Software RAMS: the opportunity

Y. González-Arechavala, J. A. Rodríguez-Mondéjar
& G. Latorre-Lario
Instituto de Investigación Tecnológica, Escuela Técnica Superior de Ingeniería, Universidad Pontificia Comillas, Spain

Abstract

Software is in the heart of many safety critical systems in the railway sector. The development of systems that include software modules requires a correct evaluation of software RAMS (Reliability, Availability, Maintainability and Safety) to get a correct value of the overall system RAMS.

In order to obtain appropriate software, the standards propose to perform a set of activities in the different phases of software development as well as tasks to control their correct accomplishment. They ensure the developed software is of adequate quality. However, it is necessary to go further and try to obtain a quantitative measure of RAMS for each software module as is usually done in hardware development. There are several techniques for the assurance of software reliability and safety that have been in use for years and must be analysed to know their real potential: reliability growth models, artificial intelligence techniques, Markov chains, Software Fault Tree Analysis and Software Failure Mode and Effect Analysis among others.

Two circumstances emphasize the strategic time the railway sector is living and the opportunity to adopt the most promising software techniques improve reliability and safety: (1) The development of high-performance railway networks that interconnect different countries and the liberalization and opening of the national markets demand new European global agreements. In this regard, the European Railway Agency has asked its Safety Unit to develop the new Common Safety Methods (CSM) and Common Safety Targets (CST) to be used in all European countries; (2) The IEC 61508-3 standard (from which some parts of CENELEC 50128 are derived) is now under revision, with the primary aim of ensuring the safety of the developed software by hardening the requirements and promoting the use of the most promising techniques.

Keywords: software safety, software reliability, RAMS, railway standards.

WIT Transactions on The Built Environment, Vol 103, © 2008 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR080141

1 Introduction

In the present world, our professional and private lives are surrounded by systems governed by software programs. Moreover, software is in the heart of many safety critical systems in the industrial sector. However, this meteoric rise of software applications has not been accompanied by the indispensable evolution in its development process in order to have total confidence in it.

The development of systems that include software modules requires a correct evaluation of software RAMS to get a correct value of the overall system RAMS. But how do we evaluate software RAMS? Moreover, what techniques should we use in order to provide the software with the best RAMS values?

To obtain safe and reliable software, most of the standards propose to perform a set of activities in the different phases of software development as well as tasks during the development to control their correct accomplishment. These standards include the generic safety norm IEC 61508 [1], as well as the CENELEC standards for the railway sector EN 50126 [2], EN 50128 [3] and EN 50129 [4].

Development activities and control tasks seek to ensure that the developed software is of adequate quality, sufficient to reach the required degree of confidence. But it is necessary to go further on and try to obtain a quantitative measure of safety and reliability for each software module, as is the usual practice in hardware development. In fact, there are several techniques that have been in use for years, although the standards do not reflect them as mandatory.

This paper emphasizes the intrinsic characteristics of software and briefly defines system RAMS in the first place. Then, it gives an overview of the current state of the standards regarding software RAMS, bringing to attention the strategic moment that faces the railway industry with the ongoing unification and opening of the railway market. In this respect, the paper highlights the development of CSMs and CSTs within the European Union, as well as the most significant improvements that the second edition of the standard 61508-3 includes. Finally, it enumerates a series of new techniques which would be interesting to analyse thoroughly so as to confirm the quantitative and qualitative improvements that their application brings in terms of reliability and safety.

2 Software RAMS

It is a fact that the techniques used nowadays for the evaluation of hardware RAMS indicators are much more advanced and provide measures closer to the actual system performance than software RAMS indicators. Given the increasing importance of software components in the overall values of RAMS of a system, this represents one of the more active research areas.

