https://doi.org/10.26552/com.C.2011.2A.104-108

Milan Slivka *

SAFETY OF RAILWAY SYSTEMS AND FORMAL/SEMIFORMAL METHODS

The contribution deals with computer based railway safety systems. It shortly concerns problems associated with using computer systems in comparison with traditional safety systems. The attention is paid to formal and semiformal methods in development and approval of railways systems, seen in the context of standardization and legislation framework. The author summarizes current state of using formal and semiformal methods from whole life cycle point of view of railway safety system in the area of Slovak and Czech railways and possible reasons for their rare use.

1. Introduction

The system with safety responsibility is a system whose incorrect function (failure) may have very serious consequences such as loss of human life, severe injuries, large-scale environmental damage, or considerable economic penalties [10]. Many safety-critical systems are typically fail-safe systems, i.e. once a fault has occurred the system must remain in the previous state (provided that this state does not represent a hazard to the controlled system) or must enter a pre-defined safe state.

Safety is then the freedom from unacceptable risk of physical injury or of damage to the health of the people, either directly or indirectly as a result of damage to property or to the environment. Functional safety is a part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

Systems with safety responsibility are applied in almost all fields of modern technology today: nuclear power plant control, medicine, space programs and transport, including interlocking systems for control and command of train movements. In the next part we will be interested only in the systems mentioned as last.

The control tasks become more complex in railway and metropolitan transport systems and their realization is hardly possible without computer systems. Nowadays the computer controlled systems with safety responsibility are applied in almost all the fields of modern technology as well as in traffic (e.g. in signaling and train control systems on the railway).

2. Background

The railway area has established a very strong safety culture during its hundred years' operation. Safety in electromechanical railway signaling was based on simple fail-safe principles that rely on impermeability of the mass and gravity attraction. By the construction of this system it was ensured that any occurrence of a critical event brought a system to the fail-safe state (e.g. all signals to stop). For example, the relay type N (safety relay) is constructed in such a way that the force of gravity itself causes the relay armature to drop off if the relay is not powered, and also the contacts are made of non-weldable materials.

These properties are taken into account by a relay system design in such a way that a controlled circuit is in error case always off (except for the unlikely case the attraction force does not work).

Computer and SW based system required an adaptation of safety approaches in order to use innovative technical systems on a high safety level. The reason is that there are some problems associated with using computers to control safety-critical systems. It is generally much more difficult to demonstrate that a computer program operates correctly than to demonstrate correct operation of traditional engineering devices. For traditional engineering hardware it is possible to use continuous analysis and rely on interpolation of test results. For example, for modeling, analyzing and predicting the track circuit properties it is possible to use mathematics based on partial differential equations (which have been studied for many years and there is a firm theoretical basis). But for computer systems the discrete nature means that traditional testing methods cannot be used: the smallest change in system state (one bit) may have enormous consequences. One of the reasons is the discrete nature of computer systems [10].

All software failures, however, are systematic. Software does not wear out or break. Most software failures are the result of errors in the software which themselves result from failures in the development process, such as incorrect specification (for instance spe-

* **Milan Slivka**
Railway Research Institute, j.s.c (VUZ), Prague, Czech Republic, E-mail: slivkam@cdvuz.cz

cifying the wrong behavior in the event of an error), or a mistake when implementing this specification.Confidence in software in safety-critical systems has to be built on the confidence in the software engineering methods used, confidence in the personnel, confidence in the management, and assurance through formal methods as well as testing. These techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realization of a system to a stated integrity level.

3. Formal and Semiformal Methods in Safety Standards

Existing software engineering techniques provide structured methodologies for design, implementation, testing, verification and validation of software. These methodologies were standardized. The overriding world standard is IEC61508 – Functional safety of Electrical / Electronic / Programmable Electronic safety-related Systems. However, railway industry currently relies on the group of CENELEC sector specific related standards. These standards describe processes to be followed in order to be able to assure the safety of a railway application in all life cycle phases:

- EN 50126 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- EN 50128 Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems
- EN 50129 Railway applications – Safety related electronic systems for signalling.

