The FME Rail Annotated Rail Bibliography

Dines Bjørner
Department of Information Technology, Bldg. 344
Technical University of Denmark, DK–2800 Lyngby, Denmark
Fax: +45-45.88.45.30, E-Mail: db@it.dtu.dk; URL: http://www.it.dtu.dk/~db

October 22, 1998 — October 25, 1999

Abstract

This document is part of the IT/DTU Work Package for the EU sponsored ESSI Project 26538: **FME Rail**.

It is posted on the web:

- Postscript: http://www.it.dtu.dk db/racosy/fmerail.ps[1]
- HTML: http://www.it.dtu.dk db/racosy/fmerail.html[2]

Contents

[1] http://www.it.dtu.dk/ db/racosy/fmerail.ps
[2] http://www.it.dtu.dk/ db/racosy/fmerail.html

1 Introduction

The following report contains annotated references to such documents (incl. publications) which report on applications of formal techniques and tools to problems of railway systems.

Some references contain abstracts:

> **Abstract:** The abstracts are usually culled from electronic versions of the reference;

some contain keywords:

> **Keywords:** The keywords are usually culled from electronic versions of the reference;

and, in synchrony with DB (IT/DTU) reviewing these references, many will contain annotations relevant, it is hoped to the endeavours of FME Rail:

> **FME Rail Annotations:**
>
> – **Rail subject:** Lists key terms of the railway domain, or of railway software (and/or hardware) requirements, and/or of software (and/or hardware) designs.
> – **Principles, techniques, tools:** Lists key methodological principles, techniques and tools applied in order to deal with the rail subject.
> – **Notes:** Ventures additional comments believed relevant in the FME Rail context.
> – **Repository:** Optional — indicates whether a copy is kept at Lyngby.

This document constitutes one result of the IT/DTU FME Rail work package.

For information on FME Rail please refer to:

- `http://www.ifad.dk/Projects/fmerail.htm`[3]

2 Methods, Techniques and Tools

Currently the following techniques and tools have been identified as having been or being used in understanding and developing experimental or commercial software and/or hardware (incl. equipment) solutions to railway problems.

The below list will be regularly updated.

In right margin citations we refer to **alpha**betic references to method, technique or tool texts.

In addition we **plain** number reference such documents which apply the itemised method, technique or tool.

1. **B:** [Abr96, Lan96, Wor96]

   [63, 122, 84, 83, 85, 199, 19, 198]

2. **CafeOBJ:** [DF96, Nak97, NSF, FD]

3. **CoFI: CASL:** [oLD97, oS97, Mos97, CHKBM97]

[3] http://www.ifad.dk/Projects/fmerail.htm

4. **ccs:** [Mil80, Mil89]

   [216, 217, 218, 219]

5. **COLD-K:** [COL90, Jon88a, Jon88b, MdL91]

6. **CSP/FDR:** [Hoa85, Ros97]

   [265, 242, 241, 267, 266]

7. **Domain Engineering:**

   [SM98]

8. **The Duration Calculi:** [CHR91, CX93, CRH93, Cha93, CH93, HC94, CHX95, HG95]

9. **ExSpect:** [KvHV91]

   [15, 14]

10. **Euris:**

    [234, 119]

11. **FOREST:** [AC91]

    [12]

12. **Graph Grammars:**

    [134]

13. **HOL:** [GM93]

    [75, 289, 74]

14. **Michael Jackson's Description Principles** [Jac94, Jac95, Jac97, ZJ97a, ZJ97b]

15. **Larch:** [GHG+93, MW93]

16. **Logic:** [GHRN93b, GHRN93a, GHRN94, GHRN95, GHRN98]

    [156, 151, 154, 153]

17. **Mathematics:**

    - General: [232, 78]
    - Galois Theory: [152]
    - Graph Theory: [290]

18. **Model–checking:**

    [135]

19. **μCRL:** [GP94, GP95, GvV95]

    [121, 120]

20. **Petri Net:** [Rei85, Rei98]

    [210, 209, 234, 211, 13, 15, 213]

21. **Prolog:**

    [18]

22. **RAISE, RSL:** [Gro95, Gro92]

    [247, 30, 111, 112, 28, 136, 27]

23. **Requirements Engineering:** [ELC+98] + Jackson, item 14

24. **SMV:** [SMV]

    [158]

25. **SPRINT:** [Jon93]

26. **Stålmarck's Method:** [SS90]

    [258, 120, 121, 196, 96, 95, 36, 38, 245, 40, 41, 39, 244]

27. **STeP/React:** [MP91, MP95]

28. **VDM, VDM–SL:** [BJ78, Jon90, FL98]

    [129, 128, 26, 130, 91, 131, 5, 132, 137]

29. **Z:** [Spi88, Spi89]

    [171, 134]

References

[Abr96] Jean-Raymond Abrial. *The B Book: Assigning Programs to meanings.* Tracts in Theoretical Computer Science. Cambridge University Press, Cambridge, England, 1996.

[AC91] W. Atkinson and J. Cunningham. Proving properties of a safety-critical system. *Software Engineering Journal*, 6(2):41–50, March 1991. .

[BJ78] D. Bjørner and C.B. Jones, editors. *The Vienna Development Method: The Meta-Language*, volume 61 of *Lecture Notes in Computer Science.* Springer-Verlag, 1978.

[CH93] Zhou Chaochen and Michael R. Hansen. Lecture Notes on Logical Foundations for the Duration Calculus. Lecture Notes, 13, UNU/IIST, P.O.Box 3058, Macau, August 1993.

[Cha93] Zhou Chaochen. Duration Calculi: An Overview. Research Report 10, UNU/IIST, P.O.Box 3058, Macau, June 1993. Published in: *Formal Methods in Programming and Their Applications,* Conference Proceedings, June 28 – July 2, 1993, Novosibirsk, Russia; (Eds.: D. Bjørner, M. Broy and I. Pottosin) LNCS 736, Springer-Verlag, 1993, pp 36–59.

[CHKBM97] M. Cerioli, A. Haxthausen, B. Krieg-Brückner, and T. Mossakowski. Permissive Sub-sorted Partial Logic in CASL. In *Proceedings, AMAST'97*, volume 1349 of *Lecture Notes in Computer Science*. Springer–Verlag, 1997.

[CHR91] Zhou Chaochen, C.A.R. Hoare, and A.P. Ravn. A Calculus of Durations. *Information Processing Letters*, 40(5):269–276, 1991.

[CHX95] Zhou Chaochen, Dang Van Hung, and Li Xiaoshan. A Duration Calculus with Infinite Intervals. Research Report 40, UNU/IIST, P.O.Box 3058, Macau, February 1995. Published in: *Fundamentals of Computation Theory*, Horst Reichel (ed.), pp 16-41, LNCS 965, Springer-Verlag, 1995.

[COL90] Algebraic Specifications. Tutorial Material, April 1990. This is COLD-K Course Material.

[CRH93] Zhou Chaochen, Anders P. Ravn, and Michael R. Hansen. An Extended Duration Calculus for Real-time Systems. Research Report 9, UNU/IIST, P.O.Box 3058, Macau, January 1993. Published in: *Hybrid Systems*, LNCS 736, 1993.

[CX93] Zhou Chaochen and Li Xiaoshan. A Mean Value Duration Calculus. Research Report 5, UNU/IIST, P.O.Box 3058, Macau, March 1993. Published as Chapter 25 in *A Classical Mind*, Festschrift for C.A.R. Hoare, Prentice-Hall International, 1994, pp 432–451.

[DF96] Razvan Diaconescu and Kokichi Futatsugi. Logical Semantics of CafeOBJ. Research Report IS-RR-96-0024S, JAIST, 1996.

[ELC+98] S. Easterbrook, R. Lutz, R. Covington, J. Kelly, Y. Ampo, and D. Hamilton. Experiences using lightweight formal methods for requirements modeling. *IEEE Transactions on Software Engineering*, 24(1):4–14, 1998. .

[FD] Kokichi Futatsugi and Razvan Diaconescu. *CafeOBJ Report — Definition of the Language*. To appear in 1998 as book in the AMAST series at World Scientific .

[FL98] John Fitzgerald and Peter Gorm Larsen. *Modelling Systems: Practical Tools and Techniques*. Cambridge University Press, 1997–1998.

[GHG+93] John V. Guttag, James J. Horning, S.J. Garland, K.D. Jones, A. Modet, , and J.M. Wing. *Larch: Languages and Tools for Formal Specification*. Texts and Monographs in Computer Science. Springer-Verlag, Springer-Verlag New York, Inc., Attn: J. Jeng, 175 Fifth Avenue, New York, NY 10010-7858, USA, 1993. .

[GHRN93a] Dov M. Gabbay, C.J. Hogger, J.A. Robinson, and D. Nute, editors. *Deduction Methodologies*, volume 2 of *Handbook of Logic in Artificial Intelligence and Logic Programming*. Oxford Science Publications, Clarendon Press, Oxford, England, 1993.

[GHRN93b] Dov M. Gabbay, C.J. Hogger, J.A. Robinson, and D. Nute, editors. *Logical Foundations*, volume 1 of *Handbook of Logic in Artificial Intelligence and Logic Programming*. Oxford Science Publications, Clarendon Press, Oxford, England, 1993.

[GHRN94] Dov M. Gabbay, C.J. Hogger, J.A. Robinson, and D. Nute, editors. *Nonmonotonic Reasoning and Uncertain Reasoning*, volume 3 of *Handbook of Logic in Artificial Intelligence and Logic Programming.* Oxford Science Publications, Clarendon Press, Oxford, England, 1994.

[GHRN95] Dov M. Gabbay, C.J. Hogger, J.A. Robinson, and D. Nute, editors. *Epistemic and Temporal Reasoning*, volume 4 of *Handbook of Logic in Artificial Intelligence and Logic Programming.* Oxford Science Publications, Clarendon Press, Oxford, England, 1995.

[GHRN98] Dov M. Gabbay, C.J. Hogger, J.A. Robinson, and D. Nute, editors. *Logic in Logic Programming*, volume 5 of *Handbook of Logic in Artificial Intelligence and Logic Programming.* Oxford Science Publications, Clarendon Press, Oxford, England, 1998.

[GM93] M.J.C. Gordon and T.F. Melham. *Introduction to HOL: A theorem proving environment for higher order logic.* Cambridge Univ. Press, England, 1993.

[GP94] J.F. Groote and A. Ponse. Proof Theory for μCRL: a Language for Processes with data. In D.J. Andrews, J.F. Groote, and C.A. Middelburg, editors, *International Workshop on Semantics of Specification Languages*, pages 232–251. Springer–Verlag, 1994.

[GP95] J.F. Groote and A. Ponse. Syntax and Semantics of μCRL. In A. Ponse, C. Verhoef, and S.F.M. van Vlijmen, editors, *Algebra of communicating processes, Utrecht 1994*, pages 232–251. Springer–Verlag, 1995.

[Gro92] The RAISE Method Group. *The RAISE Method.* The BCS Practitioner Series. Prentice-Hall, Hemel Hampstead, England, 1992.

[Gro95] The RAISE Language Group. *The RAISE Specification Language.* The BCS Practitioner Series. Prentice-Hall, Hemel Hampstead, England, 1995.

[GvV95] J.F. Groote and S.F.M. van Vlijmen. A modal logic for μCRL. In A. Ponse, M. de Rijke, and Y. Venema, editors, *Modal logic and process algebra: a bisimulation perspective*, volume 53 of *CSLI lecture notes, Stanford*, pages 131–150. Springer–Verlag, 1995.

[HC94] Dang Van Hung and Zhou Chaochen. Probabilistic Duration Calculus for Continuous Time. Research Report 25, UNU/IIST, P.O.Box 3058, Macau, May 1994. Presented at *NSL'94 (Workshop on Non-standard Logics and Logical Aspects of Computer Science, Kanazawa, Japan, December 5–8, 1994)*, submitted to *Formal Aspects of Computing.*

[HG95] Dang Van Hung and Phan Hong Giang. A Sampling Semantics of Duration Calculus. Research Report 50, UNU/IIST, P.O.Box 3058, Macau, November 1995. Published in: *Formal Techniques for Real-Time and Fault Tolerant Systems*, Bengt Jonsson and Joachim Parrow (Eds), LNCS 1135, Spriger-Verlag, pp. 188–207, 1996.

[Hoa85] C.A.R. Hoare. *Communicating Sequential Processes.* Prentice-Hall International, 1985.

[Jac94] Michael Jackson. Problems, methods and specialisation. *Software Engineering Journal*, pages 249–255, November 1994.

[Jac95] Michael Jackson. *Software Requirements & Specifications: a lexicon of practice, principles and prejudices.* ACM Press. Addison-Wesley Publishing Company, Wokingham, nr. Reading, England; E-mail: ipc@awpub.add-wes.co.uk, 1995. ISBN 0-201-87712-0; xiv + 228 pages.

[Jac97] Michael Jackson. The meaning of requirements. *Annals of Software Engineering*, 3:5–21, 1997.

[Jon88a] Hans Jonkers. A Concrete Syntax for COLD-K. Technical Report METEOR/t8/PRLE/2, Philips Research Labs, January 1988.

[Jon88b] Hans Jonkers. An Introduction to COLD-K. Technical Report METEOR/t8/PRLE/8, Philips Research Labs, July 1988.

[Jon90] C.B. Jones. *Systematic Software Development using VDM.* Prentice Hall International, second edition, 1990.

[Jon93] Hans Jonkers. An Overview of the SPRINT Method. In J.C.P. Woodcock and P.G. Larsen, editors, *FME'93: Industrial-Strength Formal Methods*, pages 403–427. Formal Methods Europe, Springer-Verlag, April 1993. Lecture Notes in Computer Science 670.

[KvHV91] L.J.S̃omers K.M.ṽan Hee and M. Voorhoeve. The ExSpect tool. In *VDM '91: Formal Software Development Methods*, pages 683–684. Springer-Verlag, October 1991.

[Lan96] K. Lano. *The B Language and Method, A Guide to Pratical Formal Development.* Springer-Verlag, Formal Approaches to Computing and Information Technology (FACIT). Ed.: S.A. Schuman, 1996.

[MdL91] Kees Middelburg and G.R.R̃enardel de Lavalette. LPF and MPL_ω – A Logical Comparison of VDM SL and COLD-K. In *VDM '91: Formal Software Development Methods*, pages 279–308. VDM-Europe, Springer-Verlag, October 1991.
.

[Mil80] R. Milner. *Calculus of Communication Systems*, volume 94 of *Lecture Notes in Computer Science.* Springer-Verlag, 1980.

[Mil89] R. Milner. *Communication and Concurrency.* C.A.R. Hoare Series in Computing Science. Prentice Hall, 1989.

[Mos97] P.D. Mosses. COFI: The Common Framework Initiative for Algebraic Specification and Development. In M. Bidoit and M. Dauchet, editors, *TAPSOFT'97*, volume 1212 of *Lecture Notes in Computer Science.* Springer–Verlag, 1997.

[MP91] Zohar Manna and Amir Pnueli. *The Temporal Logic of Reactive Systems: Specifications.* Addison Wesley, 1991.

[MP95] Zohar Manna and Amir Pnueli. *The Temporal Logic of Reactive Systems: Safety.* Addison Wesley, 1995.

[MW93] Ursula Martin and Jeannette M. Wing, editors. *First International Workshop on Larch.* Workshops in Computing. Springer-Verlag, Springer-Verlag New York, Inc., Attn: J. Jeng, 175 Fifth Avenue, New York, NY 10010-7858, USA, July 1993. .

[Nak97] Kokichi Futatsugiand Ataru Nakagawa. An Overview of CAFE Specification Environment – An Algebraic Approach for Creating, Verifying, and Maintaining Formal Specifications over Networks. In *ICFEM'97: International Conference on Formal Engineering Methods.* IEEE Computer Society, IEEE CS Press, November 1997.

[NSF] Ataru T. Nakagawa, Toshimi Sawada, and Kokichi Futatsugi. *CafeOBJ manual (for system version 1.3).* 142 pages.

[oLD97] CoFI Task Group on Language Design. CASL — The Common Algebraic Specification Language Summary. Available at http://www.brics.dk/Projects/CoFI/Documents/CASL/Summary/, 1997.

[oS97] CoFI Task Group on Semantics. CASL — The CoFI Algebraic Specification Language (version 0.97) Semantics. Available at http://www.brics.dk/Projects/CoFI/Notes/S-4/, 1997.

[Rei85] W. Reisig. *Petri Nets*, volume 4 of *EATCS Monographs: Theoretical Computer Science.* Springer–Verlag, Heidelberg, 1985.

[Rei98] W. Reisig. *Elements of Distributed Algorithms — Modeling and Analysis with Petri Nets.* Springer–Verlag, Heidelberg, 1998.

[Ros97] A. W. Roscoe. *Theory and Practice of Concurrency.* Prentice–Hall, 1997.

[SM98] A. Sutcliffe and N. Maiden. The domain theory for requirements engineering. *IEEE Transactions on Software Engineering*, 24(3):174–96, 1998. .

[SMV] K.L. McMillan *The SMV System* Carnegie Mellon University, School of Computer Science, Pittsburgh, Penn., USA, February 1992

[Spi88] J. Michael Spivey. *Understanding Z: A Specification Language and its Formal Semantics*, volume 3 of *Cambridge Tracts in Theoretical Computer Science.* Cambridge University Press, UK, January 1988.

