BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMICS
TRANSPORTATION SCIENCES

APPLICATION OF FORMAL METHODS IN RAILWAY SIGNALLING

PhD THESES

BALÁZS SÁGHI
MSc Transportation Eng.

Consultant:
Prof. Dr. habil. GÉZA TARNAI

BUDAPEST, JANUARY 2003

I. PRELIMINARIES, AIM OF THE RESEARCH

Under *formal methods* we understand such procedures, in course of which mathematical notations (e.g. logical set theoretical formulas) are applied in order to describe certain properties of a system at certain life cycle stages of a systems. The mathematical basis of a formal method is usually provided by a *formal specification language*. This basis enables to describe system properties (like consistency, completeness, correctness) formally both in connection with the specification and the implementation. Thus, formal methods include formal specification, formal development, formal design techniques as well as mathematical, i.e. formal verification and validation techniques [Inc92] and thus provide possibility to proceed the activities in connection with the life cycle stages of the system, systematically.

The development of formal methods dates back to the middle of the 1960-s. A real break-through in the field of applications although happened only in the late 80s, early 90s; in recent years the demand for formal methods have been increasing significantly.

In the last few years a part of the system development organizations have realized that for the development maintenance and management of the complex system new procedures, methods are required. Many organizations realized the formal methods are adequate for this purpose, thus the application field is increasing in recent years [Cra93].

The primary aim of the application of formal methods in the field of railway signalling is to provide such a tool for developers, designers, customers, assessors and authority persons with help of which the correctness of the signalling systems can be reached and proved cost-effectively with consideration of the characteristics of this special field.

However, in connection with the applicability of formal methods generally and especially in the field of railway signalling there seems to be a gap between the possibilities, provided by the academic world and the requirements of the practical applications.

Several efforts can be observed nowadays, the aim of which is to fill somehow this gap.

The German Research Association (DFG) has a special programme that deals with software specification techniques, in which the applicability of formal methods is investigated.

In the FME (Formal Methods Europe) project (also supported by the EU) a special working group have been established with the centre in Denmark, which organized five workshops in 1998-99 with focus on the railway applicability of formal methods. On these workshops more than 200 railway IT specialists have been participated from all over Europe [FMERail98-99].

The German Federal Railway Office (EBA) also supports the application of formal specification techniques in the field of railway signalling, which can be advantageous for EBA as well as for developers and railway companies. EBA, however, remarks that the situation can be really troubled, if each and every developer uses its own conception and notation. Therefore a workgroup has been established, as a result of the FORMS98 Symposium [FORMS98] (organized by the Institute of Control and Automation Techniques, TU Braunschweig, and by the Research and Technology Centre of the German Railways), which the aim to create a consensus between the developers, contractors, users, customers and the authority in connection with the application of formal methods.

The FORMS Symposium was organized in 1999 and 2000 too, after its start in 1998. The aim of the workshop in 1999 [FORMS99] was to discuss the so called Requirements' Catalogue (the requirements of the field of railway signalling from the formal methods), elaborated by the above mentioned workgroup. In course of FORMS2000 [FORMS00] a so-called benchmark was carried out, the aim of which was a comparative analysis of single formal description methods with consideration of the requirements of the railway domain.

The efforts, detailed above, however have not reached their aim until now. The primary reason for this can be identified in the facts, that the foregoing researches have not taken into consideration (1) certain specialities of the railway signalling systems and (2) certain characteristics of the development process of these systems.

The aim of the dissertation, among other efforts to fill this gap, is

- to clarify and to describe unambiguously those features of the field of railway signalling, which influence the application of formal methods, furthermore
- to specify such guidelines, which set the course for the possible ways of the application of formal methods in railway signalling.

Among the bibliography of the application methodology of formal methods the publications of J. Wing [e.g. Win90] must be mentioned, in which the basic definitions of formal methods are described from the application point of view.

A. Hall [Hal90] deals with the practical application of formal methods, furthermore with some myths around formal methods. On the application of formal methods J. Bowen carried out considerable research activity [Bow92, Bow93a, Bow93b, Bow94a, Bow94b].

The railway application of formal methods is mostly researched by the above mentioned research and working groups [FMERail, FORMS].

