UDC 519.686

I. BISCOGLIO, M. FUSANI

Systems & Software Evaluation Centre, ISTI – CNR, Pisa, Italy

REDUCING TEXTUAL AMBIGUITY RISK IN HIGH-IMPACT STANDARDS

Safety-related standardsindirectly impact into people's safety and environment integrity. The quality of these standards plays an important role in their correct and productive adoption. The paper is concerned with the analysis of the way standards are written, and in particular with the results of an automated textual inspection of five safety-related standards, aimed to discover possible inherent ambiguity of textual expressions. The analysis suggested that useful advice could be given to standard-making committees. Results of the analysis are shown and discussed.

Key words*: standard, error, fault, failure, glossary, safety.*

INTRODUCTION

High-impact standards are those that most deeply influence the system and software lifecycle of safety-related products and services. Adoption of such standards is mostly obliged by law and Authorities and sometimes is part of procurement contracts. So, both engineering and management processes involved in system development can be affected by possible misinterpretation of requirements coded in such standards, with possible risk of compromising safety of humans and environments.

This work arises from the apparently trivial research questions: "Are standard-defined requirements (also denoted as clauses) such that the organizations entitled to adopt them can easily understand what to do to be conformant?" [4, 7, 22].

The answer: "Of course they are, because safety-related standards have been there for many years and they are thoroughly and repeatedly revised by a wide international community of experts" should not be taken as totally satisfying.

In fact, most standards present their requirements in natural language (NL). Although NL is the most common and immediate way to express software requirements in general, however is alsoexposed to the risks of ambiguity, imprecision andsubjectivity.For this aim, several studies have defined methodologies and proposed tools for the analysis of NL requirements(e.g. [1, 3, 7, 8, 16, 17, 19, 23]).

In [3] various types of ambiguity were addressed and classified into linguistic, lexical, syntactic, semantic and pragmatic.It should be noted that this classification is not mutually exclusive, because the ambiguities occurring in a text may be a combination of several types.

We argue that detecting ambiguities in standards clauses by NL analysis is important because possible ambiguity in standard texts may impact on their understanding and adoption, and, consequently, on the products to be evaluated and certified according to those international standards.

Studying ambiguity risks in NL requirements has been for years a research work at the authors' Centre, that has started from software requirements and then has extended the analysis to standards clauses [5, 8].

In this work, we show that interesting results can be found even by limiting our analysis scope to*lexical* ambiguity. Within this boundary, we also focus on those clauses of the standards that include frequent*keywords*. Keywords are those terms that call for their meaning to be particularlyclear and unambiguous for the organizations that adopt international standards, as a recommendation says:

"A [requirement document] is unambiguous if, and only if, every requirement stated therein has only one interpretation… In cases where a term used in a particular context could have multiple meanings, the term should be included in a glossary where its meaning is made more specific." [12, p.4-5].

Actually, standard makers generally adopt this rule, but perhaps they have not always investigated enough on the consistency of the definitions throughout the whole standard text.

In this work we considered the glossaries and the texts of a sample of five safety-related standards covering different application domains: railway [6], nuclear plants [11], automotive [14], avionics [20], general [10](with the important exception of machinery and medical, which we could not investigate so far due to limited resource availability) for their high impact on society and economy. Subsequently, we chose a sample of keywords, namely: *fault*, *failure* and *error*as keywords for their significant mutual relationship [2, 13].

Starting from *fault*, *failure* and *error*, we wanted to explore, in every standard, the correspondence between the keywords defined in the glossary and those used in the standard texts.In particular, we wanted to detect possible undefined keywords, which could create ambiguity of understanding.One result of this work is to highlight, by lexical analysis,possible keywords that were not defined in the glossary so that their meaning is left to common sense and then is uncertain.

The purpose of this analysis is therefore the detection of textual consistency within the standards texts. As a result of the analysis newentriescould be added to the standards glossaries according to the ISO/IEC Directives: "Any term which is not self-explanatoryor commonly known and which can be differently interpreted in different contexts shall be clarified by defining the relevant concept" [15, p.51]

From this point of view, the results could be useful, first of all,for authors of safety-related standard and, gradually, for Certification/Accreditation bodies and for intermediate/end users.