[Spi89] J. Michael Spivey. *The Z Notation: A Reference Manual.* International Series in Computer Science. Prentice Hall, Hemel Hempstead, Hertfordshire HP2 4RG, UK, 1989.

[SS90] G. Stålmarck and M. Säflund. Modelling and Verifying Systems and Software in Propositional Logic. In B.K. Daniels, editor, *Safety of Computer Control Systems 1990 (SAFECOMP'90)*, pages 31–36. Pergamon Press, Oxford, 1990.

[Wor96] John Wordsworth. *Software Engineering with B*. Addison-Wesley Longman, 1996.

[ZJ97a] P. Zave and M. Jackson. Four dark corners of requirements engineering. *ACM Transactions on Software Engineering and Methodology*, 6(1):1–30, January 1997. .

[ZJ97b] P. Zave and M. Jackson. Requirements for telecommunications services: an attack on complexity. In *Proceedings of the Third IEEE International Symposium on Requirements Engineering (Cat. No.97TB100086)*, pages 106–117. IEEE Comput. Soc. Press, 1997. .

3 The FME Rail Railway–related Bibliography

References

[1] *Symposium on "Railway Cybernetics"*, 1979.

[2] The European Rail Network. UIC–CCFE, Paris, France, 1995.

[3] A. Casaza abd Dario Comini, Agelo Morzenti, Matteo Pradella, Pierluigi San Pietro, and Fabio Schreiber. Interlocking: Specification and Test Case Generation for the Safety Kernel of the Naples Subway. In Markus Montigel, editor, *FME Rail Workshop # 3*, volume # 3 of *FME Rail Workshop; St. Pölten*. FME: Formal Methods Europe, Fachhochschulstudiengang St. Pölten, Herzogenburgerstr. 68, A-3100 St. Pölten, Austria; Phone: +43 2742 313 228, Fax: +43 2742 313 229, February 17–19 1999. **RaCoSy Repository**. Petri Net.

[4] P. Abdulla, E. Ciapessoni, P. Marmo, K. Meinke, and E. Ratto. FAST: An Integrated Tool for Verification and Validation of Real-Time System Requirements. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Prover Techn., Sweden (PA+KM), Ansaldo, Neapels, Italy (EC+ER) and ENEL–SRI, Milano, Italy (PM). **RaCoSy Repository**. FAST.

[5] S. Agerholm, P.-J. Lecoeur, and E. Reichert. Formal Specification and Validation at Work: A Case Study using VDM-SL. In *Proceedings of Second Workshop on Formal Methods in Software Practice*. ACM, Florida, March 1998. .

[6] Sten Agerholm, Pierre Lecoeur, and Etienne Reichert. Formal Specification at Work: A Case Study using VDM–SL. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. IFAD, Denmark (SA) and Dassault Electronique, France (PL+ER). **RaCoSy Repository**. VDM, VDM–SL.

[7] P. Alle. Improving Rail Transit Line Capacity Using Computer Graphics. *Logist. and Transp. Rev. (Canada)*, 17:429–442, 1981.

Keywords: I3m railway systems simulation .

[8] A. M. Amendola, L. Impagliazzo, P. Marmo, and F. Poli. Experimental Evaluation of Computer-Based Railway Control Systems. In *Proceedings of The Twenty-Seventh Annual International Symposium on Fault-Tolerant Computing (FTCS'97)*, pages 380–384, Washington - Brussels - Tokyo, June 1997. IEEE. .

[9] A. Anselmi, C. Bernardeschi, A. Fantechi, S. Gnesi, S. Larosa, G. Mongardi, and F. Torielli. An Experience in Formal Verification of Safety Properties of a Railway Signalling Control System. In Gerhard Rabe, editor, *SAFECOMP'95: 14th International Conference on Computer Safety, Reliability and Security*, pages 474–488, Belgirate, Italy, 1995. Springer-Verlag. .

[10] G. Aprea, P. Colantuoni, P. Firpo, R.Lido, D. Pellegrino, M. Rapone, and F. Senesi. SIGAV, the Italian High Speed Railway Integrated Management System: Safety and Reliability Overview. In Erwin Schoitsch, editor, *SAFECOMP'96: 15th International Conference on Computer Safety, Reliability and Security*, page 250, Vienna, Austria, 1996. Springer. .

[11] Railway Industry Association. Safety Related Software for Railway Signalling. RIA 23, version 1.0, British Railways Board/London Underground Limited, Railway Industry Association, 6 Buckingham Gate, London SW1E 6JP, UK, 1991. .

[12] W. Atkinson and J. Cunningham. Proving properties of a safety-critical system. *Software Engineering Journal*, 6(2):41–50, March 1991.

Abstract: The paper describes the FOREST approach to formal requirements specification and particularly the role of an automated theorem prover in validating specifications written in MAL, the FOREST logic. The MAL prover uses a tableau method for constructing its proofs, with rules to handle the action modalities and quantification of MAL. The authors illustrate its use in validation by using the prover to establish that a safety-critical railway-signalling specification has some desirable safety properties.

Keywords: formal specification; program verification; safety; software reliability; theorem proving FOREST. .

[13] C. Bailey, editor. *European Railway Signalling*, London, England, 1995. Institution of Railway Signalling Engineers, A&C Black. Referenced in [153] .

[14] T. Basten, R.N. Bol, and M. Voorhoeve. Simulating and Analyzing Railway Interlocking in ExSpect. Technical Report 94-37, Department of Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands, September 1994. See [15].

Abstract: This paper describes a study on simulating and analyzing interlocking specifications in the Interlocking Specification Language (ISL), using the tool ExSpect. ExSpect is a toolkit based on the theory of coloured Petri nets. An approach to translating ISL to ExSpect is suggested. Experimental results of simulating and analyzing part of an ISL specification in ExSpect are discussed. ExSpect seems to be useful for simulating and analyzing ISL specifications. Furthermore, several interesting topics for future research are identified ExSpect.

[15] T. Basten, R.N. Bol, and M. Voorhoeve. Simulating and analyzing railway interlockings in ExSpect. *IEEE Parallel & Distributed Technology: Systems & Applications*, 3(3):50–62, Fall 1995. See [14].

Abstract: This paper evaluates the ability of ExSpect, a toolkit for simulating and analyzing complex distributed systems using colored Petri nets, to analyze ISL specifications for railway interlockings.

Keywords: railways; colored Petri nets; complex; Computational linguistics; Computer simulation; digital simulation; Distributed computer systems; distributed systems; Electric railroads; ExSpect; formal specification; Interlocking signals; Interlocking specification language; ISL specifications; Railroad traffic control; railway interlockings; software toolkit; digital simulatio ExSpect.

[16] M. A. Bayfield. British rail graphics systems. *Displays Technology and Applications*, 1:95–101, July 1979.

Keywords: Applications, transportation .

[17] D Beattie. Should Dangerous Goods be Moved by Rail rather than by Road? *SARSS'89: Reliability on the Move*, page 149, 1989. .

[18] A. Bechina, J. Hermle, and M. Siormanolakis. Using Prolog for a railway control system. In *Fourth International Conference on the Practical Application of Prolog; London, UK*, pages 19–30. Practical Application Co., Blackpool, UK, 1996.

Abstract: During the last years there has been a rapidly growing interest in the transportation and logistics domain for systems based on artificial intelligence techniques. This paper proposes a practical approach to an actual planning problem of a railway interlocking. A railway interlocking is defined as a system that is used to guarantee safe train movements. Often railway interlockings are systems of relays controlled by computer equipment and/or human operators. In order to adapt to a dynamic environment without creating dangerous situations, a formalism for describing safety requirements and interlocking behaviour is needed. This study intends to show why a logic programming language is a strong candidate for handling such a formalism. This work exploits the advantage of using external procedures written in other languages which is supplied by many software manufacturers of Prolog systems. The openness of Prolog makes it a powerful language to describe the complex environment of a railway system.

Keywords: formal specification; logic programming; planning; PROLOG; rail traffic; safety; traffic control; transport control Logic Programming, Prolog.

[19] P. Behm and J.-M. Meynadier. Météor: an Industrial Success in Formal Development. In *FME Rail Workshop 1*. Matra Transport International, a joint Matra and Siemens company, 1998. In: [185] **RaCoSy Repository**.

[20] M. Russell Bentley and Mark Boggs. Utilization of GIS in the Decision Making Process of a Transportion Master Plan: The Interstate 4 Multi-Modal Master Plan. In *Proceedings of 1996 ESRI User Conference*, Palm Springs, California, 1996.

Abstract: The east-central region of Florida, including Orlando, has experienced extremely dynamic growth in the past two decades. This has placed a continual strain on the existing transportation network. The region's primary transportation artery, Interstate 4, is experiencing much of this strain. In order to alleviate the congestion on I-4 and prepare for the future growth of the region, the State of Florida Department of Transportation (District 5) is preparing a comprehensive master plan to guide future improvements to I-4. Alternatives vary in scope from the simple addition of lanes, to the addition of extensive high occupancy vehicle lanes, park and ride facilities, and urban rail systems.

As alternatives have been developed, GIS has been introduced as a means of evaluation to assist in deciding which ones best meet the overall needs and concerns of the region. It is the purpose of this paper to describe the alternatives and illustrate how GIS is aiding planners in this complex decision making process. Two primary GIS applications will be described: the determination of wetland impacts and right-of-way acquisition costs. Each application will include a discussion of database creation using high resolution aerial photography, the overlay analysis, final reporting procedures, and benefits of using GIS versus previous methods of evaluation .

[21] Anders Berg. Adtranz Signal's Formal Verification Process: Safety Verification of Interlocking Functionality. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Adtranz, Sweden. **RaCoSy Repository**. STERNOL.

[22] J. Berger, P. Middelraad, and A.J. Smith. The European railway interlocking specification. In *IRSE*, pages 70–82, 1993. Referenced in [153] .

[23] J.A. Bergstra, W.J. Fokkink, W.M.T. Mennen, and S.F.M. van Vlijmen. *Spoorweglogica via EURIS*, volume 22 of *Quaestiones infinitae*. Universiteit Utrecht, Faculteit Wijsbegeerte, 1997. In Dutch. .

[24] C. Bernardeschi, A. Fantechi, S. Gnesi, and G. Mongardi. Proving safety properties for embedded control systems. In A. Hlawiczka, J.G. Silva, and L.Simoncini, editors, *Dependable Computing - EDCC-2. Second European Dependable Computing Conference Proceedings; Taormina, Italy*, pages 321–32. Springer-Verlag; Berlin, Germany, 1996.

Abstract: It is well known that a fundamental problem in embedded control systems is the verification of the safety requirements. Formal methods and related support tools can successfully be applied in the formal proof that a system is safe. However, the complexity of real systems is such that automated tools often fail to formally validate such systems. A typical case is when "state explosion" problems arise. We show some "abstraction techniques" to make the problem of safety requirements validation tractable by current tools. These abstraction techniques have been defined inside a verification methodology that has been tested on the specification of a railway computer based interlocking signalling control system. The conditions under which this methodology can be applied to systems in different application areas are finally discussed.

[25] W. M. Beynon, M. Slade, and Y. P. Yung. Protocol Specification in Concurrent Systems Software Development. Research Report CS-RR-163, Department of Computer Science, University of Warwick, Coventry, UK, September 1990.

Abstract: A protocol specification technique that relates concurrent system behaviour to agent activity and interaction at a high level of abstraction is described. This exploits a concurrent programming technique based on a synthesis of two new programming paradigms: "agent-oriented" and "definition-based" programming. Application of the method to modelling and simulation activity at a railway station is described. Its potential for concurrent systems software requirements specification is assessed .

[26] D. Bjørner. A Architecture for Running Map Systems. Technical Report db/arch/01, UNU/IIST, the UN University's International Institute for Software Technology, P.O.Box 3058, Macau; E-Mail: `library@iist.unu.edu`, February 1994.
Incomplete draft — the result of one week's work over Chinese New Year 1994!

FME Rail Annotations:

- **Rail subject:** Train despatch and traffic monitoring.
- **Principles, techniques, tools:** Domain and requirements engineering, software architecture, VDM.
- **Notes:** Proposes a concrete solution to the display and manipulation of (abstractions) of data screen layouts for train running maps.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository. VDM, VDM–SL.

[27] D. Bjørner. Models of the Railway Infratructure. In *FME Rail Workshop 1*, Bldg. 344, DK–2800 Lyngby, Denmark, 1998. Dept.IT, Techn. Univ. of Denmark. Copy of [28]. In: [185] **RaCoSy Repository**.

[28] D. Bjørner, C.W. George, B.S. Hansen, H. Laustrup, and S. Prehn et al. A Railway System, Coordination '97: Case Study Workshop Example. Technical Report 93, UNU/IIST, P.O.Box 3058, Macau, Spring 1997 – Fall 1998.
Torso: The report in grossly incomplete.
With contributions from: Jakob Braad, Jon Fuglsang, Karin S. Mogensen and Ulrik Svanlund.

Abstract:
This report presents a solution to the problem presented by the organisers of a Case Study Workshop in connection with "Coordination'97: The Second Intl. Conference on Coordination Models and Languages, Berlin, September 4, 1997".
The solution covers three stages of development: A domain theory of railway systems, a set of requirements definitions, a computing systems architecture and a program organisation. All stages are both informally and formally described in the RAISE Specification Language, RSL, and correctness relations are formally expressed using the RAISE Method Implementation Relation.

Keywords: domain engineering; requirements engineering; railway systems; RAISE; RSL.

FME Rail Annotations:

- **Rail subject:** Railway domain.
- **Principles, techniques, tools:** Domain engineering: intrinsics, RAISE, RSL.
- **Notes:** The approach of this report is suggested as indicative, i.e. as a model for one of a set of normative descriptions of the domain of railway systems.
  DB intends to have the present report reworked rather completely during the winter of 1998/1999 and the spring of 1999.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository. RAISE/RSL.

[29] D. Bjørner, C.W. George, and S. Prehn. *Scheduling and rescheduling of trains*, page 24 pages. Academic Press, 1999.

FME Rail Annotations:

- **Rail subject:** Scheduling, rescheduling.
- **Principles, techniques, tools:** RAISE, RSL.
- **Notes:** Main author: Chris George.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository.

[30] D. Bjørner, Dong YuLin, and S. Prehn. Domain Analysis: A Case Study of Railway Station Management. Technical Report db/03/01, UNU/IIST, the UN University's International Institute for Software Technology, P.O.Box 3058, Macau; E-Mail: `library@iist.unu.edu`, November 12 1994.
Presented at KICS'94: The Kunming (Yunnan, PRC) Intl. CASE Symposium, Nov. 1994.

FME Rail Annotations:

- **Rail subject:** Railway station management, rail topology, signalling.
- **Principles, techniques, tools:** Domain engineering: intrinsics, RAISE, RSL.
- **Notes:** Somewhat dated model.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository. RAISE/RSL.

[31] Dines Bjørner, Jakob Braad, and Karin S. Moensen (Eds.). Models of Railway Systems: Domain. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. (60 pages) Dept. of IT, Techn. Univ. of Denmark. **RaCoSy Repository**. RAISE/RSL.

[32] Dines Bjørner, Jakob Braad, and Karin S. Moensen (Eds.). Models of Railway Systems: Requirements. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. (62 pages) Dept. of IT, Techn. Univ. of Denmark. **RaCoSy Repository**. RAISE/RSL.

[33] G. Blanke. Simulation of GSM Data Channels in a Safety Critical Railway Environment. *Lecture Notes in Computer Science*, 783:334–??, 1994. .

[34] Maarten Boasson. Distributed Decisions and Asynchronous Communication. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Holland Signaalapparaten B.V. and Univ. of Amsterdam, The Netherlands. **RaCoSy Repository**.

[35] R.N. Bol, J.W.C. Koorn, L.H. Oei, and S.F.M. van Vlijmen. Syntax and Static Semantics of the Interlocking Design and Application Language. Technical Report P9422, Programming Research Group, University of Amsterdam, Kruislaan 403, 1098 SJ Amsterdam, The Netherlands, November 1994.

Abstract: An interlocking is a system used at railway yards for guaranteeing safety of train movements. This report opens a series of studies on tightly related specification languages for interlockings. These languages together are called ISL. Interlocking Specification Language. ISL is designed by P. Middelraad of the Dutch railway company, NS, de Nederlandse Spoorwegen. NS have developed a symbolic intermediate tool interface language, IDEAL, for ISL. IDEAL is the Interlingua for all men and machines using ISL. This report introduces interlockings, the long-term goals of the ISL project, and, as a first step, we present the syntax and static semantics of IDEAL in ASF+SDF, an algebraic specification formalism. Several improvements of IDEAL are suggested ExSpect.

[36] A. Borälv. A Fully Automated Approach for Proving Safety Properties in Interlocking Software Using Automatic Theorem-Proving. In S. Gnesi and D. Latella, editor, *Proceedings of the Second International ERCIM Workshop on Formal Methods for Industrial Critical Systems*, pages 39–62. Consiglio Nazionale Ricerche, Pisa, July 1997. .

[37] A. Borälv. The industrial success of verification tools based on Stålmarck's method. In O. Grumberg, editor, *Computer Aided Verification*, 9th International Conference, CAV'97, pages 7–10. Springer-Verlag, 1997.