EN 50126 addresses system issues on the widest scale, while EN 50129 addresses the approval process for individual systems which may exist within the overall railway control and protection system. This standard concentrates on the methods which need to be used in order to provide system which meets the demands for safety integrity which are placed upon it by these wider considerations.

This standard recommends the use of semiformal and formal methods, graphical description, structured specification, hierarchical separation using formalized methods, automatic consistency checks, and refinement down to functional level and model oriented procedures with hierarchical subdivision, description of all objects and their relationship in system requirements specification phase.

EN50128 identifies requirements, life cycle issues and documentation. It gives detailed descriptions of objectives, input documents, output documents and software requirements specification, as well as architecture, design and implementation, verification and testing. It covers software/hardware integration, software validation, quality assurance and maintenance. In Annex A, which is normative, it provides criteria for the selection of techniques and measures, depending on the safety integrity level. In Annex B, which is informative, it gives descriptions of the techniques identified in Annex A.

Also in this standard it is recommended to use semiformal and formal techniques in the software requirements specification. There is demand for a description of the problem in natural language and any necessary mathematical notation that reflects the application. Technique of formal proof is highly recommended in the verification and testing phase of software. Semiformal and formal methods are generally recognized as a fault avoidance technique that can increase dependability by removing errors during the specification of the requirements and design stages of development.

4. Semiformal and Formal Methods Generaly

Next, we will try to sketch what semiformal and formal methods are.

Semiformal methods are considered to be the methods that for identification and domain problem analysis use phraseology with precise defined structure and rules (syntax). They may include many CASE methodologies, diagrammatic techniques, graphical languages, pseudocode, and other systematic ways for describing the requirements, specification, or operation of computer systems. These methods eliminate disadvantages (ambiguity and imprecision) of natural language when used for technical descriptions.

The topic of formal methods covers the development and application of mathematically-based approaches in computing. Techniques founded on formal methods can offer a rigorous and an effective way for specification, modeling, designing and analyzing of computer systems and software. The idea of this approach is in description properties and behavior we are concerned with, in the terms of concepts from discrete mathematics sets, graphs, partial orders finite state machines and so on. This kind of notation is identified as a formal language. Specification in the formal language is very precise, with well defined syntax and semantic and can be mathematically manipulated. Calculation in these domains is based on the methods of formal (or mathematical) logic. Using laws of mathematical logic, it is possible to make (calculate) proofs of theorems and refutation checks, whether certain requirements are satisfied by a given specification [12]. The advantage is, that the correctness check can be performed automatically by machine and avoid reliance on human intuition.

5. Practical Use

Formal methods have been a topic of research for many years and during this research a lot of case studies of formal methods application were made. However, they are rarely used in commercial contexts, especially in area Slovak and Czech railways and development companies. Admittedly there are some examples of real use in the signaling industry, but not from whole lifecycle point of view. In these examples, they are normally used only to a limited extent (for example writing functional specification) and usually taking prototyped, non standardized tools and notations (company design language).

Incorporation of the formal methods in development process from the whole lifecycle point of view is not an easy task to do and some difficulties have to be overcome.

At first, people in railway signaling area are very conservative. Rather than adopting new technologies, they use traditional, trusted methods in development process. Each new technology is a priory considered untrustworthy. Moreover, development and approval of railway signaling systems without these methods are also possible, or, in accordance with safety standards.

Adaptation of formal methods assumes some level of education in formal logic. As it was mentioned, these methods are based on mathematics, more exactly, on mathematical logic. Formal approach requires dealing with formal logic semantics independently, although in a restricted form. People in railway practice are not usually experts in this domain. Formal science training is the way how to understand the fundamentals of these techniques. The understanding plays a crucial role especially for assessors and the supervising authority, because only then they can accept and trust in the used techniques.

A necessary issue that has to be solved by introducing formal methods into practice is to choose a kind of a method and a (formal) language that should be used for solving the tasks. This choice is not easy. Nowadays, plenty of individual notations, methods and tools exist. Following an online internet resource [7] the count is over one hundred. Probably, the real number can be higher. Formal methods may be classified according to different criteria: according to whether their primary purpose is descriptive or analytic (descriptive and analytic methods), according to the level of formality (with low, medium and high level of formality) and/or according to the type of the used specification language (algebraic and model-oriented) [11]. We have to take in consideration that it is obviously suitable to use different approach or language for different purpose. Probably, the annotation suitable for the system engineer describing an early lifecycle stage of the system might be less suitable for a programmer describing data structures and program control.