In order to understand this, it is necessary to highlight some of the most significant characteristics that make hardware and software inherently different and partially explain the uneven evolution of techniques for the evaluation of

RAMS indicators in hardware and software. The following differences are among the most significant ones:

- In hardware components, physical connections are established when the system is designed and remain unchanged during operation. However, in software components connections among the different modules are "chosen" while the system is operating, normally depending on the different values of input data. Connections in software systems are logical ones, which implies that multiple connections are possible, making it harder to analyze the whole component and carry out a complete testing of it. In this respect, we could argue that the flexibility associated with software turns out to be an additional problem in terms of safety and reliability assurance.
- As a result, given the problems that arise when analyzing and testing software components, it is of the utmost importance to avoid errors in the specification of requirements. It has been proved that a high percentage of software failure is due to an inaccurate specification, to an erroneous interpretation of the desired operation of the system, to a lacking specification regarding the performance of the system under certain operating conditions, or to a specification which can lead to system hazards.
- The interpretation and conversion of requirements when carrying out the design and subsequent implementation of the system is another important source of system failure.
- In many occasions, software experts are not sufficiently knowledgeable in system safety and reliability, and the other way round, engineers whose area of expertise is system safety and reliability are not software experts. However, most companies nowadays employ a group of experts in RAMS who are in charge of the control of all the elements involved, which minimizes the problem.

At this point, it is necessary to briefly define the four characteristics comprised by the term RAMS so that the focus of this discussion can be shifted to the current state of affairs regarding RAMS in the railway industry:

- Reliability (R): is defined in Storey [5] as 'the probability of a component, or system, functioning correctly over a given period of time under a given set of operating conditions' i.e. the probability that a system will perform the functions it was intended for when operated in a specified manner under specific conditions, for a specified length of time and for a specific purpose.
- Availability (A) of a system is defined in Storey [5] as 'the probability that the system will be functioning correctly at any given time' i.e. the probability to perform the operations that are required from it whenever they are requested. This characteristic is closely related to system reliability: for a system to be reliable, that is, for it to operate according to its specifications, it will have to deliver the services that are required from it at any given time.
- Maintainability (M) in Storey [5] is defined as 'the ability of a system to be maintained' and 'Maintenance is the action taken to retain a system in, or return a system to, its designed operating condition'. Maintainability is thus crucial for system availability, as the latter depends not only on the

frequency of system failure but also on the time necessary to return it to normal operation.

- Safety (S) is defined in IEC [1] as the 'freedom from unacceptable risk'. It is, then, the avoidance of situations which compromise human, environmental or material integrity.

This paper focuses on reliability and safety, since availability and maintainability are deeply connected with reliability, and the latter could be said to comprise both of them taking into account methods and techniques that are beyond the scope of this discussion.

3 CENELEC Standards related to RAMS

In the railway sector, the standards that deal directly with the assurance of system RAMS are CENELEC EN 50126 [2], EN 50128 [3] and EN 50129 [4]. These standards are all based on IEC 61508 [1], which is a generic international standard applicable to all kinds of industry. IEC 61508 is divided in seven parts; the third part (IEC 61508 – 3: Software Requirements) deals with software requirements, and some parts of the EN 50128 are based on it.

EN 50126 defines a development process which facilitates efficient reliability, availability, maintainability and safety management (RAMS management). This standard illustrates a series of activities to be carried out throughout the development of a system in order to achieve the levels of reliability, availability and maintainability that are required for a particular level of safety. However, only those stages that are directly related to safety (preliminary hazard analysis, hazard log, etc.) appear to have more specific recommendations. The rest of the stages of the development process (in the case of SIL1 and SIL2) do not significantly differ from those commonly followed in general projects with a high quality management.

In order to achieve the required safety level, the standard 50126 proposes a lifecycle which is, to a great extent, based on hazard analysis in the wider sense of the term, that is, understanding hazard analysis as a set of tasks that are carried out throughout all the stages of the development of the system, starting with a preliminary hazard analysis and the creation of a hazard log, establishing a plan for hazard mitigation, carrying out a fault tree analysis, etc. However, as Leveson [6] highlights, hazard analysis techniques have a series of limitations:

- Limitations related to model construction:
  - They often make unrealistic assumptions; for instance, that the system is developed according to appropriate engineering standards, testing is perfect and repair time is negligible, operators and users are experienced and trained, operational procedures are clearly defined, key events are independent and random and so on.
  - Unknown phenomena cannot be covered in the analysis.
  - Discrepancies between the written documentation and the real system mean that important causes of accident may not be considered.
  - The boundaries of the analysis are drawn incorrectly and relevant subsystems, activities, or hazards are excluded.