Abstract: Stålmarck's method (G. Stålmarck, 1992; 1994) is a patented natural deduction proof method with a novel proof-theoretic notion of proof depth, defined as the largest number of nested assumptions in the proof. An implementation of the method, called Prover, has been used as proof engine in various commercial tools since 1990, and is now integrated in a formal verification framework called NP-Tools. Prover searches for shallow sub formula proofs, which has proven to be an efficient strategy for solving many industrial problems, the largest of which today consists of several 100,000's of sub formulas. Stålmarck's method is in industrial use, for instance in the areas of telecom service specification analysis, analysis of **railway interlocking** software, analysis of programmable controllers and analysis of aircraft systems. The method seems suitable also for hardware verification.

Keywords: railway interlocking, formal specification; formal verification; hardware description languages; railways; telecommunication computing; theorem proving Stålmarck's Method.

[38] A. Borälv. The Industrial Success of Verification Tools Based on Stålmarck's Method. In Orna Grumberg, editor, *Proceedings of the Ninth International Conference on Computer Aided Verification*, volume 1254 of *Lecture Notes in Computer Science*, pages 7–10. Springer Verlag, 1997. **RaCoSy Repository**.

[39] A. Borälv. Formal Methods in Computerised Railway Interlocking at ADTranz. In *FMERail Workshop 1*, Stockholm, Sweden, 1998. Prover Technology AB. In: [185]. 11 page OH Foil Presentation **RaCoSy Repository**.

[40] A. Borälv and G. Stålmarck. Prover Technology in Railways. In Michael G. Hinchey and Jonathan P. Bowen, editors, *Industrial-Strength Formal Methods*, International Series in Formal Methods. Academic Press, 1998. In preparation .

[41] A. Borälv and G. Stålmarck. Prover Technology in Railways. In *FMERail Workshop 1*, Stockholm, Sweden, 1998. Prover Technology AB. In: [185]. Chapter preprint from *Industrial Strength Formal Methods*, Academic Press, 1998, Eds. J.P. Bowen and M. Hinchey **RaCoSy Repository**.

[42] Arne Borälv and Carl-Johan Block. Formal Verification Tools in Swedish Railways 1989–1999. In Dines Bjørner and Maria Fahlén, editors, *FMERail Workshop # 4*, volume # 4 of *FMERail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Prover Technology, Sweden. **RaCoSy Repository**. Stålmarck's Method.

[43] Jakob Braad and Karin S. Mogensen. Interlocking: Specification and Test Case Generation for the Safety Kernel of the Naples Subway (Based on: [3]). In Dines Bjørner and Maria Fahlén, editors, *FMERail Workshop # 4*, volume # 4 of *FMERail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. textslOne of a series of exercise reports re-modelling given example solutions [44, 206, 208, 207, 205, 45]Dept. of IT, Techn.Univ. of Denmark. **RaCoSy Repository**. RAISE/RSL.

[44] Jakob Braad and Karin S. Mogensen. Interlocking: The B Method (Draft) (Based on: [257]). In Dines Bjørner and Maria Fahlén, editors, *FMERail Workshop # 4*, volume # 4 of *FMERail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. *One of a series of exercise reports re-modelling given example solutions [43, 206, 208, 207, 205, 45]* Dept. of IT, Techn.Univ. of Denmark. **RaCoSy Repository**. The B Method.

[45] Jakob Braad and Karin S. Mogensen. The Automatic Railway Case (Based on [103]). In Dines Bjørner and Maria Fahlén, editors, *FMERail Workshop # 4*, volume # 4 of *FMERail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. textslOne of a series of exercise reports re-modelling given example solutions [44, 43, 206, 208, 207, 205]Dept. of IT, Techn.Univ. of Denmark. **RaCoSy Repository**. RAISE/RSL.

[46] R. A. Brand. 3-D Colour Graphics for Rail Network Simulation and Control. In Anonymous, editor, *First Australasian Conf. on Computer Graphics*, pages 38–48. 1983.

Keywords: I3m Railways and I3m Timetable Generation .

[47] R. A. Brand. 3-D colour graphics for rail network simulation and control. In *First Australasian Conf. on Computer Graphics*, pages 38–48, 1983.

Keywords: I3m Railways, I3m Timetable Generation .

[48] V. Van Breusegem, G. Campion, and G. Bastin. Traffic Modelling and State Feedback Control for Metro Rail Lines Based on Linear Discrete–Event State–Space Models. *IEEE Trans. Autom. Control*, 36(7):770–784, July 1991. .

[49] British Railways Board Issue SSI8003. *SSI data preparation guide*, February 1990. .

[50] Manfred Broy. Specification of a Railway System. Technical report, University of Passau, Bavaria, Germany, 1987. .

[51] G. Bruno, G. Ghiani, and G. Improta. Models and algorithms for the design of rapid transit networks. In *Proc. 7th Int. Special Conf. IFORS, Information Systems in Logistics and Transportation*, June 1997.

Abstract: Traditional underground metro systems, rapid rail transit systems are becoming more and more common to improve mobility in large urban areas. The design of such systems is a very critical task which has long term effects on modal aplit. Decisions are to be made about topological configuration, the number and location of lines and stations, line frequencies etc.. In this context decision making is a complex job as several players are involved, some objectives are unquantifiable and estimation of the non-inferior solutions set considering the two main quantifiable objectives (e.g. the construction cost and a measure of the social benefit); second, the choice, among the previously selected solutions, of the most suitable configuration by means of the remaining objectives. In the present paper we tackle the first step generalising a k-shortest path technique in such a way to consider complex topological patterns (grids, stars, cartwheels, triangles etc.). The proposed method was used to simulate the Rome metro system .

[52] A. Bud, A. Nicholson, and B. Chandra. Scheduling trains with genetic algorithms. Technical Report 96/250, Dept. Computer Science, Monash University, Australia 3168, October 1996. http://www.cs.monash.edu.au/ (CSci Monash home) .

[53] Michael R. Bussieck, Peter Kreuzer, and Uwe T. Zimmermann. Optimal Lines for Railway Systems. Technical Report TR-95-01, MOTUBS, 1995. .

[54] E. Canver, J.T. Gayen, and A. Moik. Formal specification of the controller software on railway switch example. *Automatiserungs Praxis*, 1997.

Abstract: This paper describes the results of a case study to assess the feasibility of formal methods provided by the verification support environment (VSE). VSE is a tool for formal specification and verification of safety critical software systems. The assessment is based on an application of VSE to develop the controller software for the computer driven electrical, locally operated railway switch. The electrical locally operated railway switch is set up and being used in low speed track systems. The switch handling is initiated by the railway switch. The case study has been carried out by a group of researchers from different disciplines, who tried to integrate an engineer's "application oriented" approach with a formal method from the area of computer science.

Keywords: computerised control; formal specification; rail traffic; safety-critical software; switching **RaCoSy Repository**.

[55] L. Ceglowski and A. Lewinski. Highly Reliable Microcomputer Systems for Railway Control. *SARSS'87: Achieving Safety and Reliability with Computer Systems*, page 182, 1987. .

[56] CENELEC European Committee for Electro-technical Standardisation. *CENELEC 50127-1: Railway Applications – Guide to the specification of a guided transport system, Part 1: General.* Referenced in [177] .

[57] CENELEC European Committee for Electro-technical Standardisation. *CENELEC 50128: Railway Applications – Software for railway control and protection systems.* Referenced in [177] .

[58] CENELEC European Committee for Electro-technical Standardisation. *CENELEC 50129: Railway Applications – Safety related electronic systems for signalling.* Referenced in [177] .

[59] CENELEC European Committee for Electro-technical Standardisation. *CENELEC EN 50126: Railway Applications – the specification and demonstration of Reliability, Availability, Maintainability and Safety.* Referenced in [177] .

[60] Ján Černý. Supply/Demand relation on a single bus route. In *The 9-th International Scientific Conference*. 1990. .

[61] Ján Černý and Pavol Kluvánek. *Foundations of Mathetical Theory of Transport.* Publishing House of the Slovak Academy of Sciences, Bratislava, 1991. .

[62] ?? Chapront. Future of Formal Methods. In Thierry Lecomte and Peter Gorm Larsen, editors, *FMERail Workshop # 5*, volume # 4 of *FMERail Workshop; Tolouse, France.* FME: Formal Methods Europe, Steria, France, September 22–24 1999. ??? (Was document distributed ?) Alstom, France.

[63] P. Chapront. Vital coded processor and safety related software design. In H. H. Frey, editor, *Safety of Computer Control Systems 1992 (SAFECOMP 92) Computer Systems in Safety-Critical Applications. Proceedings of the IFAC Symposium*, pages 141–145. Div. of Transp., GEC Alsthom, Saint-Ouen, France, Pergamon, Oxford, UK, 29-30 Oct. 1992. .

[64] Tommy W. S. Chow and Oulian Shuai. Feedforward Neural Networks Based Input-Output Models for Railway Carriage System Identification. *Neural Processing Letters*, 5(2):57–67, 1997. .

[65] Morris Chudleigh and James Catmur. Independent Safety Assessment of Rail Systems in their Operational Environment. In F. Redmill and T. Anderson, editors, *Achievement and Assurance of Safety: Proceedings of the 3rd Safety-critical Systems Symposium*, pages 80–89, Brighton, 1995. Springer. .

[66] Tadeusz Cichocki and Janusz Górksi. Safety Assessment of Computerised Railway Signalling supported by Formal Methods. In Thierry Lecomte and Peter Gorm Larsen,

editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Adtranz, Katowice, Poland (TC) and Techn.Univ. of Gdańsk, Poland. **RaCoSy Repository**. Z and Z–variants.

[67] M. T. Claessens and N. M. van Dijk. A mathematical programming model to determine a set of operation lines at minimal costs. Technical report, University of Amsterdam, 1994. .

[68] Robin Cook. Management of Dependability: A Railway Perspective. In Felix Redmill and Tom Anderson, editors, *Safety-Critical Systems: The Convergence of High Tech and Human Factors: Proceedings of the 4th Safety-critical Systems Symposium Leeds, UK 6-8 February 1996*, pages 61–70, Leeds, UK, 1996. Springer. .

[69] Teodor Gabriel Crainic and Jacques Roy. OR tools for tactical freight transportation planning. *EUJOR*, 33:290–297, 1988. .

[70] A.H. Cribbens. Solid Sate Interlocking (SSI): An integrated electronuc signalling system for mainline railways. In *IEE Proceedings*, volume 134(3), pages 148–158, 1987. .

[71] A.H. Cribbens and I.H. Mitchell. The Applicaiton of Advanced Computing Techniques to the Generation and Checking of SSI Data. In *IRSE*, London, England, 1992. Referenced in [153] .

[72] R.W. Crookes, C.D.M. Oates, D.M. Brooks, and M. Cowen. A high integrity monitor for signalling interference prevention at 50 Hz. In *International Conference on Electric Railways in a United Europe (Conf. Publ. No.405)*, pages 143–7. IEE, 1995.

Abstract: The design of a high integrity monitor for the prevention of signalling interference is described. It belongs to the family known as Interference Current Monitor Units, or ICMUs, and has to be extremely reliable since a fault would otherwise compromise railway safety; a calculated value of Mean Time Between Wrong Side Failure (MTBWSF) of five thousand million hours was specified and achieved. High levels of out of band currents had to be rejected, in particular up to 2 kA DC The basic design was kept as simple as possible with only one frequency band being detected. A hardware only solution, i.e. no software, was adopted and triplication of the circuit was used to achieve the MTBWSF specification.

Keywords: automatic test equipment; computerised monitoring; electric current measurement; interference suppression; railways; reliability; safety; signalling **RaCoSy Repository**.

[73] J. Cullyer and J. Fairclough. Safety critical systems - when computers might kill. *Information Technology & Public Policy*, 11(1):14–19, 1992.

Abstract: In order to protect both human life and the environment of the Earth, certain classes of automated control systems in industries such as nuclear power, aviation and railway signalling are subject to independent analysis and certification, before operational use is permitted. Although comparatively small, the UK safety critical control business brings substantial kudos and visibility to those companies with the scientific and engineering skills needed to satisfy the strict demands of the regulatory bodies. The subject is deeply rooted in the technology of so-called 'embedded computer systems'. The techniques which have been developed for the specification, design and verification of such systems are intended to provide a practical route for the development of such highly critical systems, at a cost which is acceptable to the operator of the potentially hazardous plant or vehicle. The results of UK research and development have been a major influence in the derivation of both national and international standards for safety-critical systems. The UK Ministry of Defence is regarded as a leader in these disciplines, with Interim Defence Standards 00-55 and 00-56 being primary inputs to debates in NATO on the safety of flight control and weapons systems. In the civil sector, the UK has been prominent in the derivation of the International Electrotechnical Commission Standards (65A/94 and 65A/96) for safety-critical systems, which have been promulgated recently. Unfortunately, these skills in the regulatory regime have not been reflected in any increase in the UK share of the market, for reasons which one dealt with .

[74] J. Cullyer and Wong Wai. Application of formal methods to railway signalling - a case study. *Computing & Control Engineering Journal*, 4(1):15–22, Feb. 1993.

Abstract: Describes techniques for applying formal mathematical methods to the specification and design of railway signalling and interlocking equipment which is implemented using microprocessors and real-time software. The results have been obtained by combining the specification language Higher-Order Logic (HOL) with the disciplined use of annotated subsets of the computer programming languages such as Ada. A global framework has been developed both for computer-aided design (CAD) tools for railway interlocking and for the future development of the operational software for practical signalling systems.

Keywords: CAD; computerised control; formal languages; formal logic; formal specification; high level languages; railways; real-time systems; signalling; specification languages **RaCoSy Repository**. ccs.

[75] W. J. Cullyer and Wong Wai. A Formal Approach to Railway Signalling. In *Compass '90: 5th Annual Conference on Computer Assurance*, pages 102–108, Gaithersburg, Maryland, 1990. National Institute of Standards and Technology. .

[76] W.J. Cullyer and J.W. Wise. Application of Formal Methods to Railway Signalling. *SARSS'89: Reliability on the Move*, page 11, 1989. .

[77] A. Cuppari and F. Zini. an Agent-based Prototype for Freight Traffic Management. In Thierry Lecomte and Peter Gorm Larsen, editors, *FMERail Workshop # 5*, volume # 4 of *FMERail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Italien State Railways (AC) and Univ. of Genoa, Italy (FZ). Logic (Non–Modal)/Logic Programming, Prolog.

[78] Jin Danhua. A Second Math. Model of Train Time Tabling. Technical Report jdh/math/05, UNU/IIST, the UN University's International Institute for Software Technology, P.O.Box 3058, Macau; E-Mail: `library@iist.unu.edu`, October 1994. RAISE/RSL.

[79] R. De Lemos, A. Saeed, and T. Anderson. A train set as a case study for the requirements analysis of safety-critical systems. *The Computer Journal*, 35(1):30–40, February 1992.

Keywords: Rail-traffic systems, Remote signalling, dispatching and safety devices, Formal logic, Actuators; actuators; development; digital control; formal logic; Formal models; formal models; Logical formalism; logical formalism; Mission; mission; Net formalism; net formalism; of operation; Physical laws; physical laws; Predicate-transition nets; predicate-transition nets; railways; Requirement analysis; requirement analysis; rules; Rules of operation; safety systems; Safety-critical systems; safety-critical systems; system; System development; System sensors; system sensors; Timed history logic; timed history logic; Train set system; train set system .

[80] Zhao Debin, Zhang Shixiong, and Gao Wen. The implementation of automatic monitoring network system for trains. In *Proceedings TENCON '93. 1993 IEEE Region 10 Conference on 'Computer, Communication, Control and Power Engineering' (Cat.No.93CH3286-2)*, volume 4, pages 72–5. IEEE, IEEE, 1993.

Abstract: The paper presents the implementation of Automatic Monitoring Network System for Trains (AMNST), and describes the dynamically remote real time network monitoring method for the safe running of trains, and discusses the configuration of network hardware, the design and implementation of the network software. The method has been used in the Da-Qin railway monitoring system and the results are satisfied.

Keywords: computer networks; computerised monitoring; railways; telemetry **RaCoSy Repository**.

[81] P. Dechering, R. Groenboom, E. de Jong, and J.T. Udding. Formalisation of a Software Architecture for Embedded Systems: a Process Algebra for SPLICE. In *FME Rail Workshop 1*, 1st and 3rd author: P.O.Box 42, NL–7550 GD Hengelo, The Netherlands; B.V.; 2nd and 4th author: P.O.Box 800, NL–9700 AV Groningen, The Netherlands, 1998. 1st and 3rd author: Applied Systems Research, Hollandse Signaalapparaten B.V.; 2nd and 4th author: Dept. Comp. Sci., Univ. of Groningen. In: [185] **RaCoSy Repository**.

[82] Gebhard Decknatel. Modelling Train Movement with Hybrid Petri Nets. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Univ. Braunschweig, Germany. **RaCoSy Repository**. Petri Net.

[83] B. Dehbonei and L.-F. Mejia. Formal Development of Software in Safety-Critical Railway Systems. In B. T. K. S. Murthy, C. A. Mellitt, G. Brebbia, and S. Sciutto, editors, *Railway Operations*, volume 2, pages 213–219. COMPRAIL94, Computational Mechanics Publications, 1994. .