Another obstacle is that not only one side is involved in the development of railway signaling system. At the beginning of a railway application development, system requirements specifications had to be prepared. According to the standards, this is a duty of the railway operating authority (usually railway company, in the Czech Republic it is SZDC – Sprava zeleznicni dopravni cesty). The operating authority is the first side. The second side involved in the development process is represented by developers (manufacturers, suppliers). Their role is to develop the system on the basis of the system requirements specification. The third side is formed by the supervising authority (safety assessor, in the Czech Republic it is for example VUZ – Vyzkumny ustav zeleznicni), who have to inspect if the system was developed satisfying the safety standards and if the system achieves a desired safety level. A selected formal method has to be compatible with all the mentioned practitioners. Only then, the model made for specification can be reused for development and approval process and takes the advantage of the used method.

Another issue is that an appropriate computer tool suitable for industrial usage has to be available for the chosen formalism. The quality of the tool, as a software product, has to provide some level of engineering, good documentation, user's interface, the support and customer specific consultancy by the supplier.

Last but not least question is the cost of the new technology. Industrial companies have established their own development processes and introduction of a new technology within the development process takes some effort. For example, the shape of a development process using formal methods is rather different: a lot of the effort is concentrated on specification and verification, while rather less is devoted to coding and testing. The uptake of formal methods into the traditional industrial development process is also limited by cost/benefits ratio.

6. Possible Way to Introduce

Problems with introducing formal methods into practice are considerable, but not insolvable. All in all "formal" development process has to begin with formalizing system requirement specification. This is what can be characterized as the basic level of formal methods use. The development process itself may be non-formal, but benefits are still gained since many bugs can be removed by formalizing and discussing the system at an early stage. Translation of needs and requirements into specifications is one of the most delicate steps – if errors made during specification phases remain undetected, they become potential sources of systematic faults during the system operation. This is confirmed by a study performed by the HSE (Health & Safety Executive, of United Kingdom) concerning the primary causes of failures, based on 34 catastrophic incidents, which shows the primordial proportion (44.1%) caused by poor specifications [6].

Taking advice from the project aiming integration of techniques used by railway-engineers with formal techniques from the software-engineering area, it seems to be a good way to begin the formalization process with formalization of functional specifications using semi-formal notation or methods. The semiformal model allows the team developing the model to eliminate possible ambiguities of the non-formal descriptions and works as a bridge between the non-formal descriptions and the formal ones. One of the semiformal languages successfully applicable and suitable for making functional specifications of railways systems is UML (Unified Modeling Language). The UML is one of the most widespread and often used modeling standards, based on the object-oriented paradigm, which does justice to engineers. The standard UML 2.0 offers various modeling and visualization elements to capture and model functional requirements. Its means of description are based on graphics and are easy to understand. The UML is implemented and supported by many SW-tools that make it possible to generate the source code directly from the diagrams. Next advantage of the UML is the animation capability of the model. Animation allows verification of the functional correctness before producing a real system.

From practical point of view, the character of the railway system as such is that it is composed from smaller components with very similar behavior. For example, a station interlocking system is composed of signals, track sections, switch points, etc. In practice, in the railway domain, the system requirements specification usually contains definition of the behavior of subsystems, the system structure and description of operational scenarios [1].

Subsystems and their parts can be regarded as objects. The whole system is then defined as a set of interacting objects or classes of the model. The relationships between these objects then describe the relationships between the system components. In this form, the static structure of a system can be grasped.

The dynamic system behavior is described by the local behavior of single objects and by interactions between the objects. This description defines the behavior of objects, including the various states that an object can enter into over its lifetime and the messages or events that cause it to transit from one state to another.

The operation scenarios can be modeled in form of interactions between the system components.