In general, there is no way to assure that all factors have been considered.

- Limitations related to simplifications of the modeling techniques: continuous variables treated as discrete variables, the ordering of events, inability to represent particular aspects of the system, and so on.
- Limitations related to the fact that the analysis represents the analyst's interpretation of the system, who may inadvertently introduce bias, especially when the system under analysis is complex.

The standard EN 50129 specifies the requirements for the acceptance and approval of electronic safety systems in the field of railway signalling. Moreover, it states what evidence of safety and quality management must be provided, as well as the required functional and technical safety levels, so that the system can be accepted and approved.

The standard EN 50128 is specific for railway software. It defines the software development process and its requirements, specifying the techniques and methods that have to be used in order to satisfy system requirements depending on the appropriate safety integrity level. Nevertheless, these techniques and methods, particularly those specified for levels 1 and 2, are not very demanding to comply with, so it would be reasonable to work on this area in order to establish a set of more specific requirements that guarantee a better overall system performance.

The deficiencies mentioned above make it necessary to research into further techniques and methods for the development of software that ensure a safer and more reliable final product.

4 Strategic opportunities

Two relevant circumstances have configured the opportunity to make up for the deficiencies referred to in the previous section.

- IEC 61508-3/Ed.2. Committee Draft: The second edition of the standard 61508-3, from which an important part of CENELEC EN 50128 is derived, is currently being produced. For this reason, once the new edition of IEC 61508-3, which has significant improvements, has been accepted, it could be interesting to transfer the new changes to a new version of the standard that is based on it.
- New European documents about the Common Safety Methods (CSMs) and Common Safety Targets (CSTs) must be created by the Safety Team of the European Railway Agency (ERA): One of the objectives of the railway sector nowadays is the interconnection of railway networks within the European Union. This has leaded the European Commission to request that a set of common safety criteria are created for all Member States to abide by. The ERA has accepted this commission to develop the Common Safety Methods (CSMs) and Common Safety Targets (CSTs) that shall apply to all systems once they have finally entered into force in the near future.

Given the fact that these two circumstances will necessarily imply the adaptation of the railway sector of European industry, the time is ripe to carry

out a detailed analysis of the more promising techniques and methods and to highlight those that prove effective.

4.1 IEC 61508-3/Ed. versus EN 50128

The IEC 61508 [1] is the general standard for the functional safety of electrical/electronic/programmable electronic systems. This standard consists of seven parts, most of them directly related to the railway standard EN 50128, though the latter is differently organized and is also related to other standards.

Annex A of EN 50128, which is normative and is entitled 'Guide to the selection of techniques and measures', consists of a series of tables associated with all the clauses defined in the standard, which identify the techniques and measures that help develop a system that conforms to the standard. To the right of each of these techniques and measures, there are recommendations for or against them for each of the safety integrity levels (mandatory M, highly recommended HR, recommended R, no recommendation for or against -, or positively not recommended NR). This annex is based on annexes A and B of IEC 61508-3, though it has more severe recommendations for SIL3 and SIL4. For this reason, changes to the recommendations of techniques and measures in IEC 61508-3/Ed.2 may lead to changes in the tables of Annex A of EN 50128.

Besides the changes to annexes A and B, IEC 61508-3/Ed.2 incorporates several new annexes (C to G), which could also have a direct impact on a hypothetical new edition of EN 50128, even though these new annexes are of informative nature. Among them, Annex C ('Properties for systematic software safety integrity') is considered to be of special relevance. It relates the techniques and methods defined in annexes A and B to the properties for systematic software integrity; these properties are achieved according to the degree of rigour with which those techniques and methods are applied.

