hazardous event descriptions. Therefore, we decided to use the same grammar with minor extensions for the controlled natural language of the severity rationales. The rationales are written in a bullet-point manner. Nominal phrases are the central elements of the grammar. They can be combined with conjunctions or prepositions to formulate more complex rationales. The usage of verbs and pronouns is prohibited.

The Listing 1 contains a simplified version of the grammar definition for the hazardous event descriptions and the severity rationales.

Listing 1: Hazardous event and severity grammar

```
  bulletPoints → (initPhrases (Conjunction phrases)* ‘.’)+
   initPhrases → nominalPhrase adjunct*
       phrases → (nominalPhrase | adjunct) adjunct*
 nominalPhrase → nounPhrase | gerundPhrase
       adjunct → prepoPhrase | compPhrase
    nounPhrase → Determiner? adjPhrase? Noun nominal*
  gerundPhrase → Determiner? adjPhrase? Gerund nominalPhrase?
     adjPhrase → Adverb* Adjective+ (Conjunction adjPhrase)*
       nominal → Noun | Gerund
   prepoPhrase → ‘not’? Preposition nominalPhrase
    compPhrase → asPhrase | thanPhrase
      asPhrase → ‘not’? ‘as’ adjPhrase
    thanPhrase → adjPhrase ‘than’ (adjPhrase | nominalPhrase)
```

The production rules of the grammar are written with a small initial letter and lexer rules with the first letter capitalized. Lexer rules contain a set of terminal words. In our case, a lexer rule contains all words of a part of speech that are contained in the vocabulary of the controlled natural languages. Terminal symbols are surrounded by single quotation marks.

A single description or rationale contains at least one noun or gerund phrase and can be extended by additional prepositional phrases or comparative phrases. Furthermore, it is possible to conjoin additional phrases with conjunctions to create longer sentences. A noun phrase contains at least one noun, and additional modifiers or a determiner can be subjoined. A gerund phrase might also have an optional determiner and an optional adjective phrase (AP) that are put in front of a gerund. After the gerund, an additional nominal phrase may be attached. The adjective phrase contains at least one adjective (JJ) which can be modified with preceded adverbs (RBs). Furthermore, it is possible to conjoin several adjective phrases with conjunctions.

Two different types of comparative phrases are part of the controlled language. The first type uses the word ‘as’ followed by an adjective phrase. The other type starts with an adjective phrase in comparative form followed by the word ‘than’ and either an adjective phrase, a noun phrase, or a gerund phrase [14].

The severity rationales 1 and 3 of Table 1 already conform to the grammar of the controlled natural language. Figure 2 shows the classification of the first example into the parts of speech [15].

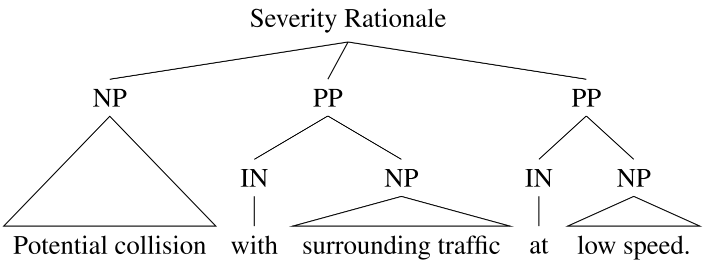

Figure 2. Severity rationale written in the CNL

4.2. Controllability Rationale

The controllability describes the ability of the driver or other traffic participants to retain sufficient control of the hazardous event to prevent the resulting harm. The major part of the rationales were formulated by using full sentences. The structure of the single sentences was analyzed resulting in the simplified grammar definition in Listing 2.

Listing 2: Controllability grammar

```
     sentences → (sentence (Conjunction sentence)* ‘.’)+
      sentence → subject verbPhrase (infPhrase | compPhrase)*
       subject → subjectElement (Conjunction subjectElement)*
subjectElement → nominalPhrase prepoPhrase*
    verbPhrase → verb (object | adjPhrase)?
          verb → (ModalVerb | AuxiliaryVerb)? Adverb* Verb
        object → objectElement (Conjunction objectElement)*
 objectElement → (nominalPhrase | prepoPhrase) prepoPhrase*
     infPhrase → ‘to’ BaseFormVerb object? adjPhrase?
    compPhrase → adjPhrase ‘than’ adjPhrase? object
```

A rationale contains at least one sentence, but it is also possible to compound more sentences. Each sentence starts with a subject and a predicate. A subject element is a nominal phrase with optional prepositional phrases. The subject contains at least one subject element, and additional subject elements can be conjoined with conjunctions. The predicate is a verb phrase (VP) that starts with a verb. The verb might have an auxiliary verb or a modal verb to formulate abilities or obligations, and additionally it is possible to modify the verb with adverbs. Moreover, it is possible to extend the verb phrase with an object or an adjective phrase. An object element is a nominal phrase or a prepositional phrase that can be extended with additional prepositional phrases. Object elements can be conjoined with conjunctions.

