Acta Polytechnica CTU Proceedings **5**:1–3, 2016
doi:10.14311/APP.2016.5.0001

PROBLEMS OF EN 50 128:2011 RAILWAY STANDARD

Tomáš Brandejský

Czech Technical University in Prague, Department of Applied Informatics in Transportation, Faculty of Transportation, Praha, Czech Republic

correspondence: brandejsky@fd.cvut.cz

Abstract. The second version of railway standard EN50128:2011 published by CENELEC is used for five years and thus the CENELEC reasons about preparation of new version of this standard are coming, because the CENELEC defined 10-year cycle of its standards innovation. The paper discusses some observations of problems of this standard application from the position of safety assessor which gives us the contact with developers applying this standard into the real railway products.

Keywords: Railway software applications, assessment, safety, reliability, accessibility, maintainability, development.

1. Introduction

Since the origin, the group of CENELEC's railway stands [1] [2] [3] was declared as standard of all safety related railway applications including not only interlocking systems, but rolling stock and related communication too.

The standard EN50126 defines its applicability to *"The specification and demonstration of RAMS for all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major systems and to individual and combined subsystems and components within these major systems, including those containing software"*.

The standard EN50128 defines its application domain as: *"This European Standard specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications. It is aimed at use in any area where there are safety implications. These may range from the very critical, such as safety signalling to the non-critical, such as management information systems. These systems may be implemented using dedicated microprocessors, programmable logic controllers, multiprocessor distributed systems, larger scale central processor systems or other architectures"*.

And the standard EN50129 defines its scope as electronic systems related to safety in application to railway interlocking systems.

It means that at least standards EN50126 and EN50128 must be reasoned in any railway system related to safety. On the beginning of application of these standards safety assessors required application of these standards especially in the domain of interlocking systems and the rest was frequently omitted. After the year 2011, when the second generation of these standards has come into the operation the situation changed and the conformity with these standards is required also by assessors of rolling stock and other railway systems. It brings some problems described below due to different requirements on system functions in situation, when the system malfunction is detected.

The main aim of the paper is the discussion of problems in nowadays application of the standard EN50128 and offering of ways how to improve it.

2. Problems of EN50128 Application

The CENELEC's standard EN 50128 *"Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems"* was defined as part of three standards group [1] [2] [3] applying standard IEC 61508 *"Functional safety of electrical/electronic/programmable electronic safety-related systems"* into the specific area of railway systems. The main difference is in different safety assessment scheme, where not only developer, validator and assessor are reasoned but also railway safety authority as next independent body. In the next chapter, particular problems will be discussed:

(1.) The last version of the standard is less transparent than original one. The change of the standard structure was asked by CENELEC due to unification of all CENELEC standard structure. Whilst the original standard was divided into 17 chapters and 2 annexes, the 2011 version is organized into 9 chapters and 4 annexes (2 are new). This change causes not only that there are no separate chapters e.g. for software validation and assessment, but software assurance chapter describing testing, verification, validation and assessment is before chapter 7 describing development process! Furthermore, the chapter 7 is named "Generic software development" now not looking that the term "generic software" in computer science doscon mean "common sense software", as this term is used in the standard, but "a class of software that can be used for a number of different purposes without requiring modification", as it is defined e.g. in [4] [5]. What is worse, the chapter 3.14 of 50128:2011 standard defines generic software meaning some way. Thus the topic of the chapter 7 does not give any sense. Similarly in the chapter v 3.1.4 of original EN50128 introduces the term "component" which is defined extremely vague (and in the EN50128:2011 even it is not defined), but especially in the area on object oriented programming the meaning of this term if defined precisely and totally different. Because the standard EN50128 is used especially by programmers, such drifting of frequent term sense might cause many misunderstandings. Because EN50128:2011 allows to understand term component also as object, module or even function, the meaning of e.g. chapter 7.5 might be understand totally different by particular people in particular situations.

(2.) There is not explicitly declared applicability of the standard to railway vehicles and especially differences in requirements to behaviours of vehicle control systems in the case of malfunction, which is opposite to required behaviours of interlocking control systems in the analogical situation. Typically, in the case of control system error vehicle must keep moving but interlocking system can signalize stop to all tracks and perform e.g. restart of the control system.

(3.) There is not solved defence against targeted attack (terrorism). Defence of mission critical systems against targeted attacks e.g. requires ability of the system to isolate attacked parts and thus to reconfigure system. It is a big problem, because dynamic reconfiguration is listed in table A.3 as technique 14 and it is not recommended non respecting fact that this technique is frequently adopted e.g. in military, cosmic or avionics systems. It is not possible to constraint this problem only to subjects of safe communication and physical barriers. On the other hand, standards of the information security like ISO 27001 are rather oriented to managing sensitive company information than to control systems located in open space and communicating across it.