The most significant differences between the second edition of IEC 61508-3 and the previous one are briefly stated below:

- Greater emphasis on traceability between different stages of the development process (set to HR for all SILs), e.g. between system safety and software safety requirements, between software safety requirements and software architecture, between software safety requirements and software design, etc. EN 50128 recommends the use of a traceability matrix in verification for SIL1 and SIL2, and considers it highly recommended for SIL3 and SIL4.
- The use of automated software generation is recommended in Table A.2, which deals with software architecture design. No reference to this is made in EN 50128.
- Object oriented design is marked as either recommended or highly recommended in Table A.4 on detailed design, while the first edition of the standard made no reference to it at all. EN 50128 simply categorizes it as recommended.
- The use of test management and automation tools is recommended in Table A.5, which covers software modules testing and integration. EN 50128 does not comment on these tools.

- Software failure analysis techniques are explicitly added among failure analysis techniques (Table B.4) under the heading 'Software functional failure analysis'. However, no particular techniques are described, so they remain to be specified. No allusion to these techniques is made in EN 50128.
- Among semi-formal methods (Table B.7) new techniques on entity-relationship-attribute data models and message sequence charts are mentioned for the first time. EN 50128 does not refer to them.
- Static analysis of run-time error behaviour and techniques related to time analysis, such as worst-case execution time analysis, are added to static analysis (Table B.8). These are not considered in EN 50128.
- New techniques related to the modular approach are mentioned for the first time in the second edition of IEC 61508-3 (Table B.9 on software complexity control), recognizing that reliability is negatively affected by complexity. There is no allusion to this whatsoever in EN 50128.

Some of the new techniques and measures have not yet been defined in detail (marked as 'TBA' – to be announced – in the text). They are supposed to be described in a new edition of IEC 61508-7, since all the techniques and measures mentioned in part 3 are explained in part 7 (EN 50128 includes them in Annex B).

The inclusion of these new features into a new edition of EN 50128 will bring about significant improvements in reliability and safety in the railway sector.

4.2 CSM-CST

The European Commission has established a series of regulations and set a new policy that aim at unifying the railway sector in order to improve its performance and competitiveness. An important objective of this policy is the development of a common approach to railway safety, which comprises the setting up of Common Safety Methods (CSMs) and Common Safety Targets (CSTs). Both CSMs and CSTs are being gradually introduced in order to ensure that a reasonable level of safety is maintained throughout the process and that the means to improve that level are provided when necessary.

According to the European Railway Agency (ERA), CSMs define risk evaluation and assessment methods that help to determine whether the required safety level has been achieved. They cover different areas:

- Risk assessment, consisting of the identification of hazards and the specification of safety measures associated with them, as well as the safety requirements that result from those measures and the demonstration that the system complies with the safety requirements specified.
- Hazard log management. All significant changes made to the system have to be registered in a hazard log whenever they are produced and their progress has to be tracked; hazard logs will also register new hazards or new safety measures when they are identified.

The projects SAMNET and SAMRAIL were launched at the request of the European Commission for the improvement of European railway safety. The results of these two projects have been used by ERA as a starting point for the development of the CSMs (Mihm [7]).

CSTs are the safety levels that the railway system as a whole and each of its parts have to reach. These levels have to be specific, measurable, achievable and realistic, and have to be reached within a certain period of time.