Aspects on the applicability and application of formal methods can be found at several places in the literature, however the widest and most consistent can be found in [NASA95, NASA97]. Further application aspects are discussed in [Ehr99, Bow93b, Bow94b, Cra93, Tho95, Pat01, Lar96, Hal90, Win90] separately. These aspects as a total, do not take some aspects into consideration, which are important for my research activity, and they do not build a system.

In connection with the Requirements' Catalogue, elaborated by the FORMS workgroup [Anf] several critical issues are emerging: some of the requirements relate to the system development generally and not to the formal methods; many of the requirements form a demand on formal methods, which are not unique in the field of railway signalling, i.e. it is not specific enough to railway signalling.

Because of the foregoing it became necessary to complement the application aspect with new ones, and by the systematization of them to build a consistent system of application aspects; and to annotate the Requirements' Catalogue by critical remarks and extensions in order to become more adequate to reach its original goal.

II. METHOD OF RESEARCH

The goal of the research determined me the direction of the research and the methods to apply at each phase of the research activity. The sequence of the steps of my research is reflected in the relation of the new scientific results too.

When analysing the scientific literature of the railway application of formal methods, it can be seen, that one of the main obstacles in the applicability of formal methods is, that the known descriptions of the development process of railway signalling appliances do not reflect the real-world process of the development. Therefore, as a first step, the life cycle of the railway signalling appliances had to be examined. As a result, by means of improving the existing life cycle models, such a model has been established, which reflects the process of the development of the railway signalling appliances adequately, thus it can serve as a basis for the further examination of the applicability of formal methods (Thesis 1).

After this, those factors have been identified, which necessitate the introduction of new methods in the system development generally, to a greater extent in the case of safety-critical system and especially in the field of railway signalling.

The advantages, which can be reached by the application of formal methods in the outlined fields, can be identified by the examination of the fundamentals of formal methods, and by taking the above mentioned demand into consideration.

Afterwards, those aspects have been identified, which influence the applicability and the efficiency of applicability of formal methods. By means of completion of the aspects found in the literature by new aspects, and by systematizing of them, a consistent system of application aspects has been elaborated (Thesis 2).

The Requirements' Catalogue [Anf99] plays a central role in the scientific literature of formal methods in railway signalling, therefore the mentioned document needed to be analysed. The results of the examination showed, that the single requirements of the Catalogue and the formulation of them make impossible, that the document can reach its aim. Hence the Requirements' Catalogue had to be supplied by such critical remarks and interpretative addenda, by means of which the document will be more appropriate for reaching its original aims (Thesis 3). In order to reach this result I personally consulted the editors of the Requirements' Catalogue at the Technical University of Braunschweig, Germany.

To the railway application of formal methods, the collection and the survey of the known application examples was unavoidable. The evaluation of the application examples is based on the system of application aspects (Thesis 2) and on the complemented Requirements' Catalogue (Thesis 3).

I studied Petri-nets, as widely used modelling language. I examined how Petri-nets can be applied for the modelling of relay circuits. In connection with this I evaluated the usual modelling method and suggested to apply a new modelling method (Thesis 4).

Based on the general system of application aspects, and by taking into account the specialities of the field of railway signalling and the lessons learned from the application examples, guidelines have been specified for the application of formal methods in railway signalling (Thesis 5).

Finally, a model is suggested for the introduction procedure of formal methods into the field of railway signalling (Thesis 6).

III. NEW SCIENTIFIC RESULTS

1.

I examined the system development life cycle models, suggested by the scientific literature for IT and process control systems. I compared them with the development practice of the safety critical and especially of the railway signalling systems. I investigated validity and the applicability of the proposed models in this special field of expertise.

I pointed out that the structure of the analyzed models does not allow them to be applied in the field of safety critical systems and especially of railway signalling systems; hence the applicability of the proposed models in the examined area is limited.

Thesis 1. *I elaborated such a model for the specification process of railway interlocking systems that considers the specific characteristics of the examined application domain, compared to the models suggested by the scientific literature. The established model*

- *differentiates and locates in the development process the different levels of specifications of the railway signalling systems (customer*

requirements, system specification, high level system design) and the activities in connection with the production of these documents;
- *considers and handles the unavoidable iterativity of the specification process of the railway domain, that originates from the multiple participants of the process; furthermore*
- *reflects that characteristics of the development process of railway signalling systems, that producing companies often modify or adapt their so-called basis systems to fulfil the requirements of a railway's customer requirements.*

Thesis 1 is based on Chapter 1.1 of the dissertation furthermore on the publications [1], [2], [3], [5] and [8].