[84] B. Dehbonei and L.-F. Mejia. Formal methods in the railways signalling industry. In M. Naftalin, T. Denvir, and M. Bertran, editors, *FME '94: Industrial Benefit of Formal Methods. Second International Symposium of Formal Methods Europe. Proceedings; Barcelona, Spain*, pages 26–34. Springer-Verlag, Berlin, Germany; Lecture Notes in Computer Science LNCS, 1994.

Abstract: Software is becoming increasingly involved in safety-critical systems. Such systems are ideal fields of application of formal methods. A rigorous development accompanied by formal proofs is a guarantee of the correctness of the development. We summarize our experience of using the B formal method in the development of safety-critical railway signalling applications. Our applications range in size from 2000 lines to 22000 lines. They are specified, refined and implemented in B. Issues (technical and non technical) related to the utilization of B are discussed and solutions presented.

Keywords: safety-critical software; signalling; traffic control; traffic engineering computing The B Method.

[85] B. Dehbonei and L.-F. Mejia. Formal Development of Safety-Critical Software Systems in Railway Signaling. In M. G. Hinchey and J. P. Bowen, editors, *Applications of Formal Methods*, Series in Computer Science, pages 227–252. Prentice Hall International, 1995. .

[86] Pierre Desforges. RATP Interlocking System Experience. In Dines Bjørner and Maria Fahlén, editors, *FMERail Workshop # 4*, volume # 4 of *FMERail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. RATP, Paris, France. **RaCoSy Repository**. The B Method.

[87] Hartmut Dienst. *Linienplanung im spurgeführten Personenfernverkehr mit Hilfe eines heuristischen Verfahrens*. PhD thesis, TU Braunschweig, 1978. .

[88] H. Dierks and C. Dietz. Graphical Specification and Reasoning: Case Study Generalised Railroad Crossing. In John Fitzgerald, Cliff B. Jones, and Peter Lucas, editors, *FME'97: Industrial Applications and Strengthened Foundations of Formal Methods (Proc. 4th Intl. Symposium of Formal Methods Europe, Graz, Austria, September 1997)*, volume 1313 of *Lecture Notes in Computer Science*, pages 20–39. Springer-Verlag, September 1997. ISBN 3-540-63533-5 .

[89] G. Dipoppa and R. Bove. Modelling a Railway Application in a Geographical and Textual Integrated Fashion. In *FMERail Workshop 2*, Via Anguillarese, 301 S.Maria di Galeria, I–00060 Roma, Italy, 1998. ENEA C.R.-CASACCIA. In: [293].

FME Rail Annotations:

- **Rail subject:** .
- **Principles, techniques, tools:** .
- **Notes:** .
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository.

[90] Josef Doppebauer. Safety Considerations on Railway Signalling Systems — is there a Future for Formal Methods ? In Thierry Lecomte and Peter Gorm Larsen, editors, *FMERail Workshop # 5*, volume # 4 of *FMERail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Alcatel, Austria. **RaCoSy Repository**.

[91] E. Dürr, N. Plat, and M. de Boer. CombiCom: Tracking and Tracing Rail Traffic using VDM++. In Michael G. Hinchey and Jonathan P. Bowen, editors, *Applications of Formal Methods*, pages 203–225. Prentice-Hall International, 1995. ISBN 0-13-3-366949-1 .

[92] Tony R. Eastham. High-speed rail. Another golden age? *Scientific American*, 273(3):100–??, September 1995.

Keywords: Attraction mode electromagnetic systems; High speed rail systems; Maglev trains; Magnetic levitation vehicles; North America; Northeast Corridor routes; Railroad transportation; Repulsion mode electrodynamic systems; Urban planning .

[93] Lars-Henrik Ericsson. Formal Verification of Railway Interlockings. Technical Report 1997:4, Swedish National Rail Administration, Banverket HK, S–781 85 Borlänge, Sweden, December 1 1997. This is a duplicate listing of [96] ! **RaCoSy Repository**. Stålmarck's Method.

[94] Lars-Henrik Ericsson. Formalising Railway Interlocking Requirements. Technical Report 1997:3, Swedish National Rail Administration, Banverket HK, S–781 85 Borlänge, Sweden, December 1 1997. This is a duplicate listing of [95] ! **RaCoSy Repository**. Stålmarck's Method.

[95] L.-H. Eriksson. Formal verification of railway interlockings. Technical Report 1997:4, Swedish National Rail Administration, 1997. Previously published in Swedish as report 1997:2

Comments: This work was carried out by Prover Technology using NP-Tools (which is based on Stlmarck's method) **RaCoSy Repository**.

[96] L.-H. Eriksson. Formalising railway interlocking requirements. Technical Report 1997:3, Swedish National Rail Administration, 1997. Previously published in Swedish as report 1997:1

Comments: The formal specification in this report was done in a formal specification tool developed by Prover Technology and Ericsson, the tool being based on Stålmarck's method **RaCoSy Repository**.

[97] Lars-Henrik Eriksson. Adtranz Signal's Formal Verification Process: The STERNOL Specification Tool (SST) (See [94, 93]). In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Industrilogik, Sweden. **RaCoSy Repository**. STERNOL.

[98] Lars-Henrik Eriksson. Some Technical Aspects of an Interlocking Specification language (See [94, 93]). In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Industrilogik, Sweden. **RaCoSy Repository**.

[99] L.H. Eriksson. Specifying Railway Interlocking Requirements for Practical Use. In Erwin Schoitsch, editor, *SAFECOMP'96: 15th International Conference on Computer Safety, Reliability and Security*, page 243, Vienna, Austria, 1996. Springer. .

[100] Maria Fahlén. A Unified Language for Railway Signalling Specification (Railway Operating Company Benefits). In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Banverket, Falun, Sweden. **RaCoSy Repository**. STERNOL.

[101] Maria Fahlén. CENELEC Norm–based Safety Approvals and Formal Specification. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Banverket, Sweden. **RaCoSy Repository**.

[102] L.M.G. Feijs, H.B.M. Jonkers, and C.A. Middelburg. *Notations for Software Design.* FACIT Series. Springer–Verlag, 1994. See [103]. **RaCoSy Repository**. COLD–K.

[103] L.M.G. Feijs, H.B.M. Jonkers, and C.A. Middelburg. *The Automatic Railway case*, chapter 6 in [102]. FACIT Series. **RaCoSy Repository**. COLD–K. Springer–Verlag, 1994.

[104] W.J. Fokkink. Safety criteria for the vital processor interlocking at Hoorn–Kersenboogerd. In *Proceedings of the 5th Conference on Computers in Railways, COMPRAIL'96, Part I: Railway Systems and Management*, pages 101–110, Berlin, 1996. Computational Mechanics Publications. Extended version is available as: technical report 135, Logic Group Preprint Series of the Department of Philosophy, Utrecht University **RaCoSy Repository**.

[105] W.J. Fokkink, G.P. Kolk, and S.F.M. van Vlijmen. EURIS, a specification method for distributed interlockings. In *Proceedings of SAFECOMP '98*, LNCS. Springer-Verlag, 1998. .

[106] Daniel Fredholm. Using Formal Methods. A practical compairsion between Z/EVES and PVS. Technical Report T97-04, Swedish Institute of Computer Science, 1998 1998.

Abstract: This paper consists of a review and comparison between Z/EVES and PVS–two tools designed for analyzing formal specifications. Z/EVES is a tool for analyzing specifications written in Z. PVS is a general theorem prover for a language that consists of higher order logic together with set theory. The review has its focus on the possibility to use these tools in an industrial context. The plan for the review was to get acquainted with the tools on a general level and then to use them to partially validate a formal specification of requirements for the safety function of railway signaling systems. The conclusion is that PVS is clearly superior to Z/EVES. PVS has such a good performance that it can be recommended for industrial use in the area of formal methods. Concerning Z/EVES, its applicability seems more restricted .

[107] Daniel Fredholm. Specifying an Interlocking System: The Alister Project. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Industrilogik, Sweden. **RaCoSy Repository**.

[108] Bruno Fringuelli, Evelina Lamma, Paola Mello, and Giovanni Santocchia. Knowledge-Based Technology for Controlling Railway Stations. *IEEE Expert*, 7(6):45–52, December 1992. .

[109] W. Gall. The Management of Change: A Case Study from the Railway Industry. In R.F. Cox, editor, *Safety and Reliability Society Symposium: Managing Risk in a Changing Organisational Climate*, Swindon,UK, 1996. SARS Ltd, Clayton House, 59 Piccadilly, Manchester, M1 2AQ. .

[110] M. Geerling. Modelling and Simulation for Innovative Train Protection and Control: Light Rail Perspective. In *FME Rail Workshop 1*. Origin Nederland, 1998. In: [185] **RaCoSy Repository**.

[111] C.W. George. Specification and Development of An Automatic Train System. Internal Research Note LACOS/CRI/CWG/38, CRI A/S, 1995. RAISE/RSL.

[112] C.W. George. A Theory of Distributed Train Rescheduling. In Marie-Claude Gaudel and Jim Woodcock, editors, *FME'96: Industrial Benefit and Advances in Formal Methods*, pages 499–517. Springer-Verlag, March 1996. .

[113] A.M. Godber. A European interlocking specification — the work of the ERRI A201 Committee. In *ASPECT–95, IRSE Intl. Conf. on Advanced Railway Control*, volume 10, pages 19–26, September 1995. Referenced in [153] .

[114] B. Godziejewski. Applying Formal Methods in a Changing Railway Environment. In *FME Rail Workshop 2*, Utrecht, The Netherlands, 1998. European Rail Research Institute. In: [293] **RaCoSy Repository**.

[115] B. Godziejewski and Y. Hirao. ERRI A 201 work to harmonise functional conditions for signalling interlocking. In *FME Rail Workshop 1*. ERRI, Utrecht, The Netherlands and Railway Technical Research Inst., Tokyo, Japan, 1998. In: [185] **RaCoSy Repository**.

[116] Bogdan Godziejewski. On Formal Notation to Express Requirements Specifications — Phase 1 of the Euro–Interlocking Project. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. ERRI, The Netherlands. **RaCoSy Repository**.

[117] Frits Goebel. Railsway nets. Available from UB Göttingen, ZB: 560.01712 .

[118] C.A. Grimes. Application of Genetic Techniques to the Planning of Railway Track Maintenance Work. In A.M.S. Zalzala, editor, *First International Conference on Genetic Algorithms in Engineering Systems: Innovations and Applications, GALESIA*, volume 414, pages 467–472, Sheffield, UK, 12-14 September 1995. IEE.

Abstract: Track maintenance work was planned using GA and GP, with profit as the optimisation criteria. The results where compared with an existing determinstic technique. It was found the GP method gave the best results, with the GA method giving good results for a short section (10 miles) and poor results for a long section (50 miles). 12–14 September 1995, Halifax Hall, University of Sheffield, UK see also http://www.iee.org.uk/LSboard/Conf/program/galprog.htm .

[119] J.F. Groote. A Language for Railway Interlocking Specification. In *FME Rail Workshop 1*, Amsterdam, NL, 1998. CWI. In: [185] **RaCoSy Repository**.

[120] J.F. Groote, J.W.C. Koorn, and S.F.M. van Vlijmen. The Safety Guaranteeing System at Station Hooen-Kersenboogerd. Technical Report 121, Utrecht University, Utrecht University, Department of Philosophy, Heidelberglaan 8, Utrecht The Netherlands, October 1994. See [121].

Abstract: At the Dutch station Hoorn-Kersenboogerd, computer equipment is used for the safe and in time movement of trains. The computer equipment can be divided in two layers. A top layer offering an interface and means to help a human operator in scheduling train movement. And a bottom layer which checks whether commands issued by the top layer can safely be executed by the rail hardware and which acts appropriately on detection of a hazardous situation. The bottom layer is implemented with a programmable piece of equipment namely a Vital Processor Interlocking[4] *(VPI)*. This paper introduces the most important features of the *VPI* at Hoorn-Kersenboogerd. This particular *VPI* is modelled in *μCRL*. Furthermore, the paper touches upon correctness criteria and tool support for *VPI*s, and suggests ways for verification of properties of *VPI*s. Experiments show that it is indeed possible to efficiently verify these correctness criteria.

Comments: The analysis of this station was based on a Prover developed by Jan Frison Groote. The prover in question is based on Stålmarck's method μCRL.

[121] J.F. Groote, S.F. van Vlijmen, and J.W.C. Koorn. The safety guaranteeing system at station Hoorn-Kersenboogerd. In *COMPASS '95. Proceedings of the Tenth Annual Conference on Computer Assurance (Cat. No.95CH35802); Gaithersburg, MD, USA*, pages 57–68. IEEE, New York, N.Y., USA, 1995. See [120].

Abstract: At the Dutch station Hoorn-Kersenboogerd computerized control is used for the safe and in time movement of trains. It can be divided in three layers. A top layer assisting an operator in scheduling train movement. A bottom layer with hardware that can monitor and change the state of the railway. And an intermediate layer mainly checking whether commands issued by the top layer can safely be executed by the bottom layer. The intermediate layer is responsible for the safety of the railway. It is implemented with a programmable piece of equipment namely a Vital Processor Interlocking (VPI). This paper introduces the most important features of VPIs and models them using the process algebraic language μCRL. The form of correctness criteria of VPIs is described and these criteria are classified in the categories STATIC, JUST and NEXT. We verify the correctness criteria by transforming both the program and the criteria to propositional logic. We describe our experiences with tool support, both for the transformation and for proving formulas. Experiments show that it is also rather straightforward to verify correctness criteria on larger railway yards.

Keywords: formal logic; formal specification; formal verification; railways; safety-critical software; traffic information systems.

Comments: The analysis of this station was based on a Prover developed by Jan Frison Groote. The prover in question is based on Stålmarck's method μCRL.

[122] G. Guiho and L.-F. Mejia. Operational safety critical software methods in railways. In Anon, editor, *IFIP Transactions A (Computer Science and Technology),*, pages 262–9. IFIP World Congress, Hamburg, Germany, 1984.

[4] VPI and Vital Processor Interlocking are registered trademarks of the General Railway Signal Company.

Abstract: Railway signalling manufacturers have been designing safety-critical software for around ten years (1984-94). This software is crucial for interlocking systems and speed control systems. The techniques used by the railways and the manufacturers were dissimilar in the past because of the heterogeneousness of signalling equipment and exploitation rules among different countries. Recently some efforts have been underway at the European level to harmonize the processes and methods for cross-acceptance of safety-critical software between nations. The work of the IRSE Technical committee and the CEN/CENELEC WG A1 are presented. Formal specifications and formal proofs seem to be considered as one of the best techniques to use in that field. Some of the systems that we have produced using them are presented.

Keywords: formal specification; rail traffic; railways; safety; software reliability; traffic computer control The B Method.

[123] F. Guldan. Maximization of distances of regular polygons on a circle. *APLMA*, 25:182–195, 1980. .

[124] Shigeru Haga. Prevention of Accidents at Road-Rail Level Crossings Protected with Automatic Barriers. In *Proceedings of the Human Factors Society 32nd Annual Meeting*, volume 1 of *Safety: Transportation Safety*, pages 933–937, 1988.

Abstract: A recent study on level crossing safety is reported. The study employed three different approaches: a survey of drivers' attitude to the level crossing, quantitative estimation of accident risk from characteristics of level crossings, and improvement of crossing design from the human factors point of view. The results have been utilized by railway companies and police authorities in safety campaigns, driver education, safety investment, and improvement of warning systems for level crossings .

[125] G. Hagelin. ERICSSON Safety systems for railway control. In U. Voges, editor, *Software diversity in computerized control systems*, pages 11–21. Springer, 1988. .

[126] K. M. Hansen. Validation of a Railway Interlocking Model. *Lecture Notes in Computer Science*, 873:582–??, 1994. .

[127] Kirsten Mark Hansen. Validation of a Railway Interlocking Model. In M. Bertran M. Naftalin, T. Denvir, editor, *FME'94: Industrial Benefit of Formal Methods*, pages 582–601. Springer-Verlag, October 1994. .

[128] K.M. Hansen. Formalising Railway Interlocking Systems. In *Nordic Seminar on Dependable Computing Systems*, pages 83–94, Technical University of Denmark, August 1994. Department of Computer Science. .

[129] K.M. Hansen. Validation of a railway interlocking model. In M. Naftalin, T. Denvir, and M. Bertran, editors, *FME '94: Industrial Benefit of Formal Methods. Second International Symposium of Formal Methods Europe. Proceedings; Barcelona, Spain*, pages 582–601. Springer-Verlag, Berlin, Germany; Lecture Notes in Computer Science LNCS, 1994.

Abstract: Presents a VDM model of a real-life railway interlocking system, and describes how this model is validated through simulation in ML. The model development illustrates how concepts may be captured for a non-trivial system. The steps from a predicative VDM model to an executable ML program are also outlined. The importance of validation by simulation is highlighted by giving two equally plausible safety requirements for the system and the end user's reaction to the simulation. For safety reasons, we find it important that the model also can form the basis for formal program development, where the correctness of the program with respect to the specification can be formally verified. Therefore, we advocate to make a model which can be used for simulation as well as formal program development.

Keywords: digital simulation; formal verification; railways; safety-critical software; Vienna development method **RaCoSy Repository**. VDM, VDM–SL.

[130] K.M. Hansen. Modelling Railway Interlocking Systems. Technical Report ID-TR: 1996-167, Department of Computer Science, Technical University of Denmark, Building 344, DK-2800 Lyngby, Denmark, September 1995. **RaCoSy Repository**.