Infinitive phrases (IP) and a comparison phrases (CP) can be appended to the sentence to construct more complex expressions. The infinitive phrase starts with the word “to” followed by a verb in its base form. Then, an optional object and an optional adjective phrase can be appended. The comparison phrase starts with an adjective phrase in comparative form followed by the word ‘than’, another optional adjective phrase, and an object.

Figure 3 shows an example of a controllability rationale according to the controlled natural language. The example contains a single sentence with an object and an infinitive phrase.

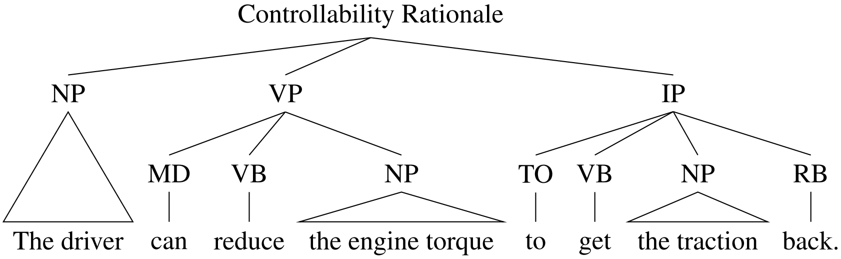

Figure 3. Controllability rationale written in the CNL

4.3. Exposure Rationale

The exposure parameter describes the estimation of the probability of being exposed to the hazard in terms of time and location. The rationale for justifying the selected value can be formulated using a combination of both created controlled natural languages.

Listing 3: Exposure grammar

```
rationale → (bulletPoints | sentences)+
```

Figure 4 shows an example of an exposure rationale that is according to the controlled natural language. The example contains a bullet-point phrase followed by a single sentence with an adjective phrase and an infinitive phrase.

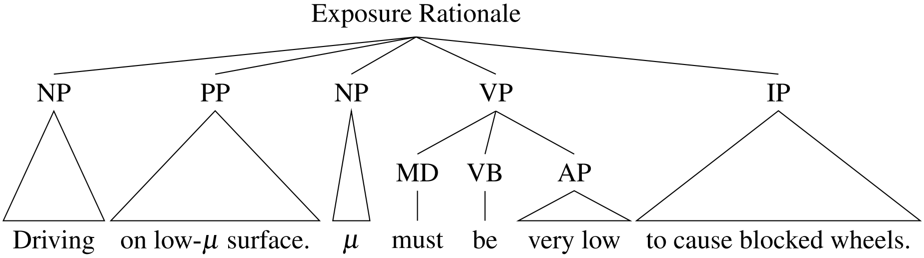

Figure 4. Exposure rationale written in the CNL

4.4. Vocabulary

The controlled languages for the hazardous event descriptions and for the three risk parameter rationales share the same vocabulary. It arose from the used terms in the given HARA documents. In a first version all used terms were added to the vocabulary. Afterwards, the vocabulary was partitioned into sets of terms with equivalent semantics [16]. For every set, only one representative was selected to remain as part of the vocabulary. Synonyms and terms with meanings that overlap widely enough are regarded as equivalent. The first part was determined by the help of existing thesauri, and the domain-specific meanings were specified by domain experts. The terms 'big' and 'large' are synonym, and for example the terms 'non-motorist' and 'child' are also equivalent in our domain-specific case. The reason for this is that the distinction between traffic participants should only be made between motorized and non-motorized participants. Further details like the age of the participants should not be taken into account while rating the hazardous event.

5. Evaluation

The newly created controlled natural languages for the rationales have been evaluated against the provided data to show that the languages are highly related to the already written rationales.

More than a half of the severity rationales (62.9 %) was written in a bullet-point manner. 116 out of these 176 rationales were compliant to the CNL (65.9 %). It was possible to translate another 45 severity rationales into a correct form by replacing a synonym with the corresponding word that is part of the vocabulary (25.6 %). The major part of the controllability rationales was already formulated using full sentences (84.6 %). Again, after replacing the synonyms, 126 out of 347 rationales are in line with the created CNL (36.3 %). More than the half of the 351 exposure rationales is already conform to the new controlled language (54.7 %). The remaining rationales of the three risk parameters can all be translated into a semantically equivalent version.

The translations were performed manually, and in the following, two examples are shown for rationales written in a bullet-point manner and using full sentences. The severity rationale in row 4 of Table 1 is not conform to the controlled natural language. One possibility is to translate each sentence separately resulting in the rationale "Vehicle movement into the path of oncoming traffic. Possible side collision with speed greater than 35 km/h.". Another possibility is to describe the relation between these two sentences in more detail. The second sentence is a consequence of the first one, and therefore, the translation "Possible side collision with speed greater than 35 km/h due to vehicle movement into the path of oncoming traffic." might be better.

Row 1 of Table 3 contains a controllability rationale that is not correct with respect to the new CNL. The rationale is not a complete sentence since the subject and the verb are missing. Adding the missing parts results in the correct sentence "The situation is difficult to control for an average driver.".