The way of UML application reflecting different aspects system definition mentioned above is demonstrated in figures included. It shows fragments (due to the limited size of the paper) of most often used diagram types. The application domain is a part of the station interlocking, in this case the control of a switch point. In Fig. 1 there is a Class Model Diagram, describing static structure of a station interlocking system. Included are only parts related to the switch point, i.e. parts (class) which can, for example, ask for changing point position etc.

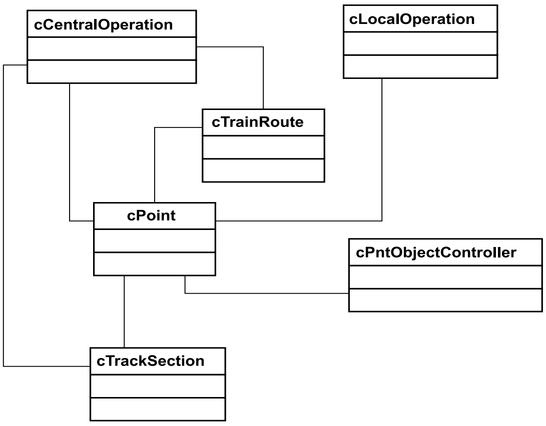

Fig. 1 Class Diagram

Operational scenarios in this example are modeled by means of the Use Case diagram Fig. 2. This kind of diagram shows typical interactions between the system under design and external objects that may want to interact with it. Dynamic system behavior is described by the state diagram in Fig. 3. This diagram is presenting realization of one of the use cases – individual control. In this diagram we can recognize the condition which has to be fulfilled to change the point position (in form of guards of transitions between states).

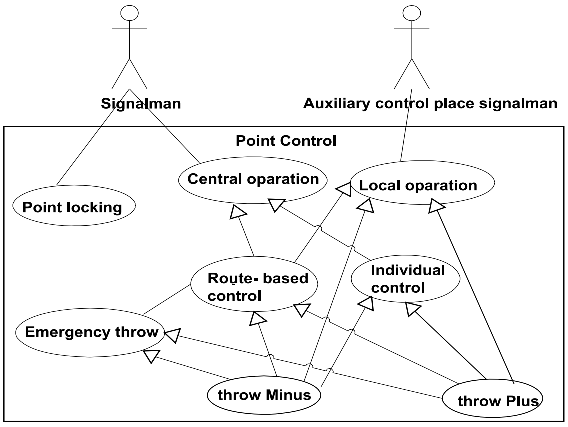

Fig. 2 Use Case Diagram

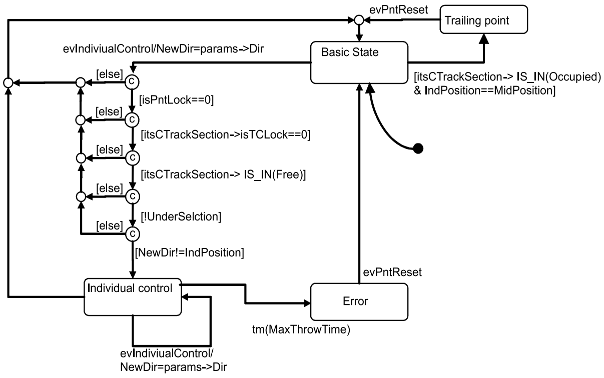

Fig. 3 Statechart Diagram

7. Functional Safety and Technical Safety

The given examples show that semiformal methods are good tools for describing or modeling functional requirements of the railway interlocking system. But, there are some additional factors. Railway interlocking is a safety system and requirements of such a system are considered in two parts: Safety functional requirements (functional safety) and Safety integrity requirements (technical safety).

Safety functional requirements are the current safety-related functions which the system, sub-system or equipment is required to carry out. These requirements concern correct operation of the system/sub-system/equipment under fault-free conditions (that is, with no faults in existence), in accordance with the specified operational and safety requirements.