In this paper we do not tackle the problem of semantic consistency directly, but we are aware that semantics is behind the necessity of using glossaries.

In Section II our experiment is shown, by presenting the different steps of work and the respective results. In Section III the results are discussed and some conclusions drawn.

THE EXPERIMENT

As above reported, in a NL text, the ambiguity risk can be of different types [3].In this work, we limited our attention on lexical ambiguity, focusing on *keywords* and *key expressions*. If the *keyword* meaning is quite intuitive, it can be more useful to use a *key expression*, that is a set of numerically limited words that contains one keyword and identifies a new definable term. Key expressions appear as well as keywords in standards glossaries and are intended to have a unique meaning.

The starting point of our work was the study of the glossaries of five safety-related standards [6, 10, 11, 14, 20],in relation to *fault*, *failure* and *error* as keywords and to their correlated key expressions. We collected and presented *all defined terms*(both keywords and key expression) in Table 1, where the standards they belong are also shown.

Subsequently, using a technique calledConcordance Analysis [18],we examined every standard *text* in order to survey a textual correspondence between keywords / key expression defined in the glossary and those used in the text. This allowed to find, for each standard, those keywords and key expressions *not defined in the standard glossary but in other* glossaries. These are presented, grouped by standard, in Tables 2 – 6. This fact revealspossible incompleteness of the standard glossaries.

Keywords and key expressions *used in the standard texts but not defined by any glossaries* are collected in Table 7. These could represent new possible definable terms to be included in the considered standards glossaries.

Below the different steps of work are presented.

A. Keywords and Key Expressions across standards

In Table 1 we marked the presence of a definition for the three keywords and for the correlated key expressions collected from all five standards.

It is evident thatthe IEC 61508-4 and the ISO 26262-1glossaries appear richer, more complex and detailed than the others.

B. Keywords and Key Expressions inside every standard

Table 1 gives a global and approximate measure of the detail level covered by the glossaries. Inside every standard, this coverage changes and the glossaries are differently articulated.

Regarding the problem of determining consistency between the glossary and the text body of eachstandard, relating to *fault*, *failure* and *error*, we may ask if undefined keywords and key expressions exist that are used in the text. Eventual findings could open the doors to ambiguous interpretations.

Then, after considering the glossaries, we analyzed the text of every standard using the Concordance Analysis performed by Wordsmith Tool Suite [21]. By this analysis, we can find the keywords together with "some" adjoining words so that the former may be seen in their use context. The range of considered words is defined by the researcher and, in our work, in section C is shown. From the results of this analysis, we can observe the use of specific keywords, the sequences of words that contain them and the occurrence frequencies of keywords and key expressions. We also decided to limit our investigation to keywords and key expressions listed in Table1.

Table 2 – 6 present, for every considered standard, keywords and key expressions (always containing *fault*, *failure* and *error*)*that appear in the text but are undefined in the corresponding glossary*. For standards consisting of different parts (except for IEC 60880 of which we have only the part 2), also the parts containing the reported sequences of words are shown.

We can argue from this analysis that in ISO 26262 there is more textual consistency between its glossary and its text, although *fault tolerance* is not defined. In contrast, CEI EN 50128 or IEC 61508 show important uncovering: for example, in the former, the missing definition for *failure Rate* or for *Common Cause Failure*, and in the latter, the missing definition for *Failure Mode*.

Table 1

Keywords and key expressions defined per standard

	CEI EN 50128	IEC 61508-4	ISO 26262-1	IEC 60880-2	DO 178B
ERROR	X	X	X		X
Human Error				X	
Soft-Error		X			
FAILURE	X	X	X	X	X
Cascading Failure			X		
No Part Failure		X			
No Effect Failure		X			
Failure Mode			X		
Failure Rate		X	X		
Single-point Failure			X		
Dual-point Failure			X		
Multiple-point Failure			X		
Failure Condition					X
Random Hardware Failure (s)		X	X		
Systematic Failure		X	X		
Dangerous Failure		X			
Safe Failure		X			
Safe Failure Fraction		X			
Independent Failure(s)			X		
Dependent Failure(s)		X	X		
Common Cause Failure (s)		X	X	X	
Target Failure Measure		X			
Probability of dangerous failure on demand		X			
Average Probability of dangerous failure on demand		X			
Probability of dangerous failure per hour		X			
FAULT	X	X	X	X	X
Detected Fault			X		
Single-point Fault			X		
Dual-point Fault			X		
Multiple-point Fault			X		
Multiple-point Fault Detection Interval			X		
Perceived Fault			X		
Permanent Fault			X		
Residual Fault			X		
Fault Model			X		
Latent Fault			X		
Safe Fault			X		
Systematic Fault			X		
Transient Fault			X		
Fault Reaction Time			X		
Fault Tolerant Time Interval			X		
Fault Avoidance	X	X			
Fault Tolerance	X	X			X