In addition, the new languages were prototypically applied in hazard analyses and risk assessments for new systems within the domains steering, fuel cell, and powertrain to make first experiences in a productive usage just like the CNL for the hazardous event descriptions [5]. The same results were made for the languages of the rationales. After extending the vocabulary, it was possible to write the rationales conform to the CNLs.

6. Conclusion and Outlook

The formalization of the rationales for the severity, exposure, and controllability classification extends the set of controlled natural languages for the hazard analysis and risk assessment activity according to ISO 26262. During the analysis of the severity rationales, it turned out that the structure of the rationales is similar to the hazardous event descriptions. Therefore, it was possible to reuse the controlled natural language for the hazardous event descriptions [5].

The controllability rationales differ in their structure comparing to the severity rationales and hazardous event descriptions. The major portion is written in full sentences. The single sentences were further analyzed to determine a common structure. Based on these results, a new controlled natural language for justifying the chosen controllability parameter was developed.

The structure of the exposure rationales is bipartite. Bullet-point phrases and full sentences were nearly equally used to reason the exposure value. Thus, it was possible to use a combined version of the two controlled natural languages.

Altogether, two different controlled natural languages were developed. The bullet-point manner controlled natural language (BP-CNL) is used to describe the hazardous events and severity rationales. The full sentence controlled natural language (FS-CNL) enables to formulate the controllability rationale in a structured way. A combination of both languages serves as the formalization of the exposure rationales. The languages share the same vocabulary, which evolved from the given HARA documents and needs to be extended beyond this scope.

During the evaluation, it was possible to translate every rationale of the provided HARA documents into the respective controlled natural language as exemplarily shown. The manually performed translation example of the severity rationale shows that it is possible to translate it into two different correct versions depending on the understanding. The second translation connects the two sentence in a semantically way, whereas the first translation keeps the two sentences unrelated. This example shows that further means need to be developed to be able to determine the similarity for sentences of the controlled natural language. In this case, the used words are nearly the same in the two rationales, which might be a first simple and suitable method to calculate a similarity score.

In a next step, the set of CNLs shall be implemented within a prototype tool to simplify the usage. The prototype tool can then be used to further examine and improve the concept of the languages. Furthermore, a case study should be performed to gather more user experiences and to show the benefits of the concept.

References

[1] International Organization for Standardization: ISO 26262: Road Vehicles – Function Safety (2011)

[2] International Organization for Standardization: ISO 26262-3: Road Vehicles – Function Safety – Part 3: Concept Phase (2011)

[3] Kittredge, R. I.: Sublanguages and Controlled Languages. In: The Oxford Handbook of Computational Linguistics, pp. 403–447. 2nd edition (2003)

[4] Kuhn, T.: A Survey and Classification of Controlled Natural Languages. Computational Linguistics, 40(1):121–170 (2014)

[5] Chomicz, P., Müller-Lerwe, A., Wegner, G.-P., Busch, R., Kowalewski, S.: Towards the Use of Controlled Natural Languages in Hazard Analysis and Risk Assessment. Automotive-Safety & Security-Sicherheit und Zuverlässigkeit für automobile Informationstechnik, pp. 163–174 (2017)

[6] Jang, H. A., Kwon, H. M., Hong, S.-H., Lee, M. K.: A Study on Situation Analysis for ASIL Determination. Journal of Industrial and Intelligent Information, 3(2):152-157 (2015)

[7] Pool, J.: Can Controlled Languages Scale to the Web?. In: Proceedings of the 5th Int. Workshop on Controlled Language Applications (2006)

[8] Tommila, T., Antti, P.: Controlled Natural Language Requirements in the Design and Analysis of Safety Critical I&C Systems. SAFIR2014 Reference Group 2 (2014)

[9] Luo, Y., van den Brand, M.G.J., Kiburse, A.: Safety Case Development with SBVR-based Controlled Language. In: Model-Driven Engineering and Software Development. pp. 3–17 (2015)

[10] Kamprath, C., Adolphson, E., Mitamura, T., Nyberg, E.: Controlled Language for Multilingual Document Production: Experience with Caterpillar Technical English. In: Proceedings of the Second International Workshop on Controlled Language Applications, pp. 51–61 (1998)

[11] Lee, A.: Controlled English with and without Machine Translation. In: Aslib Proceedings, 46(5):131–133 (1994)

[12] Crabbe, S.: Controlling Language in Industry: Controlled Languages for Technical Documents. Palgrave Macmillan (2017)

[13] Meyer, P. G. et al.: Descriptive English Linguistics. Gunter Narr Verlag (2008)

[14] Radford, A.: An Introduction to English Sentence Structure. Cambridge University Press (2009)

[15] Brill, E.: Part-of-Speech Tagging. Handbook of Natural Language Processing, pp. 403–414 (2000)

[16] Svenonius, E.: Design of Controlled Vocabularies. Encyclopedia of Library and Information Science, 45(10):82–109 (1989)