Safety integrity requirements define the level of safety integrity required for each safety-related function. The term integrity refers generally to the probability of a system, or a piece of equipment, satisfactorily performing the required safety functions. Fulfillment of safety integrity requirements ensures that in the case of faults occurrence in the system itself, the safety of the controlled process is still not endangered. If we assume only one independent error/failure can arise in a given instant, the technical safety requirements can be briefly recapitulated as follows:

- No failure must jeopardize the train movement safety.
- Any failure must be conveniently and promptly, considering failure frequency, detected so that it is possible to eliminate any further failure that may arise and jeopardize safety in conjunction with the previous one.
- If a failure goes undetected, the possible emergence of other failures is to be assumed.
- If a failure could possibly result in other subsequent failures, all combinations of these must be taken into account.
- After a failure detection, the faulty equipment or part should be shut down automatically without delay. At any rate, the output of the equipment or the part must remain in, or immediately change to, a state not jeopardizing operational safety.
- Equipment that was shut down because of a failure must not be reactivated by another failure occurrence [9].

The use of semiformal or formal techniques for describing technical safety requirements or checking their fulfillment (in case of formal methods) for concrete system is hardly possible and question is, if ever possible. Fulfillment of technical safety requirements is very important part of the development process and plays important role by the assigning of certain safety integrity level.

8. Conclusion

The computer and SW based system required an adaptation of safety approaches in order to use computer systems in railway interlocking on a high safety level. Formal methods are one of the ways of increasing confidence in computer systems in this area. The design and verification of systems based on formal or semi-formal methods give a chance to check functional correctness just before creating the system itself (in term of functional safety). This approach to a system design is in accordance with requirements of the European standards. But, some difficulties have to be overcome to introduce these methods in the development process and take advantages from their use. One of the possible ways to begin the formalization process is using semi-formal methods for the system specifications. It produces an environment suitable for communication not only between development teams, but also towards other subjects involved in the process of the system verification and approval. But, we have to keep in mind that the safety systems have to be considered also from the technical safety point of view. Semiformal and formal methods in this field are very hardly applicable, if applicable at all.

References

[1] BITSCH, F.: *Process Model for the Development of System Requirements Specifications for Railway Systems.* Internnatonal Workshop on Software Specification of Safety Relevant Transportation Control Tasks, Fortschritt-Berichte VDI, Reihe 12, Verkehrstechnik/Fahrzeugtechnik, Nr. 535, 2002.

[2] CENELEC EN 50126: *Railway applications: The Specification and Demonstration of Dependability – Reliability, Availability, Maintainability and Safety (RAMS),* 1999.

[3] CENELEC EN 50128: *Railway applications: Software for Railway Control and Protection Systems, 2001.*

[4] CENELEC EN 50129 *Railway Applications – Communications, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling, 2003.*

[5] CIMATTI, A., GIUNCHIGLIA, F., MONGARDI, G., PIETRA, B., ROMANO, D., TORIELLI, F., TRAVERSO, P.: *Formal Validation & Verification of Software for Railway Control and Protection Systems: Experimental Applications in ANSALDO,* Proc. of World Congress on Railway Research (WCRR'97), 1997. Vol. C, p. 467–473.

[6] *Final Report. Safety-Related Complex Electronic Systems.* Contract SMT 4CT97-2191, Project "Standards for Safety Related Complex Electronic Systems (STSARCES)", 2000. p. 137.

[7] *Formal methods, Individual notations, methods and tools.* [Online]. http://formalmethods.wikia.com/wiki/Formal_methods.

[8] FRANEKOVA, M., RASTOCNY, K: Modelling in Development of Safety-related Communication Systems, *Communications – Scientific Letters of the University of Zilina,* 2008. Vol 10, Nr.1, p 24–30. ISSN 1335-4205.

[9] CHUDACEK, V., LOCHMAN, L., STOLIN, M.: Navigation Satellite Systems in Railway Signalling? *Signal+draht International* 2002, No.5, p. 44–47. ISSN 0037-4997.

[10] ISAKSEN, U., BOWEN, J. P., NISSANKE, N.: *System and Software Safety in Critical Systems.* The University of Reading, Department of Computer Science, 1996.

[11] JANOTA, A.: Using Z Specification for Railway Interlocking Safety. *Periodica Polytechnica, Ser. Transport Engineering,* Hungary, 2000. Vol. 28, No. 1-2, p. 39–53. ISSN 0303-7800.

[12] RUSHBY, J.: Formal Methods and their Role in the Certification of Critical Systems *Computer Science Laboratory,* SRI International, Menlo Park, 1993.