Table 2

CEI EN50128: new keywords and key expressions

Detected *Fault*
Systematic *Fault*
Failure Rate
Common Cause *Failure* (s)
Human *Error*

Table 3

IEC 61508: new keyword and key expressions

Detected *Fault*	Parts 6,7
Residual *Fault*	Part 3
Fault Model	Part 2
Systematic Fault	In all parts
Transient*Fault*	Part 2
Cascading/Cascade *Failure*	Part 6
Failure Mode	Part 7
Single-point *Failure*	Part 7
Failure Condition	Part 3
Independent *Failure* (s)	Part 6
Human *Error*	Part 1, 2

Table 4

DO178B: new keyword and key expressions

Failure Mode
Failure Rate

Table 5

IEC 60880-2: new keyword and key expressions

Systematic *Fault*
Failure Condition
Error

Table 6

ISO 26262: new keyword and key expressions

*Fault*Tolerance	Parts 3, 4

C. New emerging terms

We noticed that the concordance analysis pointed out *new* recurring sequences of words providing suggestions on possible integrations in considered glossaries.

We chose to delimit our research in two directions:

1. Maximum number of words: starting from *fault*, *failure* and *error*, we searched concordances limiting to max 7 words (4 to the left of the keyword + 3 to the right of the keyword) in according to the longest key expression found in the considered glossaries, that is *Average Probability of dangerous failure on demand* [10].

2. Frequency of the new sequences of words: we considered new sequences of words that occurred at least 3 times in the standard text.

Obviously, we excluded sequences of words with *fault*, *failure* and *error* interrupted by punctuation, sentence break and section break, numbers and conjunction.

Below we can observe the discussed sequences of words with the note of the parts of standards that contain them.

The new detected sequences of words (Table 7) could be indicated as new possible key expressions to be included in the standardglossaries. Such inclusion should be suggested to safety experts and standard makers and by them defined.

It is also noted that some undefined sequences of words appear in the standards among the Techniques and Measures (for example *error guessing* and *error seedin*gin the part 7 of IEC 61508). However, this is not true for all of them.

CONCLUSIONS

The paper presented some findings from atextual consistency analysis of five safety-related standards, limited to the terms: *fault*, *failure* and *error*. This analysis compared the occurrence of the terms in each standard body with that in the related glossary section.

Some uncovered terminological issues were found, that is keywords and key expressions are used in some standard texts but are defined in other standards glossaries. Besides, lexical analysis isolated undefined, recurrent sequences of words, suggesting the opportunity of their introduction as new glossary entries, possibly according to the rules of [15].

The proposed experiment is just an example of a possible methodology that could be adopted by standard makers to answer the research question cited in the Introduction: “Are standard-defined requirements (also denoted as clauses) such that the organizations entitled to adopt them can easily understand what to do to be conformant?”. Beyond this specific case, NL analysis applied to safety-related standards can mitigate the risk of ambiguity and misinterpretation in a such sensitive area.

We also argue that these results might be the basis for considering the possibility of a unique glossary for the safety-related domain. Much more work would be necessary to extend textual analysis to all the terms and word sequences that in this domain may be considered as keywords and key sentences, as well as to perform textual consistency checks within a standard body. However it could be an interesting activity to carry out towards better disambiguation, on which to invest time and resources.