2.

The scientific literature discusses several aspects on the application of formal methods, but these aspects
- do not reflect numerous factors and
- do not form a unified system.

Thesis 2. *I complemented the application aspects of the literature by new ones, and systematized the complemented aspects, thus elaborated such a system of aspects for the application of formal methods, which includes the*
- *rigor,*
- *scope,*
- *technical and*
- *administrative aspects,*
- *costs, limitations and difficulties*

of the application of formal methods.

For the sake of the applicability of the system of application aspects I annotated the single aspects by theoretical and practical considerations.

The system of application aspects enables the objective evaluation of former applications and allows determining optimal application parameters for future applications.

Based on the system of application aspects, application directives can be defined for a given domain (e.g. railway signalling systems), which consider the specialities of the domain (*see* Thesis 5).

Thesis 2 is based on Chapter 3 of the dissertation and on the publications [3], [5], [7], [8], [9] and [10].

3.

I investigated and evaluated the so-called Requirements' Catalogue [And99], which plays a central role in scientific literature of the application of formal methods in railway signalling, and the aim of which is to help on the adequate choice of formal methods for the domain of railway signalling.

I pointed out that

- a party of the requirements is not connected directly to formal methods, but are relating to the system development in general, and
- the document contains numerous general requirements that are not specific to the domain of railway signalling.

Therefore, the requirements of the Requirements' Catalogue and the formulation of the requirements make the document unsuitable for reaching its original goal.

In course of the detailed evaluation I

- formulated methodological and substantial critiques in connection with the single requirements and
- added interpretations which are partly general, partly concerning the domain of railway signalling.

Thesis 3. *I made the so-called Requirements' Catalogue appropriate to help on the choice and on the adequate application of formal methods, suitable for different tasks of the domain of railway signalling, together with the elaborated system of application aspects (Thesis 2).*

Thesis 3 is founded on Chapter 4 of the dissertation and on the publication [9].

4.

I examined Petri-nets, the widely used modelling notations, how they are adequate for the description of relay based railway interlocking systems. I founded that the usual Petri-net description method for logical systems, are only limitedly appropriate for the modelling of relay nets.

Thesis 4. *I developed such a Petri-net based modelling method for the modelling of relay nets, by the application of which*

- *the production of the model becomes easier,*
- *the size of the model becomes smaller,*
- *the model itself becomes clearer,*
- *and the operation of the relays can be modelled more realistic,*

compared to the usual modelling method.

Thesis 4 is founded on Chapter 6 of the dissertation, and on the publication [6].

5.

Thesis 5. *I elaborated directives for the application of formal methods at the stage of customer requirements and high level system design. The directives define the rigor, scope, technical and administrative aspects of the application of formal methods to the relating phases. Furthermore the directives are concerning the transformability of customer requirements and system design, furthermore the applicability of formal methods in further life cycle phases of railway signalling systems.*

To the elaboration of the directives I preliminary evaluated the known railway application of formal methods.

The application directives are based on the general system of application aspects (Thesis 2), and in course of the elaboration the following factors were taken into account:

- the specialities of the railway signalling domain (Thesis 1 and 3),
- the results of the evaluation of the known application examples.

Thesis 5 is based on Chapters 7.1-7.4 of the dissertation and on the publications [11] and [12].

6.

Thesis 6. *I elaborated such a multiphase model for the introduction of formal methods into the domain of railway signalling, the phases of which are determined by the formalization level of the customer requirements and high level system design.*

To the elaboration of the model, preliminary I fixed those phases of the development process of railway signalling system that are distinctive form the application point of view of formal methods and took into consideration

- the features of the development process of the railway signalling domain,
- the characteristics of formal methods and that of the application of them and
- the different interests of the participants of development process.

Thesis 6 is based on Chapter 7.5 of the dissertation, furthermore on the publications [11] and [12].

IV. APPLICABILITY OF THE NEW RESULTS

Nowadays, to the application of formal methods a rich method and tool support is available. However there has been a lack in the domain of railway signalling; there has been a gap between the possibilities provided by the academic world and the requirements of the practical application. In course of the research and by the elaboration of the dissertation my goal was to fill or to reduce this gap.

The new scientific results have been published in several domestic and international forums.