[131] K.M. Hansen. *Linking Safety Analysis to Safety Requirements*. PhD thesis, Department of Computer Science, Technical University of Denmark, Building 344, DK-2800 Lyngby, Denmark, August 1996. **RaCoSy Repository**.

[132] K.M. Hansen. Formalising Railway Interlocking Systems. In *FMERail Workshop 2*, ScanRail Consult, Signalling Assessment, Pilestræde 58/6, DK–1112 Copenhagen K, Denmark, 1998. Danish National Railway Agency. In: [293].

FME Rail Annotations:

- **Rail subject:** Railway interlocking.
- **Principles, techniques, tools:** VDM.
- **Notes:** Simulation, end-user validation.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository.

[133] S. Hanžel. Electronic Data Interchange in Railway Traffic. In J. Gričar, editor, *EDI: Business Strategy For 90's The 4th Electronic Data Interchange Conference*, pages 309–317, Bled, Slovenia,Yugoslavia, June 10-12 1991.

Abstract: The increasing internationalization of the transportation market and the rising pressure of competition characterize the transportation sector today. This demands a high degree of adaptability with the ability to react quickly to the market and to technological changes. For railways this means meeting the information requirements along the transportation logistic chain. Data interchange becomes unavoidable also in passenger traffic. This paper presents some examples of electronic data interchange in the field of railway traffic .

[134] A.J. Harrison and I.D.R. Shannon. The application of formal methods to railway signalling systems specification and the Esprit III project CASCADE. In *SAFECOMP 95. 14th International Conference on Computer Safety, Reliability and Security*, pages 101–12. Springer-Verlag, 1995.

Abstract: This paper discusses the preparation of a requirements specification for a railway signalling interlocking system using the Z notation. It then reviews the use of the specification project as a case study within the Esprit III project, CASCADE, which aims to develop a generic assessment method for safety critical software-based systems.

Keywords: formal specification; railways; research initiatives; safety-critical software; signalling; specification languages; traffic engineering computing **RaCoSy Repository**.

[135] V. Hartonas-Garmhausen, T. Kurfess, E.M. Clarke, and D. Long. Automatic verification of industrial designs. In *Workshop on Industrial-Strength Formal Specification Techniques (Cat. No.95TH8051); Boca Raton, FL, USA*. IEEE Comput. Soc. Press, Los Alamitos, CA, USA, 1995.

Abstract: This study presents new risk analysis tools and demonstrates the feasibility and applicability of these tools in the design verification of railway interlocking control systems and deadlock prevention in automated manufacturing systems. Our verification methodology consists of the following stages. First, we analyze the rules executed by the controller and extract a state machine model of the controller. Second, we compose safety, reliability, and operability system specifications using a propositional temporal logic. Finally, we use the model checker to check the state machine model of the system against its requirements. The verification approach allows an exhaustive search of all possible behaviors and scenarios. We verified two real railway interlocking control applications with 125 and 452 constraints respectively. Checking two opposing signal protection specifications involving 3 signals ranged between 74 and 1223 seconds depending on the size and the complexity of the interlocking. Traditional verification methods typically require several person weeks.

Keywords: CAD/CAM; computer integrated manufacturing; concurrency control; formal specification; formal verification; industrial control; risk management; temporal logic Model Checking.

[136] A.E. Haxthausen and J. Peleska. Formal Development and Verification of a Distributed Railway Control System. In *FME Rail Workshop 2*, DK–2800 Lyngby Denmark; P.O.Box 340440, D–28334 Bremen, Germany, 1998. Dept. of IT, Techn. Univ. of Denmark; BISS, Bremen Univ. A repeat [137]. In: [293]. 15 pages.

Abstract:

FME Rail Annotations:

- **Rail subject:** Simple, single railway line.
- **Principles, techniques, tools:** RAISE, RSL; domain model, safety requirements, software design, distributed control.
- **Notes:** Stepwise development, correctness proof arguments.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository.

[137] A.E. Haxthausen and J. Peleska. Formal Development and Verification of a Distributed Railway Control System. In *FME Rail Workshop 1*, DK–2800 Lyngby Denmark; P.O.Box 340440, D–28334 Bremen, Germany, 1998. Dept. of IT, Techn. Univ. of Denmark; BISS, Bremen Univ. See also: [136]. In: [185].

FME Rail Annotations:

- **Rail subject:** Simple, single railway line.
- **Principles, techniques, tools:** RAISE, RSL; domain model, safety requirements, software design, distributed control.
- **Notes:** Stepwise development, correctness proof arguments.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository.

[138] I. Hayashi, K. Itoh, and S. Suzuki. Man-machine interactive guidance for urban railway networks passenger information system. *Computers and Graphics*, 7(1):59–72, 1983. .

[139] U. Heinrichs and C. Moll. On the scheduling of one-dimensional transport systems. Technical report, Mathematisches Institut, Universität zu Köln, 1997.

Keywords: scheduling, shortest path, cran, galvanization, production planning, transportation.

Abstract: In this paper we consider the problem of finding a feasible routing for one-dimensional transport systems. This problem arises as a subproblem in production planning, when a mono-rail crane with several crabs is part of the production lane. Practical restrictions like finite speed of crabs and a minimal distance between crabs lead to a special routing problem. We show that this problem corresponds to the geometric problem of covering segments with angle-restricted curves with the additional constraint that all curves have at least distance 1. We prove that this question can be formulated as a shortest path problem. Finally we discuss how the presented algorithm can be used as a module for a greedy-algorithm solving a no-wait scheduling problem .

[140] A. Hidden. Investigation into the Clapham Junction railway accident. HMSO Cm 820, UK Department of Transport, 1989. .

[141] Yuji Hirao, Takahiko Ogino, Mitsuyoshi Fukuda, and Ikuo Watanabe. Interest in Formal Methods from Japanese Perspective. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Railway Technical Researhc Inst., Tokyo, Japan. **RaCoSy Repository**.

[142] G. Hoffmann, S. Balemi, and U. Brunner. Design of a Discrete Event Controller for a Model Railway. In D. Franke and F. Kraus, editors, *Proc. of 1st IFAC Symposium on Design Methods of Control Systems*, pages 451–456, Zurich, Switzerland, September 1991. Pergamon Press, Oxford, UK. .

[143] M. Hollenberg, J.F. Groote, and S.F.M. van Vlijmen. *Laris 1.0 Language for Railway Interlocking Specifications*. Utrecht. Referenced in [177] **RaCoSy Repository**.

[144] A.A. Holzbacher, M. Perin, and M. Sudholt. Modeling railway control systems using graph grammars: a case study. In D. Garlan and D. Le Metayer, editors, *Coordination Languages and Models. Second International Conference COORDINATION '97*, pages 172–86. Springer-Verlag, 1997.

Abstract: In this paper we develop in three phases a railway control system. We are mainly concerned with the software architecture of the control system and its dynamic evolution; we do not discuss here the implementation details of the components forming the control system. First, we informally discuss our design proposal for the architecture of the control system: a hierarchy of controllers whose leaves are local controllers connected in a network that mimics the underlying railway topology. Second, we formally define by means of particular graph grammars a style of software architectures for the railway control system consisting of two complementary views and ensuring several desirable properties by construction. The dynamic evolution of the architecture is modelled by a set of coordination rules which define graph transformations and are verified with respect to to the graph grammar. Third, using a coordination rule as a formal specification of a dynamic modification of the railway control system, we derive its implementation in ConCoord, a programming environment for concurrent coordinated programming. With regard to software engineering, the two first phases belong to the system design while the third one forms the first implementation step.

Keywords: formal specification; graph grammars; rail traffic; railways; software engineering; traffic control; traffic engineering computing **RaCoSy Repository**. Graph Grammars.

[145] A.A. Holzbacher, M. Perin, and M. Suedholt. Modeling railway control systems using graph grammars: A case study. *Lecture Notes in Computer Science*, 1282:172–??, 1997. .

[146] C Horellou, C Rossi, and G Sissa. An AI/Real Time Solution for Expert Scheduling of Underground Rail Traffic. *SARSS'89: Reliability on the Move*, page 47, 1989. .

[147] P. D. Horne. A hybrid test rig with real time rail vehicle modelling. In T. S. Durrani, W. A. Sandham, J. J. Soraghan, and J. Hulskamp, editors, *Applications of Transputer 3*, pages 20–25, Amsterdam, 1991. IOS Press. .

[148] G. Howarth, B.C. Ashcroft, and N.R. Jenkins. Computer graphics as a tool for a consultation (in railway projects) — Computer Applications in Railway Planning and Management. In T.K.S. Murthy, R.E. Rivier, G.F. List, and J. Mikolaj, editors, *Proceedings of the Second International Conference on Computer Aided Design, Manufacture and Operation in the Railway and Other Advanced Mass Transit Systems*, pages 63–73. Comput. Mech. Publications, 1990.

Abstract: The development of a computer-based graphics display for the Channel Tunnel Rail Link is outlined. The specification of the graphics display package is shown to be a trade-off between flexibility in terms of running the package on standard microcomputers independently of proprietary software, the constraints of present computer graphics technology and the costs of producing suitable graphics images. The use of computer-based graphics is seen to offer a flexible and innovative method of communicating the details of railway schemes to a non-technical audience, particularly in terms of illustrating the concepts and ideas underlying railway projects and the measures undertaken to reduce environmental impacts. The use of the package has resulted in more structured, informed and constructive discussions within the consultation programme.

Keywords: CAD/CAM; railways **RaCoSy Repository**.

[149] IEEE. *Proceedings of 1995 IEEE Workshop on Industrial-Strength Formal Specification Techniques.* IEEE Comput. Soc. Press, 1995.

Abstract: The following topics were dealt with: AAMP5 microprocessor verification; architectural specification of an avionic subsystem; software requirements analysis; formal methods; C++ library for specification implementation; system critical flight software verification; industrial design verification; timing analysis of real-time systems; real-time reactive systems specification; finite state machines; reactive systems software; **railway signalling**; and LOTOS specification.

Keywords: formal specification; formal verification; hardware description languages; real-time systems; specification languages **RaCoSy Repository**.

[150] J. A. Profeta III, N. P. Andrianos, Bing Yu, B. W. Johnson, T. A. DeLong, D. Guaspart, and D. Jamsck. Safety-critical systems built with COTS. *IEEE Computer*, 29(11):54–60, November 1996.

Abstract: In the rail transportation industry competitive pressure has led to the increased use of COTS (commercial off-the-shelf equipment in safety critical systems), making it imperative that we extend proven safety techniques to COTS based systems as well. To this end, we have developed the Vital Framework (V-Frame), which is used to develop a safety critical platform from COTS hardware and software. The key technologies in this framework are formal methods, information redundancy, a proprietary data format, and a concurrent checking scheme. Combining these technologies results in a real time, checkable correctness criterion that is a signature of the application's algorithm structure and is independent of both the hardware and the operating system. V-Frame's most significant attribute is that the fail safe properties of applications do not require the firmware to be correct: the application will operate in a fail safe (or vital) manner even if there are design faults in the operating system and/or the hardware fails. This does not mean that the application does not have to be correctly specified and designed. Formal methods are appropriate in the design of safety critical COTS systems because a generic processing environment is analogous to a formal system: it is designed to apply well defined transformation rules to inputs (7 Refs.) .

[151] M. Ingleby. Safety properties of a control network: local and global reasoning in machine proof. In *Proceedings of Real Time Systems.* Paris, January 1994. .

[152] M. Ingleby. A Galois theory of local reasoning in control systems with compositionality. In *Proceedings of Mathematics of Dependable Systems.* Oxford UP (UK), 1995. .

[153] M. Ingleby. A predicate logic for harmonised interlocking functions. In *FME Rail Workshop 1*, Huddersfield HD1 3DH, UK, 1998. School of Computing and Mathematics, University of Huddersfield. In: [185] **RaCoSy Repository**.

[154] M. Ingleby and D.J. Mee. A calculus of hazard for railway signalling. In *Workshop on Industrial-Strength Formal Specification Techniques (Cat. No.95TH8051); Boca Raton, FL, USA*, pages 146–58. IEEE Comput. Soc. Press, Los Alamitos, CA, USA, 1995.

Abstract: Interlockings-systems which control railway signals-are modeled as situated automata holding in memory an image of their trackside environment. Interlocking functionality is generic, but each interlocking consults a geographic database which specifies the topography of its environment. A 'calculus of hazard' comprising a theory of trackside geography and generic state of trackside environments is set up using a predicate calculus based on incidence relations. The calculus is sufficiently expressive for the articulation hazard defence rules-which are obtained from a typical IEC fault modes and effects analysis (FMEA)-free of area-specific reference. Safety of an interlocking is formulated as an NP-complete proof problem expressing the invariance of a set of hazard defence predicates of the calculus. A scaleable approach to this proof problem is developed by representing a signalling area as a set of weakly interacting localities of low combinatorial complexity. The approach uses Galois connection tools borrowed from formal concept analysis.

Keywords: computational complexity; failure analysis; formal logic; formal specification; geographic information systems; rail traffic; signalling; traffic control Logic (Non–Modal).

[155] M. Ingleby and I. Mitchell. Proving Safety of a Railway Signalling System Incorporating Geographic Data. *SAFECOMP '92: Safety of Computer Control Systems1992*, pages 129–134, 1992.

[156] M. Ingleby and I.H. Mitchell. Proving Safety of a Railway Signaling System Incorporating Geographic Data. In H.H. Frey, editor, *SAFECOM'92 Conference Proceedings of IFAC*, pages 129–134, Zürich (CH), November 1992. Pergamon Press. .

[157] Michael Ingleby. Galois Connections in Railway Formalisation. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Univ. of Huddersfield, England. **RaCoSy Repository**. Mathematics (Galois Connections).

[158] Dave Jackson. Verification of BR Interlocking. In *FME Rail Workshop 2*, Bath, England, 1998. Praxis Critical Systems. In: [293]

FME Rail Annotations:

- **Rail subject:** Railway interlocking.
- **Principles, techniques, tools:** Geographic Data Language, logic, process algebra, SMV.
- **Notes:** .
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository.

[159] J. Jarmulak, E. J. H. Kerckhoffs, and P. P. Van't Veen. Case-Based Reasoning in an Ultrasonic Rail-Inspection System. *Lecture Notes in Computer Science*, 1266:43–??, 1997. .

[160] Jacek Jarmulak, Eugene J. H. Kerckhoffs, and Peter Paul van't Veen. Case-Based Reasoning in an Ultrasonic Rail-Inspection System. In David B. Leake and Enric Plaza, editors, *Proceedings of the 2nd International Conference on Case-Based Reasoning (ICCBR-97)*, volume 1266 of *LNAI*, pages 43–52, Berlin, July25–27 1997. Springer. .

[161] M. Jelaska. Computer Elaboration of Time-Table for Single Railway Line. In Jean Cea, editor, *Proceedings of the 7th IFIP Conference on Optimization Techniques: Modeling and Optimization in the Service of Man - Part 1*, volume 41 of *LNCS*, pages 657–675, Nice, France, September 1975. Springer. .

[162] Li-Min Jia and Xi-Di Zhang. Distributed Intelligent Railway Traffic Control Based on Fuzzy Decision Making. *Fuzzy Sets and Systems*, 62(3):255–265, 1994. .

[163] R. M. J. Jose, G. vom Scheidt, and J. F. Boyce. Application of Connectionist Local Search to Line Management Rail Traffic Control. In *Proceedings of the 3rd International Conference on the Practical Application of Constraint Technology*, pages 193–212, Blackpool, April23–25 1997. The Practical Application Ltd. .

[164] F. Piriard & J. J. Kalker. Curve squeal noise by trams; Part II: Wheel/rail interaction. Technical Report DUT-TWI-95-119, Delft University of Technology, Department of Technical Mathematics and Informatics, Delft, The Netherlands, 1995. .

[165] J. J. Kalker. Computational contact mechanics of the wheel-rail system. Technical Report DUT-TWI-92-28, Delft University of Technology, Department of Technical Mathematics and Informatics, Delft, The Netherlands, 1992. .

[166] J. J. Kalker. Considerations on rail corrugation. Technical Report DUT-TWI-92-26, Delft University of Technology, Department of Technical Mathematics and Informatics, Delft, The Netherlands, 1992. (telephone +31 15 78 4568) (hardcopy only) .

[167] J. J. Kalker. A railway rail on irregular, discrete supports. Technical Report DUT-TWI-94-11, Delft University of Technology, Department of Technical Mathematics and Informatics, Delft, The Netherlands, 1994.

[168] J. J. Kalker. Wheel-rail contact; Theory, algorithms, applications. Technical Report DUT-TWI-96-69, Delft University of Technology, Department of Technical Mathematics and Informatics, Delft, The Netherlands, 1996. .

[169] J.J. Kalker. The railway track response function. Technical Report DUT-TWI-93-40, Delft University of Technology, Department of Technical Mathematics and Informatics, Delft, The Netherlands, 1993. .

[170] H. Kantz and C. Koza. The ELEKTRA Railway Signalling-System: Field Experience with an Actively Replicated System with Diversity. In *The Twenty-Fifth International Symposium on Fault-Tolerant Computing (FTCS '95)*, pages 453–458, Los Alamitos, June 1995. IEEE Computer Society Press. .