Table 7

Undefined Keywords

	EN 50128	IEC 61508	ISO 26262	IEC 60880	DO 178B
ERROR					
Error Effect	X				
Error Detecting and Correcting Codes	X	X(Part 7)	X (Parts 5,6)		
Error Seeding	X	X (Parts 3,7)			
Error Guessing	X	X (Parts 3, 7)	X(Part 4)		
Error Detection	X	X(Part 7)	X (Parts 5,6)		X
Error Prevention					X
Error Sources					X
Error Rates					X
Equivalent Error					X
Error Handling		X (Part 6)			
Error Prone	X	X (Part 7)			
FAILURE					
Failure Assertion Programming	X	X(Parts 2,3,6,7)			
Failure Detection		X(Parts 2,3,6,7)	X (Part 5)		
Target Failure		X (Parts 1,3)			
Failure Mechanisms		X (Part 3)			
Failure On Demand		X (Parts 1,5,6)			
Element Failure			X (Part 5)		
Hardware Element Failure			X (Part 5)		
Failure Assumption			X (Part 5)		
Severe Failure					X
FAULT					
Fault Tree	X	X (Parts 2,3,5,6,7)			
Fault Detection	X	X(Parts 6, 7)	X (Part 3)		X
Fault Correction	X	X (Parts 3,6,7)			
Fault Simulation		X (Part 7)			
Software Fault		X (Parts 2,7)		X	
Generic Fault			X (Part 5)		
Fault Recovery	X	X (Parts 6,7)			
Intelligent Fault	X	X (Part 7)			
Fault Injection			X (Part 4)		
Retry Fault		X (Part 7)			
Fault Coverage					X
Fault Effect			X (Part 6)		
Design Fault	X	X (Part 3)			

REFERENCES

1. Ambriola, V. The Circe approach to the systematic analysis of NL requirements [Text] / V. Ambriola, V. Gervasi. – TR-03-05, University of Pisa, 2003.

2. Basic Concepts and Taxonomy of Dependable and Secure Computing [Text] / A.Avizienis, J.-C. Laprie, B. Randell, C.Landwehr // IEEE Trans. Dependable and Secure Computing. – Jan.-Mar. 2004. – Vol. 1, no. 1. – P. 11 – 33,

3. Berry, D.M. From contract drafting to software specification: Linguistic sources of ambiguity [Text] / D.M. Berry, E. Kamsties, M.M. Krieger. – TR, University of Waterloo, 2003.

4. Biscoglio, I. Analyzing Quality Aspects in Safety-related Standards [Text] / I. Biscoglio, M. Fusani // Proceedings NPIC&HMIT 2010,Las Vegas, Nevada, November 7-11. – P. 1741 – 1748.

5. An approach to Ambiguity Analysis in Safety-related Standards [Text] / I. Biscoglio, A. Coco, M. Fusani, S. Gnesi, G. Trentanni // Procedings of QUATIC 2010, Porto, Portugal. – P. 461 – 466.

6. CENELEC - EN 50128 – Railway applications – Communications, signalling and processing

systems – Software for railway control and protection systems [Text] / CENELEC, 2002.

7. Fenton, N. A Strategy for Improving Safety Related Software Engineering Standards [Text] / N. Fenton, M.Neil // IEEE Transactions on Software Engineering. – 2002. – Vol. 24. – P. 1002 – 1013.

8. An Automatic Tool for the Analysis of Natural Language Requirements [Text] / S. Gnesi, G. Lami, G. Trentanni, F. Fabbrini, M.Fusani // Int. Journal of Computer Systems Science and Engineering, Special issue on Automated Tools for Req. Engineering. CRL Publishing Ltd. Leicester, UK. Volume 20 No 1, January 2005.

9. Hooks, I. Writing Good Requirements [Text] / I. Hooks // Proc/ of the Fourth International Symposium of the NCOSE 2, San Jose, CA, 1994. – P. 197 – 203.

10. IEC 61508, Functional safety of electrical/ electronic/programmable electronic safety-related systems, Part 3, Software requirements [Text] / IEC, 1997.

11. IEC 60880-2, Software for Computers in the Safety Systems of Nuclear Power Stations – Software aspects of defence against common cause failures, use of software tools and of pre-developed software [Text] / IEC, 2000.