The successful solution of the research task helps on the practical application of former scientific results, and on the stepwise introduction of the applications to the domain of railway signalling.

The development model of Thesis 1 can primarily be directive in future research activities.

The system of application aspects, introduced in Thesis 2 can be useful for researchers and practitioners active in the field of railway signalling systems.

Results of Thesis 3, similarly to that of Thesis 1, can be applied in future researches.

The modelling methods, elaborated in Thesis 4, augmented with an adequate analysis method, can be advantageously applied for checking relay interlocking systems or subsystems.

Directives of Thesis 5 can be used both in future researches and in practical applications.

Finally, model of Thesis 6 can serve as a basis for the introduction of formal methods into the railway signalling; it can be the foundation of an introduction strategy which includes the definition material and personal conditions.

V. PUBLICATIONS ON THE DISSERTATION'S SUBJECT

[1] Tarnai G., **Sághi, B.**: Application of Formal Methods for Specification of Safety-Relevant Traffic Process Control Systems" *INTCOM '98 Symposium on Intelligent Systems in Control and Measurement* Miskolc-Lillafüred, 1998. November 21-27. pp. 237-244.

[2] Tarnai G., **Sághi B.**: Erhöhung der Bahnsicherheit durch formale Methoden. *Periodica Polytechnica,* Transportation Engineering, Vol. 26, No 1, Budapest, 1999. pp. 175-186.

[3] Tarnai G., **Sághi B.**: Einsatz von formalen Methoden in die Eisenbahnsicherungstechnik. *ZEL '2000 7. internationales Symposium*. Žilina, Szlovákia, 2000. May 30-31. pp. 80-88.

[4] Tarnai G., **Sághi B.**: Method for the Development of a Special Railway Interlocking Subsystem. *9th IFAC Symposium on Control in Transportation Systems*. Braunschweig, Németország, 2000. June 13-15., pp. 495-500.

[5] Tarnai G., **Sághi B.**: Formális módszerek alkalmazása a vasútbiztosító technikában. *Vezetékek Világa. Vasúttechnikai szemle.* Budapest 3/2000 pp. 11-15.

[6] **Sághi B.**: Jelfogós sorompó illesztő kapcsolás modellezése Petri-hálóval. BME Ipari nyílt nap 2000. Poszter-előadás.

[7] Tarnai G., **Sághi B.**: Követelményrendszerek formalizálása a vasútbiztosításban. *III. Országos Vasúti Távközlési és Biztosítóberendezési Konferencia* Miskolc-Lillafüred, 2000. October 9-11. pp. 86-98.

[8] Tarnai G., **Sághi B.**: Chapter *Safety-critical Systems*. p. 53. In: Pataricza A. (szerk.): Formal Methods of Informatics – KHVM 96/2000 technical report.

[9] Tarnai G., **Sághi B.**: Zusätzliche Aspekte zur Anwendung von formalen Techniken in der Eisenbahnsicherungstechnik. *Signal+Draht* (Germany) **(93)** 7-8/2001. pp. 42-45.

[10] Tarnai G., **Sághi B.**: Application Aspects of Formal Methods in Railway Signalling. *The Transport of the 21st Century – International Scientific Conference.* Warsaw, Poland, 2001. September 19-21. pp. 199-205.

[11] Tarnai G., **Sághi B.**: Software Specification and Development in the Domain of Railway Signalling. *Workshop on Software specification of safety relevant transportation control tasks.* 3rd Workshop in the course of the DFG-Priority Program Integration of Software Specification Techniques for Application in Engineering. Braunschweig, 2002. April 23-24.

[12] **Sághi B.**: Irányelvek a formális módszereknek a vasútbiztosítás területén történő alkalmazásához. *Közlekedéstudományi szemle*. LII. évf. 8. szám, 2002. pp. 291-299.

VI. REFERENCES

[Anf99] Formale Techniken für die Eisenbahnsicherungstechnik. Anforderungskatalog – Zusammenfassung der Arbeitsunterlagen. *Signal+Draht* (91) 10/1999, pp. 38-42.

[Bow92] Bowen, J.P., V. Stavridou: Formal Methods and Software Safety. *SAFECOMP 1992: Safety of Computer Control Systems,* 1992.

[Bow93a] Bowen, J., V. Stavridou: Safety-Critical Systems, Formal Methods and Standards. *Software Engineering Journal*, 1993.