(4.) The standard does not solve design of programmable HW, where on interface of SW/HW occur many specific problems which solution is not defined in the actual standard. Many of these problems were discussed in [6], like specific problems of design, timing and application structure but there also another problems like problem of dedication of safety related functions to development tools which is related to problems discusses herein in chapter (6.) and which is not solved. Design tools transforming e.g. VHDL language into configuration bit stream of the chip does not work deterministically and this fact is hard to accept in safe system design.

(5.) The standard EN50128 contains extensive appendix B "Key software roles and responsibilities" on ten pages and small appendix C "Documents control summary", which only recapitulate textual part of the standard and do not bring any additional information. It is good to delete such chapters because they only decrease clarity of the standard.

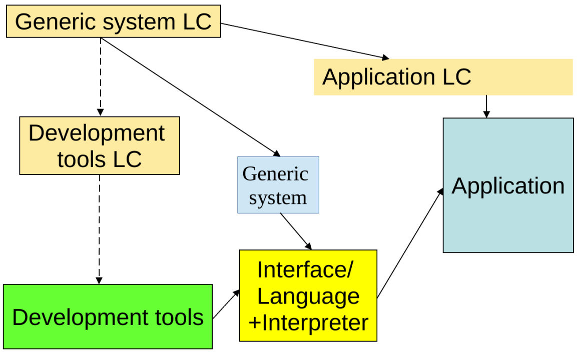

Figure 1. The example of lifecycle hierarchy of complex system.

(6.) Chapter 8 "Development of application data or algorithms: systems configured by application data or algorithms" should explain better requirements of systems with different level of configurability. It is hard to compare simple system which is configured by one dimensional table of parameters and system where safety-related functions are described in configuration language, which is interpreted in real time and where part on safety checks is dedicated to development tools. The Figure 1 draws possible configuration of different life-cycles cooperating on development of final (sometimes also generic) application based on configurable generic kernel where e.g. life cycle of generic system determines requirement on LC of final application and final application development tools life cycle.

(7.) In comparison to standard IEC 61508-3 this railway standard does not contain equivalent of IEC 61508-3 appendix C explaining which SW property is achieved by which technique. Such explanation is useful both for designers and assessors because it simplifies, objectivises and formalizes selection of design techniques in atypical, non-standard situations where groups of design techniques predefined in the table A.3 are inapplicable. Typical example of this situation is in this moment application of programmable HW, which is not solved in the standards and which requires a little bit different approach than standard HW and SW.

(8.) There is not solved problem of design of systems with Safety Integrity Level greater than 4. Growing complexity of railway systems, especially of such systems as ERTMS, tends to requirement of such SIL. It is true, that many calls for higher SILs are given by misunderstandings of SIL meaning. SIL is related to tolerable hazard rate, as it is introduced in the standard EN 50129, table A.1. Tolerable hazard rate is related to one hour and one function, but many designers of railway systems missrelates it to number of invocations of the function and means that systems working on higher operation frequency must have higher SIL. It is mistake.

(9.) There is not well defined that SILs are determined to top-level functions, not to whole system and not to any sub-functions. The standard EN50129 uses formulation single function without precision of the complexity of the function. Many top-level functions are performed by groups of lower level functions. This lack of precise definition tends to many useless discussions between manufactures and assessors.

(10.) The standard defines five different SIL levels but de facto it specifies only three different cases: SIL0, SIL1 and 2; and SIL 3 and 4. In addition, requirements to SIL 1 and 2 systems are inappropriate strict as well as there are requirements to documentation complexity of SIL0 systems, especially in comparison to COTS systems of the equal SIL level. But in fact it would be just opposite – e.g. it is need to do precise testing developed by other company, which design process is not well described, where the documentation is missing, than in the case of well documented one.

3. Discussion

Ten year cycle of CENELEC standard upgrade is difficult especially to rolling stock manufacturers. Locomotives, carriages and other vehicles have extremely long life-cycle taking any tens of years. There is long design phase including real research, own assessment phase sometimes takes about ten years and also operation is reasoned in horizon of thirty years or more. Thus the idea that between start of design and start of operation the required standard will be once or even two times changes is not acceptable. Because CENELEC does not accept this fact, rolling stock making companies provide "diverse activity" in related CENELEC work-groups and prevents significant changes of these standards. On the opposite side, above mentioned problems does not represent significant changes of the standards and their acceptance in the new generation of them might increase their applicability.

4. Conclusions

The above presented paper summarises problems on the today railway standard EN50128:2011, which were observed in certification body of Czech technical university in Prague – COV FD ČVUT v Praze during certifications of many railway systems serving especially (but not only) in Czech Republic.

References

[1] EN50126 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

[2] EN50128 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems.

[3] EN50129 Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling.

[4] http://www.teach-ict.com/glossary/G/genericsoftware.htm.

[5] http://www.computingstudents.com/dictionary/?word=Generic%20Software.

[6] T. Musil. Návrh metodiky pro vývoj a verifikaci bezpečných algoritmøu implementovaných v dynamicky rekonfigurovatelných FPGA, PhD. Thesis, 2015.