[171] T. King. Formalising British Rail's Signalling Rules. In M. Bertran M. Naftalin, T. Denvir, editor, *FME'94: Industrial Benefit of Formal Methods*, pages 45–54. Springer-Verlag, October 1994. .

[172] T. King. Formalising British Rail's Signalling Rules. *Lecture Notes in Computer Science*, 873:45–??, 1994. .

[173] F. Kitahara, H. Katano, T. Ono, Y. Kakumoto, K. Kikuchi, and M. Shinomoto. Distributed management for software maintenance in a wide-area railway system. In *Proceedings - ISADS 97 - Third International Symposium on Autonomous Decentralized Systems (Cat. No. 97TB100111)*, pages 311–18. IEEE Comput. Soc. Press, 1997.

Abstract: In a large scale real time control system, functions of subsystems differ slightly although they seem to be identical. Functions change when hardware is replaced or when the function itself is upgraded. If the standard system is generated by merging the differences and is installed then to each subsystem, subsystems become different with maintenance being carried out in each subsystem to fit its operational conditions. Furthermore, subsystems are distributed in a wide area. Software maintenance therefore becomes very difficult. The paper describes a distributed management for software maintenance in the Tokyo metropolitan area railway system. This management has two phases: generating programs for making maintenance easy and executing programs for increasing the reliability of the system. There it contributes to the effectiveness of maintenance and increases the reliability of the total system.

Keywords: networks; rail traffic; railways; real-time systems; reliability; software development management; software maintenance; traffic control **RaCoSy Repository**.

[174] Salomon Klaczko, Jörg Fiebelkorn, and Jan Philip Porschke. Formal Modelling and Graphical Representation of Intermodal Transit Points. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. Lopos, Hamburg, Germany. **RaCoSy Repository**.

[175] R. Knigge, H. Eilers, and V. Freitag. New Generation of Microcomputer-Based Operations Control Systems for High-Speed Rail and Guided Transportation as Demonstrated by TRANSRAPID. In *IFIP World Computer Congress, Hamburg*, pages 174–179. IFIP, 1994. .

[176] J. Knight, M. Elder, J. Flinn, and P. Marx. Summaries of Three Critical Infrastructure Applications. Technical Report CS-97-27, Department of Computer Science, University of Virginia, November 14 1997.

Keywords: survivability critical infrastructure applications.

Abstract: Modern society has grown to depend heavily upon a set of infrastructure services for day-to-day operations to proceed normally and efficiently. Examples of these infrastructure services include power distribution, telecommunications, transportation, and financial systems. In the event of widespread failure in any of these systems, normal activities would be severely disrupted; therefore, these systems are referred to as critical infrastructure applications. This report presents the results of a study of three particular critical infrastructure applications: the banking and finance domain, the rail transport industry, and the air traffic control system. An overview of each application area is provided, including major processes and information concerning system architecture and implementation. In addition, a detailed bibliography is provided for each application domain .

[177] G. Kolk. Formal Methods: Possibilities and difficulties in a Railway environment from a user perspective. In *FME Rail Workshop 1*. Holland Railconsult, 1998. In: [185] **RaCoSy Repository**.

[178] N. König. uro–Interlocking, a UIC Project. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France.* FME: Formal Methods Europe, Steria, France, September 22–24 1999. SBB (Swiss Federal Railways), Switzerland. **RaCoSy Repository**.

[179] Carsten Krabiell. Analyse des Problems der Linienoptimierung im öffentlichen Personennahverkehr. Master's thesis, TU Braunschweig, 1995. .

[180] Peter Kreuzer. Linienoptimierung im schienengebundenen Personenverkehr. Diplomarbeit an der Abt. für Mathematische Optimierung, TU Braunschweig, 1994. .

[181] Leo G. Kroon, H. Edwin Romeijn, and Peter J. Zwanefeld. Routing Trains through railway stations: complexity issues. *European Jounral of Operational Research, Elsevier Science B.V., The Netherlands*, 98:485–498, 1997.

[182] M. Kuby, Z. Y. Xu, and X. D. Xie. A minimax method for finding the k best "differentiated" paths. *Geographical Analysis*, 29(4):298–313, October 1997.

Abstract: In real-world applications, the k-shortest-paths between a pair of nodes on a network will often be slight variations of one another. This could be a problem for many path-based models, particularly those on a capacitated networks where different routing alternatives are needed that are less likely to encounter the same capacity constraints. This paper develops a method to solve for k differentiated paths that are relatively short and yet relatively different from one another, but not necessarily disjoint. Our method utilizes the sum of a path's distance plus some fraction of its shared distance with each other path. A minimax algorithm is used to select the path whose largest sum of length, plus shared length vis-a-vis each previously selected path, is as simple as possible. We present computational results for the **Chinese railway system**, comparing the paths generated by a standard k-shortest-path algorithm with those from our new model .

[183] Gao Lan. Human-Computer Interaction System in Railway Management Administration Network. In *Proceedings of the Fifth International Conference on Human-Computer Interaction – Poster Sessions: Abridged Proceedings*, volume 3 of *Case Studies and Applications*, page 103, 1993. .

[184] Peter Gorm Larsen. Abstract Metro Specifications in VDM++. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. IFAD, Denmark. **RaCoSy Repository**. VDM++.

[185] P.G. Larsen, editor. *FME Rail Workshop*, volume 1 of *1st FME Rail Seminar*, Forskerparken, DK–6000 Odense, Denmark, 8–9 June 1998. IFAD. ESSI Project 26538.
Workshop venue: Breukelen, The Netherlands.
Organised by Origin Nederland, a member of the Philips group of companies, P.O.Box 1444, NK–3430 BK Nieuwegein, The Netherlands.

Contents: [110, 153, 110, 279, 220, 27, 199, 19, 177, 119, 81, 137, 41, 39, 115, 213] **RaCoSy Repository**.

[186] Thierry Lecomte. Dwarf Signal Formalisation in B. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 5 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Atelier B, Steria, France. **RaCoSy Repository**. The B Method.

[187] Neil D. Lerner and Donna J. Ratte. Drivers as Decision Makers at Rail-Highway Grade Crossings. In *Proceedings of the Human Factors Society 34th Annual Meeting*, volume 2 of *Safety: Risk Perception*, pages 1042–1046, 1990. .

[188] Benjamin G. Lewis and James P. Cowan. A holistic approach to modeling outdoor acoustical environments. In *Proceedings of the Eighth Annual Symposium on Geographic Information Systems for Transportation (GIS-T)*, pages 435–440, Sparks, Nevada, 1995.

Abstract: The dominant noise sources in our current outdoor environment are typically related to highway vehicles, aircraft, construction, and rail and industrial operations. Typical environmental analyses examine each of these sources independently without combining them into one model that would predict the complete acoustical environment in a specific geographic area. Without the capability to combine all potential noise sources, a realistic prediction of a noise environment cannot be achieved. A GIS model has been developed that considers all dominant noise sources and propagation effects to yield contour mapping of a predicted environment including all of these sources simultaneously. The capability also exists to separate each component to view the contribution that each noise source has toward the complete acoustic environment. This model uses standard methodologies prescribed by the Federal Highway Administration, the Federal Aviation Administration, the Federal Transit Administration, and the Society of Automotive Engineers, combined with empirical methodologies associated with them .

[189] J. N. K. Liu and K. Y. Sin. Fuzzy Neural Networks for Machine Maintenance in Mass Transit Railway Systems. *IEEE Transactions on Neural Networks*, 8(4):932–941, July 1997. .

[190] S. Liu, M. Asuka, K. Komaya, and Y. Nakamura. An approach to specifying and verifying safety-critical systems with practical formal method SOFL. In , Fourth IEEE International Conference on Engineering of Complex Computer Systems (Cat. No.98EX193), pages 100–14. IEEE Comput. Soc, 1998.

Abstract: One of the primacy concerns in developing computer embedded safety-critical systems is how to develop quality software. Software must fulfill its functional requirements and must not contribute to the violation of safety properties of the entire system. To this end, capturing error free and satisfactory functional requirements is crucial before proceeding to the subsequent development phases. We describe an approach to specifying and verifying software for safety-critical systems with the practical formal method SOFL (Structured-Object-based-Formal Language). Requirements specification focuses on the functionality of the software, but with the consideration of safety constraints and its interaction with the surrounding operational environment. The verification of specifications can be carried out using three techniques: data flow reachability checking, specification, testing, and rigorous proofs, respectively. We apply this approach to a realistic **railway crossing controller** for a case study and analyzes its result.

Keywords: railway crossing, formal specification; formal verification; object-oriented languages; real-time systems; safety-critical software .

[191] Lorna Love and Chris Johnson. Using Diagrams to Support the Analysis of System 'Failure' and Operator 'Error'. In *Proceedings of the HCI'97 Conference on People and Computers XII*, pages 245–261, 1997.

Abstract: Computers are increasingly being embedded within safety systems. As a result, a number of accidents have been caused by complex interactions between operator 'error' and system 'failure'. Accident reports help to ensure that these 'failures' do not threaten other applications. Unfortunately, a number of usability problems limit the effectiveness of these documents. Each section is, typically, drafted by a different expert; forensic scientists follow metallurgists, human factors experts follow meteorologists. In consequence, it can be difficult for readers to form a coherent account of an accident. This paper argues that fault trees can be used to present a clear and concise overview of major failures. Unfortunately, fault trees have a number of limitations. For instance, they do not represent time. This is significant because temporal properties have a profound impact upon the course of human-computer interaction. Similarly, they do not represent the criticality or severity of a failure. We have, therefore, extended the fault tree notation to represent traces of interaction during major failures. The resulting Accident Fault Tree (AFT) diagrams can be used in conjunction with an official accident report to better visualise the course of an accident. The Clapham Junction railway disaster is used to illustrate our argument .

[192] Pawel Lubonski. Natural language interface for a Polish railway expert system. In Veronica Dahl and Patrick Saint-Dizier, editors, *Natural Language Understanding and Logic Programming*, pages 21–31. North-Holland, Amsterdam, 1985.

Keywords: logic PROLOG .

[193] David J. Maguire, Robert C. Smith, and Suzanne Jones. GIS on the Move: Some Transportation Applications of GIS. In *Proceedings of the Thirteenth Annual ESRI User Conference*, volume 3, pages 39–46, Palm Springs, CA, 1993.

Abstract: The transportation industry has traditionally been a major driving force in GIS. Transportation applications have a number of industry specific characteristics, principally the need to handle large quantities of linear-based data. This paper reviews the main characteristics of transportation applications and presents three case studies which illustrate some of the ways transportation organisations are using GIS in the UK. The case studies are concerned with highway management and maintenance at Lancashire County Council, developing a bus route database at London Regional Transport, and creating a track infrastructure database at British Rail .

[194] Gabriele Malavassi and Stefano Ricci. Petri Nets in the Railway Signalling Model. In Thierry Lecomte and Peter Gorm Larsen, editors, *FMERail Workshop # 5*, volume # 5 of *FMERail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Univ. of Rome, Italy. **RaCoSy Repository**. Petri Net.

[195] V C Marshall. Modes and Consequences of the Failure of Road and Rail Tankers Carrying Liquefied Gases and Other Hazardous Liquids. *SARSS'89: Reliability on the Move*, page 136, 1989. .

[196] J. Meertens. Verifying the safety guaranteeing system at railway station Heerhugowaard. Master's thesis, Utrecht University, Department of Philosophy, Faculteit Wijsbegeerte, August 1996. Referenced in [279].

Comments: The analysis of this station was based on a Prover developed by Jan Frison Groote. The prover in question is based on Stlmarck's method. .

[197] Karl Meinke. Introduction to FAST. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Prover Technology, Sweden. **RaCoSy Repository**. FAST.

[198] L.-F. Mejia. Formalizing existing safety-critical software. In *FME Rail Workshop 2*, 33, rue des Bateliers, F–93400 Saint–Ouen, France, 1998. Alstom Transport. In: [293] **RaCoSy Repository**.

[199] L.-F. Mejia. Formalizing existing safety-critical software. In *FME Rail Workshop 1*, 33, rue des Bateliers, F–93400 Saint–Ouen, France, 1998. Alstom Transport. Paper was not presented due to transport strike in France! See [198]. In: [185] **RaCoSy Repository**.

[200] F.H. Mertens. A traffic system compatible with trams on the Bahnhofsplatz in Zurich. *Strassenverkehrstechnik*, 17(2):37–42, 1973.

Abstract: The traffic in front of the main railway station has been re-organized. Almost all pedestrian movement is channelled underground. A computer-controlled signal system for motor traffic and for up to 180 trams per hour yields the highest safety and travel comfort. Every second a freely programmable computer evaluates information supplied by sensors and produces a signal program in real time. If the computer fails a control equipment takes command automatically using a multi-structured emergency program and takes demands for special conditions into consideration at least once an operating cycle. The control equipment and control strategy are outlined and the software described. Experience gained in practice is discussed.

Keywords: control engineering applications of computers; control equipment; real-time systems; road vehicles; signalling; traffic control systems **RaCoSy Repository**.

[201] ?? Meynadier. Future of Formal Methods. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. ??? (Was document distributed ?) Matra Transport, France.

[202] P. Middelraad. *Euris: European Railway Interlocking Specifications.* UIC 7A/16, Utrecht, 1992. Referenced in [177] .

[203] S. Mitra and I.D.R. Shannon. Assessment and Certification Requirements in the European Railway Industry. In Erwin Schoitsch, editor, *SAFECOMP'96: 15th International Conference on Computer Safety, Reliability and Security*, page 276, Vienna, Austria, 1996. Springer. .

[204] M.J. Morley. Safety in Railway Signaling Data: A Behavioural Analysis. In J.J. Joyce and C.-J.H. Seger, editors, *International Workshop on Higher Order Logic Theorem Proving and its Applications*, volume 780 of *Lecture Notes in Computer Science*, pages

465–476, Vancouver, Canada, August 1993. University of British Columbia, Springer-Verlag, published 1994. .

[205] Karin S. Mogensen and Jakob Braad. Control Process for Dwarf Signal (Based on: [214]). In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. textslOne of a series of exercise reports re-modelling given example solutions [44, 43, 206, 208, 207, 45]Dept. of IT, Techn.Univ. of Denmark. **RaCoSy Repository**.

[206] Karin S. Mogensen and Jakob Braad. Interlocking: Harmonised Interlocking Functions and Railway Signalling (Based on: [154, 153]). In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. textslOne of a series of exercise reports re-modelling given example solutions [44, 43, 208, 207, 205, 45]Dept. of IT, Techn.Univ. of Denmark. **RaCoSy Repository**. RAISE/RSL.

[207] Karin S. Mogensen and Jakob Braad. Modelling Railway Interlocking Systems (Based on: [132]). In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. textslOne of a series of exercise reports re-modelling given example solutions [44, 43, 206, 208, 205, 45]Dept. of IT, Techn.Univ. of Denmark. **RaCoSy Repository**. RAISE/RSL.

[208] Karin S. Mogensen and Jakob Braad. SIST: A System for Checking Safety in Interlocking (Based on: [254]). In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden*. FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. textslOne of a series of exercise reports re-modelling given example solutions [44, 43, 206, 207, 205, 45]Dept. of IT, Techn.Univ. of Denmark. **RaCoSy Repository**. RAISE/RSL.

[209] M. Montigel. Elemente eines computergestützten Werkzeugs zur Entwicklung von Eisenbahnsicherungsanlagen mit Petri-Netzen. Technical Report Schriftenreihe des IVT Nr. 92, IVT: Institut für Verkerhrsplanung, Transporttechnik, Strassen- und Eisenbahnbau, ETH, Zürich, Dezember 1992. In German **RaCoSy Repository**.

[210] M. Montigel. Formal Representation of Track Topologies by Double Vertex Graphs. In *Proceedings of Railcomp 92 held in Washington DC, Computers in Railways 3*, volume 2: Technology. Computational Mechanics Publications, 1992. **RaCoSy Repository**.

[211] M. Montigel. Modelling and enforcement of dependencies in railway safety systems. Technical Report 1995DI-th10776, Swiss Federal Institute of Technology, Zurich, August 21 1995.

Abstract: A logical data model of railway safety systems is developed, based on distributed discrete event systems. The dependencies between states and events are formulated on a local basis exclusively. Therefore, for developing a model of a component, it is sufficient to consider the component and its direct environment only. This approach allows the separation of the description of dependencies during the system design process and their reinforcement during the runtime of the system. Consequently, the whole modelling process is simplified. This applies to the initial development, as well as to modifications and extensions of the model. Further, a new algorithm is presented. This so-called Eunomic Algorithm guarantees that the occurrence of controllable events will be permissible always during the runtime of the system. Thus, the previously formulated dependencies are continuously enforced. The data of a railway safety system are divided into different layers of abstraction, so-called domains. Each domain is described with an appropriate modelling language, Petri nets for the dynamic domains, and double point graphs as well as logic invariants for the static domains. For abstract type data and for actual instance data, respectively, specific variants of these domains are developed. The goal of the global system structure is a rigorous separation between the main safety layer and the controlling layer. As a result, the system components with relevance on safety can be simplified and reduced considerably. An example is discussed, which covers the basic functions and properties of a railway safety system. The application of the proposed modelling languages shows that railway safety systems may be described by such a model in a precise, compact manner. Furthermore, their properties can be verified by mathematical means, and simplifications of the system can also be identified from the model .