[Bow93b] Bowen, J., V. Stavridou: The Industrial Take-up of Formal Methods in Safety-Critical and Other Areas: A Perspective. *FME'93: Industrial-strength formal methods, 1st International Symposium of Formal Methods Europe,* April 1993 (Springer-Verlag, *Lecture Notes in Computer Science* 670, 1993.

[Bow94a] Bowen, J. Formal Methods in Safety-Critical Standards. (?) 1994.

[Bow94b] Bowen, J., M.G. Hinchey: Seven More Myths of Formal Methods: Dispelling Industrial Prejudices. *FME'94: Industrial Benefit of Formal Methods*, Springer-Verlag, October 1994.

[Bow95] Bowen, J., M.G. Hinchey: Ten Commandments of Formal Methods. *IEEE Computer*, 28 (4) April 1995. pp. 56-63.

[Cra93] Craigen, D., S. Gerhart, T. Ralston: An International Survey of Industrial Application of Formal Methods (Volume 1: Purpose, Approach, Analysis and Conclusion, Volume 2: Case Studies). *Atomic Energy Control Board of Canada, U.S. National Institute of Standards and Technology, and U.S. Naval Research Laboratories*, NIST GCR 93/626, 1993.

[Ehr99] Ehrig, H., F. Orejas, J. Padberg: Relevance, Integration and Classification of Specification Formalisms and Formal Specification Techniques. In: [FORMS99]

[FMERail98/1] 1st Workshops on Formal Methods in Railway Industry, June 8-9 1998, Nieuwegein, The Netherlands http://www.ifad.dk/Projects/fmerail.htm

[FMERail98/2] 2nd Workshops on Formal Methods in Railway Industry. October 15-16 1998, London, U.K. http://www.ifad.dk/Projects/fmerail.htm

[FMERail99/1] 3rd Workshops on Formal Methods in Railway Industry. February 24-26 1999, St. Pölten, Austria. http://www.ifad.dk/Projects/fmerail.htm

[FMERail99/2] 4th Workshops on Formal Methods in Railway Industry. May 11-12 1999, Stockholm, Sweden. http://www.ifad.dk/Projects/fmerail.htm

[FMERail99/3] 5th Workshops on Formal Methods in Railway Industry. September 22-24, 1999 Toulouse, France. http://www.ifad.dk/Projects/fmerail.htm

[FORMS00] FORMS 2000 - Formale Techniken für die Eisenbahnsicherung. *Fortschr.-Ber. VDI Reihe 12 Nr. 441 Düsseldorf: CDI Verlag* 2000 p.220

[FORMS98] *International Workshop on the Formal Specification of Train Control Systems in Europe.* May 12-13 1998, Braunschweig http://www.ifra.ing.tu-bs.de/forms/

[FORMS99] *Formale Techniken für die Eisenbahnsicherung. Workshop*, December 1-2 1999, Braunschweig. http://www.ifra.ing.tu-bs.de/forms/

[Hal90] Hall, J.A.: Seven Myths of Formal Methods. *IEEE Software,* September 1990. 7 (5) pp.11-19.

[Inc92] Ince, D. C.: An Introduction to Discrete Mathematics, Formal System Specification, and Z. *Oxford University Press, Oxford.* 1992.

[Lar96] Larsen, P.G., J. Fitzgerald, T. Brookes: Applying Formal Specification in Industry. *IEEE Software*, May 1996. pp. 48-56.

[NASA95] NASA Office of Safety and Mission Assurance: Formal Methods Specification and Verification Guidebook for Software and Computer Systems. Volume I: Planning and Technology Insertion. NASA-GB-002-95 Washington, 1995.

[NASA97] NASA Office of Safety and Mission Assurance: Formal Methods Specification and Analysis Guidebook for the Verification of Software and Computer Systems. Volume II: A Practitioner's Companion. NASA-GB-001-97 Washington, 1997.

[Pat01] Pataricza A., Csertán Gy., Majzik I., Bartha T.: Formális módszerek az informatikában. Jegyzet kézirat. 2001. március.

[Tho95] Thomas, M.: IEE/BCS Workshop report 20/3/95. University of Glasgow, Dept. of Computing Science. 1995.

[Win90] Wing, J.: A Specifier's Introduction to Formal Methods. *IEEE Computer* September 1990. pp. 8-24.