5 New techniques for the assurance of reliability and safety

The aim of this section is to highlight some techniques that look promising in a first approach, though they only represent a fraction of the many possible techniques available:

- Software Fault Tree Analysis (SFTA) (Lyu [8]). Fault tree analysis (FTA) is a widespread technique used to ensure the safety of safety critical systems. It considers all the potential damages associated with a system and tracks them backwards so as to determine the events which could have caused them. Incidents records from similar systems are crucial as a starting point for the analysis. Although this technique has traditionally been applied to hardware analysis, it can provide excellent results if used to analyse the software component of systems. Each potential failure of the software can be considered, evaluating its possible causes and representing them in a fault tree model. Tracking the events which may lead to an undesired consequence helps to define the module or modules of the system affected by it, so that appropriate action can be taken to minimize or eliminate the risk.
- Software Failure Mode and Effect Analysis (SFMEA) (Storey [5]). Failure Mode and Effect Analysis is a methodology that attempts at identifying all possible failures of a system or a component or feature of a system, often at different levels, considering their possible causes and studying their consequences. In FMEA, a categorization of failures is made according to the seriousness of their consequences, so that the measures taken to reduce failures focus on those with a higher priority first. Even though this technique is commonly used for the assessment of safety in hardware systems, it can prove very useful too if applied to software systems or components.
- Artificial Intelligence for Software Reliability Engineering (Lyu [8]). There are different artificial intelligence techniques that are used for estimating software reliability, such as neural networks or fuzzy logic. Neural networks are mathematical models that interconnect and process information. They consist of nodes, which represent processing units, connected by means of mathematical functions. Their strength lies in the possibility to apply them to make predictions given a set of preliminary observations and solutions. This technique could bring about very positive results if it is applied to the assessment of software reliability.
- Markov chains (Lyu [8]). Markov chains represent the transitions between different states (failure-success) in systems, assuming that the probabilities of those transitions do not depend on previous states, but are only determined by the initial and final state. It is a useful technique to predict the reliability and availability of a system.

- Software reliability growth model [8]. The aim of reliability growth models is the construction of a model that represents the evolution of system failures detection, based on data of failures detected during the previous testing stages in order to predict the reliability of the system in operation. Because of the particular characteristics of software, it may not be possible to use traditional system reliability growth models to predict software reliability, so it would thus be interesting to adapt these reliability growth models.

6 Conclusion

As this paper has highlighted, software is becoming the most critical part of safety critical systems. The use of new techniques for the attainment of higher software reliability and safety values is necessary in order to get a better performance of the system as a whole in terms of reliability and safety.

Some of the techniques that have been mentioned in previous sections have already been in use for years. It is necessary to analyze them thoroughly to check what their actual effect on systems is, at least in the industrial sector. In fact, it would be interesting to study them in the context of the railway sector, which is the area of focus of this paper.

Finally, if a new edition of EN 50128 were to be released, these points ought to be considered:

- Since system failures are very often due to faulty requirements specifications, the improvement of the system's specification would lead to higher software reliability and safety.
- The most significant modifications made to IEC 61508-3/Ed.2 and also to the new edition of IEC 61508-7.
- Analysis of experiences for safety assurance in the European railway sector, as well as in other areas, such as the nuclear and the aeronautic sectors.
- The techniques and methods specified in the first and second sets of CSMs.
- The study of other standards, such as 60300, which also discuss techniques and methods for the improvement of system reliability and safety.

References

[1] IEC, IEC 61508: Functional safety of electrical / electronics / programmable electronic safety-related systems, International Electrotechnical Commission, Geneva, 2000.
[2] CENELEC, EN 50126: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), CENELEC: European Committee for Electrotechnical Standardization, 1999.
[3] CENELEC, EN 50128 Railway Application - Communications, signalling and processing systems - Software for railway control and protection systems CENELEC: European Committee for Electrotechnical Standardization, 2001.

[4] CENELEC, EN 50129: Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling, CENELEC: European Committee for Electrotechnical Standardization, 2003.
[5] Storey, N. Safety-Critical Computer Systems, Addison-Wesley, 1996.
[6] Leveson, N. G. Safeware: System Safety and Computers, Addison Wesley, 1995.
[7] Mihm, P. Evaluation of the results of SAMRAIL and SAMNET projects. European Railway Agency, City, 2006. http://www.era.europa.eu /public/core/Safety/Pages/useful_docs_links.aspx
[8] Lyu, M. R. Handbook of Software Reliability Engineering, First ed., Computing McGraw-Hill, 1996.