[212] Markus Montigel. *Modellierung und Gewährleistung von Abhängigkeiten in Eisenbahnsicherungsanlagen.* PhD thesis, ETH: Swiss Federal Institute of Technology, ETH Honggerberg, CH-8093 Zürich, Swtizerland, June 1994. **RaCoSy Repository**. Petri Net.

[213] Markus Montigel. A Formal Model of Dependencies in Railway Interlockings (Abstract). In *FME Rail Workshop 1*, Now: Fachhochschulstudiengang St. Pölten, Herzogenburgerstr. 68, A-3100 St. Pölten, Austria; Phone: +43 2742 313 228, Fax: +43 2742 313 229, 1998. Then: Alcatel Austria, AG, Systems Engineering, Scheydgasse 41, A-1211 Vienna, Austria. In: [185] **RaCoSy Repository**.

[214] Markus Montigel. Formal Methods in Computer-based Safety Systems: Design of a Control Process for an Alcatel-like Dwarf Signal. In Markus Montigel, editor, *FME Rail Workshop # 3*, volume # 3 of *FME Rail Workshop; St. Pölten.* FME: Formal Methods Europe, Fachhochschulstudiengang St. Pölten, Herzogenburgerstr. 68, A-3100 St. Pölten, Austria; Phone: +43 2742 313 228, Fax: +43 2742 313 229, February 17–19 1999. **RaCoSy Repository**.

[215] Markus Montigel. Specification of the Control Process for a Dwarf Signal (See also [214]). In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 5 of *FME Rail Workshop; Tolouse, France.* FME: Formal Methods Europe, February 17–19 1999. Fachhochschulstudiengang St. Pölten, Herzogenburgerstr. 68, A-3100 St. Pölten, Austria; Phone: +43 2742 313 228, Fax: +43 2742 313 229. **RaCoSy Repository**.

[216] M.J. Morley. Modelling British Rail's Interlocking Logic: Geographic Data Correctness. Technical Report ECS-LFCS-91-186, University of Edinburgh, 1991. .

[217] M.J. Morley. Safety in Railway Signalling Data: A Behavioural Analysis. In J. Joyce and C. Seger, editors, *Proc. 6th annual workshop on higher order logic and its applications,*

Vancouver, 4-6 August, pages 465–474. Springer–Varlag Lecture Notes in Computer Science, Vol.780, 1993–4. .

[218] M.J. Morley. *Safety Assurance in Interlocking Design.* PhD thesis, University of Edinburgh, 1996. .

[219] M.J. Morley. Safety-level Communication in Railway Interlockings. *Science of Computer Programming*, 29(1-2):147–170, July 1997. .

[220] M.J. Morley. Semantics of geographic data languages. In *FMERail Workshop 1*, Leeds LS2 9JT UK, 1998. School of Computer Studies, Univ. of Leeds. In: [185] **RaCoSy Repository**.

[221] Rudolf G. Mortimer. Visual Factors in Rail-Highway Grade Crossing Accidents. In *Proceedings of the Human Factors Society 35th Annual Meeting*, volume 1 of *Forensics Professional: Real-World Problems and Practices in Forensics*, pages 600–602, 1991. .

[222] Rudolf G. Mortimer. Oh! Say, Can You Hear that Train Coming to the Crossing? In *Proceedings of the Human Factors and Ergonomics Society 38th Annual Meeting*, volume 2 of *SAFETY: Safety Potpourri II [Lecture]*, pages 898–902, 1994.

Abstract: WARNING: THE ABSTRACT OF THIS ENTRY HAS NOT BEEN VALIDATED. How effective is the horn on trains in alerting motorists, cyclists and pedestrians of the approach of a train to a highway-railroad crossing? Road users become aware of trains approaching crossings either by seeing them, hearing the warning horn or by warning devices at the crossing. Auditory warnings have some advantages over others, but practical problems of sound transmission and the noise environment of road users limit their effectiveness. Factors that affect the audibility of train horns and crossing bells are discussed. Train and crossing bells are generally effective for persons in their immediate environment, but are relatively ineffective for occupants of closed vehicles. Because of the lack of reliability of the detectability of auditory warning signals provided to motorists and others approaching rail-highway crossings, they should visually scan the tracks to ascertain the presence of a train .

[223] Paul Mukherjee. A VDM++ Specification of a Metro Door Management System. In Dines Bjørner and Maria Fahlén, editors, *FMERail Workshop # 4*, volume # 4 of *FMERail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. IFAD, Denmark. **RaCoSy Repository**. VDM++.

[224] Kathleen Murphy, Elizabeth Ralston, David Friedlander, Rodney Swab, and Paul Steege. The Scheduling of Rail at Union Pacific Railroad. In *Proceedings of the 14th National Conference on Artificial Intelligence and 9th Innovative Applications of Artificial Intelligence Conference (AAAI-97/IAAI-97)*, pages 903–912, Menlo Park, July27–31 1997. AAAI Press. .

[225] T. K. S. Murthy, L. S. Lawrence, and R. E. Rivier, editors. *Computers in Railway Management*, Computational Mechanics Publications. Springer Verlag, 1987. .

[226] T.K.S. Murthy et al., editors. *Computers in railways IV: Fourth International Conference on Computer Aided Design, Manufacture, and Operation in the Railway and*

Other Mass Transit Systems, COMPRAIL '94, Madrid, Spain, 7–9 September 1994, volume 4, Southampton; Boston, 1994. Computational Mechanics Publications. .

[227] Karl Nachtigall. Exact solution methods for periodic programs. Technical Report 14, Universität Hildesheim, 1993. .

[228] Karl Nachtigall. Time periodic network optimization. Technical Report 8, Universität Hildesheim, 1993. .

[229] Karl Nachtigall and Stefan Voget. A genetic algorithm approach to periodic programs. Technical Report 14, Universität Hildesheim, 1993. .

[230] H. Nakamura and K. Takeshi. Fault-Tolerant Microcomputer Design and Application for Railway Train Control. In Jan van Leeuwen, editor, *Proceedings of the IFIP 12th World Computer Congress. Volume 1: Algorithms, Software, Architecture*, pages 652–658, Amsterdam, The Netherlands, September 1992. Elsevier Science Publishers. .

[231] M. Nelli, A. Bondavalli, and L. Simoncini. Dependability Modeling and Analysis of Complex Control Systems: An Application to Railway Interlocking. *Lecture Notes in Computer Science*, 1150:93–??, 1996. .

[232] J. Nievergelt. Thoughts on Traffic Scheduling and Time Table Design. Technical Report dyl/9/2, ETH, Zürich, Switzerland, Informatik, ETH, CH-8092 Zurich, Switzerland, January 1994. .

[233] A. Norcliffe and S. Valentine. Z Readers Video Course. PAVIC Publications, 1992.

Abstract: Video-based Training Course on the Z Specification Language. The course consists of 5 videos, each of approximately one hour duration, together with supporting texts and case studies. The course is aimed software engineers in industry who wish to take a look at formal methods. It is specifically designed to give skills in *reading* Z specifications. The material is also suitable for use in academic institutions where students are to be introduced to Z.

There are 5 video tapes, each about 1 hour long. The tapes contain material on supporting mathematics followed by a tutorial specification showing the mathematics in action. Each part of the course is accompanied by a booklet containing the specifications discussed on the tapes with annotations. The contents is as follows:

1 An introduction to sets. Specifying a (very) simple Security System.

2 Functions. Specifying a simple Banking System.

3 Sequences. Modelling queues at a petrol filling station.

4 Relations. Specifying an e-mail system.

5 A review of the Z mathematical tool kit. Three further written specifications to practice reading skills: Modelling Family Relationships; Specifying a Lift (elevator) System; Railway Signalling.

Formats: VHS(PAL) for UK, Europe, Australia, etc.; VHS(NTSC) for American continent; SECAM for France & Russia. Other formats could be made available on request. Further details, including free preview material, are also available. For information, please contact: Anthony Meehan, School of Engineering Information Technology, Sheffield Hallam University, Pond Street, Sheffield S1 1WB, UK .

[234] L.H. Oei. Pruning the Search Tree of Interlocking Design and Application Language Operational Semantics. Technical Report P9418, University of Amsterdam, Programming Research Group, Kruislaan 403, 1098 SJ Amsterdam, The Netherlands, November 1994.

Abstract: An interlocking is a system used at railyards for guaranteeing safety of train movements. This paper succeeds the study on the syntax and static semantics of tightly related graphical specification languages for interlockings. These languages together are known in NS documents as the Euris method. The Euris method has been designed by P. Middelraad of the Dutch railway company, NS, de Nederlandse Spoorwegen[5]. It concentrates on a graphical definition of Railway Interlocking by means of the so called Logic Sequence Charts, short LSCs, which is a derivation of the well known Flow Charts. NS have already developed a symbolic intermediate tool interface language, IDEAL to automate processing of LSC specifications. IDEAL, Interlocking Design and Application Language, is therefore effectively used as an Interlingua within the Euris-Simulation project. A feasibility study of strategies of translations of IDEAL to the ExSpect simulation specification language is made. ExSpect, Executable Specification Tool—a formalism based upon Petri Nets—, would mean a first step toward proof theoretical correctness of the Euris method. As in the previous study, we have made use of the Algebraic Specification Formalism and the Syntax Definition Formalism which has been integrated in the ASF+SDF Meta-environment, for this purpose. The major question addressed is whether it is possible to apply full automated transformation of manageable complexity of IDEAL to ExSpect, without losing the LSC operatonal semantics, and at the same time gain the Petri Net invariants Petri Net.

[235] Takahiko Ogino and Yuji Hirao. Formal methods and their applications to safety-critical systems of railways. *Quarterly Report of RTRI. Ken-yusha for Railway Technical Research Institute of Japan, Tokyo*, 36(4), 1995.

Abstract: This paper describes a formal approach to requirements specifications for railway safety critical software systems and their formal safety definitions. Considering the programs and the data in a software system as the axioms and the inference rules in a formal system, we can claim that the system is safe if and only if, within the formal system, we can prove theorems that are equivalent to the safety requirements. This approach has many advantages. First, a specification is rigorous so that any ambiguity may be excluded. Secondly, specifications can be compared easily so that differences between systems will be clearer than in a natural language. This would be very useful for confirming interoperability for two systems. Thirdly, there may be systems or methods to mechanically convert a formal specification into an executable program. These are the reasons we started this investigative study. Part of an on-going study, this paper looks into the research carried out in various places abroad and seeks to clarify the underlying principle, and in particular its safety requirements. Some indications of our possible future studies are included.

Keywords: formal specification; rail traffic; railways; safety-critical software; traffic control; traffic engineering computing **RaCoSy Repository**.

[5] The project we are involved in we sometimes refer to as ISL: Interlocking Specification Language.

[236] Christine Oltrogge. *Linienplanung für mehrstufige Bedienungssyteme im öffentlichen Personenverkehr*. PhD thesis, TU Braunschweig, 1994. .

[237] J. Padget, P. Broadbery, and D. Hutchinson. Mixing Concurrency Abstractions and Classes. In *Workshop on Research Directions in High Level Parallel Programming Languages*, Lecture Notes in Computer Science., Berlin, DE, 1991. Springer-Verlag.

Abstract: We report experience with the construction of a system supporting several concurrent programming abstractions (futures, Linda, CSP, time-wap and paralations) and of an experiment (in an earlier system) in which time-warp was modelled in Linda. As a result of this work we can now cast these competing abstractions in a common framework by the use of classes. This leads to the concept of the generic scheduler. As an application of these techniques, we discuss a railway simulation which uses Linda and time-warp .

[238] G. Parkin. Complex systems proved. *RAIL BULLETIN*, pages 49–51, June/July 1995. .

[239] A. Patz. Die richtige Auswahl von Verkehrslinien bei großen Straßenbahnnetzen. *Verkehrstechnik*, 50/51, 1925. .

[240] Jan Storbank Pedersen. Specifying Aspects of a Dwarf Signal System Using RAISE. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 5 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. Terma Electronics, Denmark. **RaCoSy Repository**. RAISE/RSL.

[241] J. Peleska. Test Automation for Safety-Critical Systems: Industrial Application and Future Developments. In Marie-Claude Gaudel and Jim Woodcock, editors, *FME'96: Industrial Benefit and Advances in Formal Methods*, pages 39–59. Springer-Verlag, March 1996. .

[242] J. Peleska and M. Siegel. From testing theory to test driver implementation. In M.-C. Gaudel and J. Woodcock, editors, *FME '96: Industrial Benefit and Advances in Formal Methods. Third International Symposium of Formal Methods Europe. Proceedings; Oxford, UK*, pages 538–56. Springer-Verlag; Berlin, Germany, 1996.

Abstract: We describe the theoretical foundations for the VVT-RT test system (Verification, Validation and Test for Reactive Real Time Systems) which supports automated test generation, test execution and test evaluation for reactive systems. VVT-RT constructs and evaluates tests based on formal CSP specifications (C.A.R. Hoare, 1985), making use of their representation as labelled transition systems generated by the CSP model checker FDR. The article provides a sound formal basis for the development and verification of high quality test tools; since, due to the high degree of automation offered by VVT-RT, human interaction becomes superfluous during critical phases of the test process, the trustworthiness of the test tool is an issue of great importance. The VVT-RT system will therefore be formally verified so that it can be certified for testing safety critical systems. The article represents the starting point of this verification suite, where the basic strategies for test generation and test evaluation used by the system are formally described and verified. VVT-RT has been designed to support automation of both untimed and real time tests. The article describes the underlying theory for the untimed case. Exploiting these results, the concepts and high level algorithms used for the automation of real time tests are described in a second report which is currently prepared (J. Pelaska, 1995). At present, VVT-RT is applied for hardware in the loop tests of railway and tramway control computers.

Keywords: formal specification; program testing; program verification; real-time systems; safety-critical software CSP.

[243] Jakob Lyng Petersen. Automatic Verification of Railway Interlocking Systems: A Case Study. In Mark Ardis, editor, *Proceedings of the 2nd Workshop on Formal Methods in Software Practice (FMSP-98)*, pages 1–6, New York, March4–5 1998. ACM Press. .

[244] Jakob Lyng Petersen. *Mathematical Methods for validating Railway Interlocking Systems.* PhD thesis, Dept. of IT, Techn. Univ. of Denmark, Bldg. 344, DK–2800 Lyngby, February, November 1998.

Comments: Uses Prover Technology **RaCoSy Repository**.

[245] J.L. Petersen. Formal Requirement Verification of a Swedish Railway Interlocking System. Technical Report IT-TR: 1997-005, Technical University of Denmark, Department of Information Technology, April 1997.

Comments: This work was carried out by Petersen when he was at an internship at Prover Technology, and the verifiation was based on NP-Tools (based on Stålmarck's method) **RaCoSy Repository**.

[246] J. Piotrowski and J. J. Kalker. A non-linear mathematical model for finite, periodic rail corrugations. Technical Report DUT-TWI-93-49, Delft University of Technology, Department of Technical Mathematics and Informatics, Delft, The Netherlands, 1993. .

[247] S. Prehn. Distributed Train Time-tables and Dispatching. Technical Report SP/13/2, UNU/IIST, the UN University's International Institute for Software Technology, P.O.Box 3058, Macau; E-Mail: `library@iist.unu.edu`, July 1994. RAISE/RSL.

[248] C. Proctor and S. Young. Dialogue Control in Conversational Speech Interfaces. In M. M. Taylor, F. Neel, and D. G. Bouwhuis, editors, *The Structure of Multimodal Dialogue*, number 29 in Part 5: Applications and Architectures, pages 385–398. North-Holland, Elsevier Science Publishers, Amsterdam, 1989.

Abstract: The VODIS project is focused on the area of speech-based interfaces to information systems accessible via the public telephone network. The key features of this environment are a highly restricted topic domain, goal oriented dialogue, continuous speech from a small (150 word) vocabulary, naive untrained users and highly variable recognition rates. Our dialogue design strategy has been motivated by two major requirements: (i) to provide a habitable user interface and (ii) to give direct support of the speech recognition process. Our implementation strategy has been to use the frame approach using our special purpose programming language UFL. For (i) we have been guided by two influences. Firstly, we have analyzed real data obtained from transcripts of an existing (human) information service: the British Rail Timetable Enquiry Service. Secondly, we have adopted a formal measure of "goodness" based on minimisation of transaction time. For (ii), we have developed an adaptive strategy whereby the user responses are syntactically constrained. When recognition is good, user inputs are relatively unconstrained. When performance is poor, questions to the user are made much more specific ultimately to the point where only single word answers are invited and accepted. The purpose of this chapter is to review our overall system design strategy from the point of view of dialogue control and reflect upon the lessons learnt .

[249] Javier Gutierrez Puebla and Rafael E. Gonzalez Aguayo. Transport in Europe: A study of train accessibility using GIS. In *Fifteenth Annual ESRI User Conference Proceedings*, Palm Springs, California, 1995.

Abstract: This paper reports the design, implementation and results of a trans-European scale transportation accessibility model. This study reports only the results of the railways portion of the model, which includes multiple categories of lines within the transportation hierarchy. The rail network was digitized over the road network and the design considers not only the railways but also the possibility of taking another means of transport in order to access the train. Implementation of the model used indicators of 'absolute accessibility' similar to those reported in Gutierrez et al. (EGIS '93), except for important differences resulting from enhanced network analysis capabilities in the most recent version of the GIS software. Analysis includes construction of isoaccesibility contours zones showing net increase in accessibility and differences maps .