12. IEEE Std 830-1998 [Text]. – IEEE Recommended Practice for Software Requirements Specification., 1998.

13. IEEE Std 610.12-1990 [Text]; IEEE Standard Glossary of Software EngineeringTerminology. 1990.

14. ISO DIS 26262, Road vehicles — Functional safety [Text], BL19:2010, Parts 1-10.

15. ISO/IEC Directives [Text], Part 2, 2004.

16. Automated review of natural language requirements documents: generating useful warnings with user-extensible glossaries driving a simple state machine [Text] / P. Jain, K. Verma, A. Kass, R.G. Vasquez // Proceedings of ISEC 2009, ACM, 2009. P. 37 –46..

17. Requirements for tools for ambiguity identification and measurement in natural language requirements specifications [Text] / N. Kiyavitskaya, N. Zeni, L. Mich, D.M. Berry // Requir. Eng. – 2008. – Vol. 13, no. 3. – P. 207 – 239.

18. Manning, C. Foundations of Statistical Natural Language Processing [Text] / C. Manning, H. Schutze. – Cambridge, 1999, MA: MIT Press.

19. Mich, L. Ambiguity measures in requirement engineering [Text] / L. Mich, R. Garigliano // Feng Y., Notkin D., Gaudel, M., eds.: Proceedings of ICS2000, Sixteenth IFIP World Computer Congress, Beijing, Publ. House of Electronics Industry, 2000. – P 39 – 48.

20. RTCA DO-178B, Software considerations in airborne systems and equipment certification [Text] / RTCA, 1992.

21. Scott, M. WordSmith Tools version 5 [Text] / M. Scott. – Liverpool: Lexical Analysis Software, 2008.

22. Tuohey, W. Benefits and Effective Application of Software Engineering Standards [Text] / W. Tuohey. – Software Quality Journal. – 2002. – Vol. 10, Kluwer Academic Publishers. – P. 47 – 68.

23. Wiegers, K.: Software Requirements [Text] / K. Wiegers. – Microsoft Press, 2003.

Поступила в редакцию 8.02.2013, рассмотрена на редколлегии 6.03.2013

Рецензент: д-р техн. наук, проф., зав. каф. компьютерных систем и сетей В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

СНИЖЕНИЕ РИСКА НЕОПРЕДЕЛЕННОСТИ В ТЕКСТАХ СТАНДАРТОВ БОЛЬШОГО ВЛИЯНИЯ

И. Бисколью, М.Фузани

Стандарты, относящиеся к безопасности, косвенно влияют на безопасность людей и окружающей среды. Качество таких стандартов играет важную роль при их правильном и продуктивном принятии. Статья посвящена анализу способа написания стандартов и, в частности, результатам автоматизированной проверки текстов пяти стандартов, относящихся к безопасности, с целью выявить возможную неустранимую неясность текстовых описаний. Проведенный анализ показал, что для комитетов по созданию стандартов могут быть даны полезные советы. В работе описываются и обсуждаются результаты анализа.

Ключевые слова – стандарт, ошибка, сбой, отказ, глоссарий, безопасность.

ЗНИЖЕННЯ РИЗИКУ НЕВИЗНАЧЕНОСТІ В ТЕКСТАХ СТАНДАРТІВ ВЕЛИКОГО ВПЛИВУ

І. Бісколью, М.Фузані

Стандарти, пов'язані з безпекою, опосередковано впливають на безпеку людей і цілісність навколишнього середовища. Якість таких стандартів грає важливу роль при їх правильному і продуктивному прийнятті. Стаття присвячена аналізу способу написання стандартів і, зокрема, результатам автоматизованої перевірки текстів п'яти стандартів, пов'язаних з безпекою, з метою виявити можливу неусувну неясність текстових описів. Проведений аналіз показав, що для комітетів по створенню стандартів можуть бути дані корисні поради. У роботі описуються й обговорюються результати такого аналізу.

Ключові слова – стандарт, помилка, збій, відмова, глосарій, безпека.

Biscoglio Isabella – a post doc at CNR-ISTI since 2007, Systems & Software Evaluation Centre, ISTI – CNR, Pisa, Italy, e-mail: isabella.biscoglio@isti.cnr.it.

Fusani Mario has been with the National Research Council (CNR) of Italy since 1973, Systems & Software Evaluation Centre, ISTI – CNR, Pisa, Italy, e-mail: mario.fusani@isti.cnr.it.