[250] Emile Quinet. Issues in Building the European High-Speed Train Network. *Journal of Infrstructure Systems*, pages 49–54, March 1997. **RaCoSy Repository**.

[251] S. M. Reddy, I. Pomeranz, and R. Jain. On Codeword Testing of Two-Rail and Parity TSC Checkers. In *Proceedings of the 24th Annual International Symposium on Fault-Tolerant Computing*, pages 116–127, Los Alamitos, CA, USA, June 1994. IEEE Computer Society Press. .

[252] S. Dillon Ripley. On the long, long trail of the rail. *Smithsonian*, 19(5):38–??, August 1988.

Abstract: Fourteen years of tracking culminate in a unique film record of the lives of these bashful birds .

[253] E. Roanes-Lozano, L. M. Laita, and E. Roanes-Macias. An Application of an AI Methodology to Railway Interlocking Systems Using Computer Algebra. *Lecture Notes in Computer Science*, 1416:687–??, 1998. .

[254] Eugenio Roanes-Lozano, Luis M. Laita, and Eugenio Roanes-Macias. An Algebraic Model for Decision-taking in Railway Interlocking. In Markus Montigel, editor, *FME Rail Workshop # 3*, volume # 3 of *FME Rail Workshop; St. Pölten*. FME: Formal Methods Europe, Fachhochschulstudiengang St. Pölten, Herzogenburgerstr. 68, A-3100 St. Pölten, Austria; Phone: +43 2742 313 228, Fax: +43 2742 313 229, February 17–19 1999. **RaCoSy Repository**. Mathematics(Category Theory).

[255] B. Ropke, W. Seibel, and A. Wozniak. Verification and function test of electronic interlockings in the system test centre (rail traffic control). *Signal und Draht*, 87(4):120–2, 1995.

Abstract: In the system test centre described, railway electronic interlockings are comprehensively tested and verified. Until now, this could only be done on site, at the original system for the customer. Configuration of the test centre allows simulation of every route system in service which is available as real-time simulation. In the system test centre, the system checks for new installations as well as for reconstructions, internal acceptances and fault processing are carried out. System checks consist of a function integrity test, detection of time response and interface and stress tests. By this procedure, faults in the software can be detected and corrected before delivery of the interlocking. The quality of the product is increased and additional costs arising for the concerned railway authority at a later stage due to limited availability are prevented. When interlockings are reconstructed, the new data can be prechecked so that the change on site can be realized much faster than until now. Consequently, operational inconveniences can be reduced to a minimum.

Keywords: engineering; digital simulation; program testing; program verification; rail traffic; railways; real-time systems; software reliability; traffic control; traffic engineering computing **RaCoSy Repository**.

[256] N. Rowden. A Safe, Reliable Control and Supervisory System for Railway Networks. In Erwin Schoitsch, editor, *SAFECOMP'96: 15th International Conference on Computer Safety, Reliability and Security*, page 266, Vienna, Austria, 1996. Springer. .

[257] Denis Sabatier. The B Method in Railways. In Markus Montigel, editor, *FMERail Workshop # 3*, volume # 3 of *FMERail Workshop; St. Pölten*. FME: Formal Methods Europe, Fachhochschulstudiengang St. Pölten, Herzogenburgerstr. 68, A-3100 St. Pölten, Austria; Phone: +43 2742 313 228, Fax: +43 2742 313 229, February 17–19 1999. Steria, France. **RaCoSy Repository**. The B Method.

[258] M. Säflund. Modelling and Formally Verifying Systems and Software in Industrial Applications. In Xu Furong, editor, *Proceedings of the second International Conference on Reliability, Maintainability and Safety (ICRMS '94), Beijing*, pages 169–174. International Academic Publishers, June 1994. ISBN 7-80003-303-1/TB.25 .

[259] M. J. Savage. Junction optimisation technique. *The Computer Journal*, 12(3):268–272, August 1969.

Keywords: optimisation; rail traffic; traffic control .

[260] Andreas Sethy. Connection between reliability and signalling-safety in railway technology. In *Reliability and Maintainability Symposium*, pages 75–79, Las Vegas, Nevada USA, 1992. .

[261] T. Shimazoe, N. Omokawa, and O. Yoshida. Development of a scheme design and verification tool based on software design diversity for solid state interlocking systems. In *Transactions of the Institute of Electrical Engineers of Japan, Part C; vol.115-C, no.5*, pages 665–71. Kyosan Electric Manuf. Co., Japan, May 1995. In Japanese.

Abstract: In this paper development of a scheme for the newest solid-state interlocking system named PRIME, is introduced, Interlocking systems need different specifications on each station. The interlocking tables form most of that specification. By utilizing this tool, the railway signal engineer is able to manage a large number of data easily and efficiently, and compiles interlocking data from the interlocking tables for PRIME. Interlocking function which is required for fail-safe control, is dependent on interlocking data. Therefore fault avoidance of interlocking data is indispensable. It is for this reason that we utilized software design diversity for construction of this tool. We have four phases of the design diversity in the software life cycle: Phase-1 - diversity data input of interlocking table and geographical data; Phase-2 - decompile of interlocking database; Phase-3 - interlocking data compile and interlocking functional test; and Phase-4 - diversity compile for track remodeling support data.

Keywords: control .

[262] R.C. Short. Software validation for a railway signalling system. In *SAFECOMP'83*, pages 183–193. Pergamon Press, 1983. .

[263] R.C. Short. Railway Safety Cases: Control of Risk in a Changing Industry. In R.F. Cox, editor, *Safety and Reliability Society Symposium: Managing Risk in a Changing Organisational Climate*, Swindon,UK, 1996. SARS Ltd, Clayton House, 59 Piccadilly, Manchester, M1 2AQ. .

[264] Thomas H. Short. An Algorithm for the Detection and Measurement of Rail Surface Defects. *Journal of the American Statistical Association*, 88(422):436–??, June 1993. .

[265] A. Simpson. A Formal Specification of an Automatic Train Protection System. In M. Bertran M. Naftalin, T. Denvir, editor, *FME'94: Industrial Benefit of Formal Methods*, pages 602–617. Springer-Verlag, October 1994. .

[266] A.C. Simpson. Model Checking for Interlocking Safety. In *FME Rail Workshop 2*, Parks Road, Oxford OX1 3QG, UK, 1998. Oxford Univ., Computing Lab. In: [293].

Abstract:

FME Rail Annotations:

- **Rail subject:** Railway signalling, interlocking.
- **Principles, techniques, tools:** CSP, model checking, refinement.
- **Notes:** Safety.
- **Repository:** Optional — indicates whether a copy is kept at Lyngby.

RaCoSy Repository.

[267] A.C. Simpson, J.C.P. Woodcock, and J.W. Davies. The mechanical verification of Solid State Interlocking geographic data. In L. Groves and S. Reeves, editors, *Proceedings of Formal Methods Pacific*, pages 223–242, Wellington, New Zealand, 9–11 July 1997. Springer–Verlag. .

[268] Stuart Sirota and Victor Henry. Using GIS to identify locations with the greatest potential increased light rail ridership. In *Proceedings of the Eighth Annual Symposium on Geographic Information Systems for Transportation (GIS-T)*, pages 371–382, Sparks, Nevada, 1995.

Abstract: This paper represents how GIS was used in support of a marketing initiative to increase ridership on the Central Light Rail Line in Baltimore, Maryland. A primary objective of the initiative was to develop a marketing strategy which identified geographic locations in the region in which to target marketing efforts. GIS was identified as an ideal tool to perform spatial analysis to yield the desired results. The analysis was performed by importing several existing data sources into the GIS. These data sources included passenger survey data, census data, and local demographic forecasts. Using GIS, it was possible to ultimately isolate individual transportation analysis zones which contained the greatest potential for new ridership. GIS also created dramatic color thematic maps used to present the findings of the study to senior management .

[269] R. Smokvina. EDIFACT Standard in Communication Between Seaport and its Business Surroundings. In J. Gričar, editor, *EDI: Business Strategy For 90's The 4th Electronic Data Interchange Conference*, pages 318–322, Bled, Slovenia,Yugoslavia, June 10-12 1991.

Abstract: In the paper are presented the feasibility study and work on the project for the introduction of the EDI system at the Port of Koper based on the EDIFACT standard and also plans to introduce the EDI transactions through three phases. The Port of Koper has started the project to connect its business partners through the EDI system. The aim of project in the first phase is to communicate messages about work orders (dispozicija) which is the main source of information for the short term planning. The data are collected mainly from shipping agents, forwarding firms, railway companies and trucking companies. Since the Port of Koper is a customs free zone the goods are under strict Customs surveillance so the data must also be available for customs inspection and control. The present state of the international EDIFACT standard is offering some messages to be used for the purpose of planning at the Port of Koper. The most suitable is the IFTMFR(International Forwarding and Transport Message Framework) a message framework consisting of six different messages. The preliminary study has shown that some segments have to be added to the IFTM messages to suit the needs of Port of Koper and ita partners. The CUSDEC (Customs Declaration Message) and CUSRES (Customs Response Message) messages are also important to this project but the customs documents currently in use in Yugoslavia are not prepared according to those standards
The first part of project, which has to be operational by the end of the first quarter of the year 1992, will cover the introduction of the standard message for the data interchange between the Port of Koper and its business partners with all necessary coding and organizational instructions. The system will also cover the feed- back information about work which has been accepted and planned at the Port of Koper. In the next phase of the project, to be commenced after the first phase has started, the EDI system will also cover the information about ships coming and going to the port, work completed and direct data interchange with the railways .

[270] B. Stamm, R. Baumann, and M. Kündig-Herzog. A Safety Critical Computer System in a Railway Application. In Janusz Gorski, editor, *SAFECOMP'93: 12th International Conference on Computer Safety, Reliability and Security*, pages 182–194, Poznan-Kiekrz, Poland, 1993. Springer-Verlag. .

[271] Bengt J. Sterner. A Geographical Model for Computerised Interlocking and Dispatching. In *Symposium on "Railway Cybernetics"* [1], pages 125–135. **RaCoSy Repository**. STERNOL.

[272] R. G. Stone. Points recurring. The history of a railway problem. *ACM SIGPLAN Notices*, 17(9):88–94, September 1982.

Keywords: class exercise; computer science education; derived problems; programming theory; recursion; shunting railway trucks; students; triple siding .

[273] L. Szten and R. Ninard. Microcomputer Dispatcher System MSD-Busz. *Techniki Komputerowe Biuletyn Informacyjny*, 30(1):27–40, 1995. In Polish.

Abstract: Microcomputer Dispatcher System (MSD-Busz) provides a tool for graphical visualization of the state of both railway and municipal transport services-traction networks as well as for remote control of network elements. The paper presents specification of the system including its block diagram, operation and software structure.

Keywords: data visualisation; microcomputer applications; railways; traffic engineering computing; transportation .

[274] Lajos Takács. On a probability problem connected with railway traffic. *Journal of Applied Mathematics and Stochastic Analysis*, 4(1):1–27, 1991.

Keywords: limit distribution, random walk, Airy function, path length .

[275] K. Tsiflakos and S. C. Mathewson. A Rapid Railway Simulation Model Development System Incorporating Automatic Model Generation. In *Winter Simulation Conference*, pages 792–801. IEEE Computer Society Press, December 1991. .

[276] K. Tsiflakos and D. B. Owen. A graphical sytem for the interactive visual modelling of railway transportation layouts. In *COMPUGRAPHICS '91*, volume I, pages 409–418, 1991. .

[277] Arun G. Vaidya. When information is everyone's business. In *Business Geographics*, volume 2, pages 24–26. 1994.

Abstract: Philadelphia-based Consolidated Rail Corp. (Conrail), a $3.5 billion corporation, is applying geographic information systems (GIS) technology to position itself as an "information-based" company, where employees find and use information to improve processes and support decision making via their desktop PCS .

[278] S.F.M. van Vlijmen. *Algebraic Specification in Action.* Quaestiones infinitae. Universiteit Utrecht, Faculteit Wijsbegeerte, 1998. .

[279] S.F.M. van Vlijmen. Verification of the Vital Processor Interlocking. In *FME Rail Workshop 1*. Utrecht University, Faculty of Philosophy, 1998. In: [185] **RaCoSy Repository**.

[280] M. C. Van Wezel, J. N. Kok, J. Van den Berg, and W. Van Kampen. Genetic Improvement of Railway Timetables. *Lecture Notes in Computer Science*, 866:566–??, 1994. .

[281] M. C. VanWezel, J. N. Kok, J. VanDenBerg, and W. VanKampen. Genetic Improvement of Railway Timetables. In Y. Davidor and H.-P. Schwefel, editors, *Parallel Problem Solving From Nature – PPSN III*, volume 866 of *Lecture Notes in Computer Science*, pages 566–575, Berlin, 1994. Springer Verlag. .

[282] Reinhard von Hanxleden. Robustness Analysis: A Light–weight Approach to the Formal Analysis of Safety–Critical Systems. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. DaimlerChrysler Research, Berlin, Germany. ESPRESS.

[283] Reinhard von Hanxleden, Ali Botorabi, and Slawomir Kupczyk. A Co–Design Approach for Safety–Critical Automotive Applications. In Dines Bjørner and Maria Fahlén, editors, *FME Rail Workshop # 4*, volume # 4 of *FME Rail Workshop; Stockholm, Sweden.* FME: Formal Methods Europe, Banverket, Falun, Sweden, May 12–14 1999. DaimlerChrysler Research, Berlin, Germany. **RaCoSy Repository**. ESPRESS.

[284] M.A. Watson-Walker and R.J. Gray. The Institution of Railway Sigalling Engineers' Licensing Scheme - Promoting Competence in the Workplace. In Felix Redmill and Tom Anderson, editors, *Safety-Critical Systems: The Convergence of High Tech and Human Factors: Proceedings of the 4th Safety-critical Systems Symposium Leeds, UK 6-8 February 1996*, pages 124–138, Leeds, UK, 1996. Springer. .

[285] S.J. Westerman, N.M. Shryane, and J. Sauer. *Task Analysis of the Solid-State Interlocking Design Process.* Department of Psychology, 1994.

Abstract: This report details the initial analysis of the safety-critical design task used as a case study for the project; that of data preparation for Solid-State Interlocking, a microprocessor- based control system for railway signalling. Hierarchical Task Analysis is used to study task structure, staff allocation and the impact of computer automation of parts of the task .

[286] F. Widebäck. Logical Foundations of CVT. Technical report, formerly: Logikkonsult NP AB, now: Prover Technology, 1993. NP-RES-CVT-1.

Comments: CVT was our first tool in the railway domain, and it is based on Stlmarck's method .

[287] R. Wilkinson. Electronic Data Interchange and its Relevance to Australian Railway Organisations. Westrail position paper, June 1989. .

[288] G. Wirthumer and H. Lutnik. Fault Tolerance for Railway Signalling - VOTRICS in Practice. *SARSS'89: Reliability on the Move*, page 29, 1989. .

[289] Wong Wai. *A Formal Theory of Railway Track Networks in Higher-order Logic and its Applications in Interlocking Design.* PhD thesis, University of Warwick, 1991. .

[290] Wong Wai. A Simple Graph Theory and its Application in Railway Signaling. In M. Archer, J.J. Joyce, K.N. Levitt, and P.J. Windley, editors, *International Workshop on Higher Order Logic Theorem Proving and its Applications*, pages 395–410, Davis, California, August 1991. IEEE Computer Society, ACM SIGDA, IEEE Computer Society Press. .

[291] T. Wood. Living with complexity (in railway software engineering). In *Living with Microprocessor Controlled Traction Systems*, IEE Colloquium (Digest No.056), pages 3/1–4, 32 pages. IEE, 1990.

Abstract: In this paper, the author argues that there are no reasons why the railway industry should be different from other industries with respect to its attitude to software engineering. For some years (perhaps about five) almost every new large railway control project has been applying structured techniques, mainly because of earlier disasters with other software methods. The author shows that we are now beginning to see them applied to smaller developments (with one or two software engineers) with good results. Whereas three years ago, one saw little evidence of these techniques, the author highlights how we are now beginning to see them being taken up by the railway industry.

Keywords: rail traffic; software engineering; structured programming; traffic computer control .

[292] J. Woodcock. A CSP Model of the Alcatel Dwarf Case Study. In Thierry Lecomte and Peter Gorm Larsen, editors, *FME Rail Workshop # 5*, volume # 4 of *FME Rail Workshop; Tolouse, France*. FME: Formal Methods Europe, Steria, France, September 22–24 1999. No copy ?? CSP.

[293] J.C.P. Woodcock, editor. *FME Rail Workshop*, volume 2 of *2nd FME Rail Seminar*, Parks Road, Oxford OX1 3QD, England, October 1998. Oxford Univ., Computing Lab. ESSI Project 26538.
Workshop venue: Canary Wharf, London Docklands, England.
Organised by Formal Systems Ltd., Oxford. Hosted by London Underground.

Contents: [136, 266, 132, 158, 89, 198, 114] as well as: A Tutorial: The RAISE Development Method (D. Bjørner based on 1994 material by A.E. Haxthausen), A Tutorial: CSP — Communicating Sequential Processes (Jim Woodcock) **RaCoSy Repository**.