No. 7 / December 2011

Insight

berner & mattner
optimizing your development

Business Unit Transportation

News – Projects – Technical Papers

Mixed Operation – Eliminating Tunnel Encounters

CENELEC Standards – Challenge and Opportunity

Software Architecture – Basis for the System Life Cycle

PREFACE

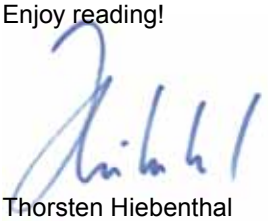
Dear Reader,

We would like to use the editorial of this newsletter edition to present a project that is of particular importance to us. As an engineering service provider, we have developed a technical system directly for an infrastructure provider for the first time. The customer was DB Netz, who has started using the "mixed traffic conflict warning system" along the high-speed section Fulda-Burgsinn. During system development, Berner & Mattner was in charge of the subsystems "central conflict detection" and "operating workstation".

The fact that we were able to put the system into operation as planned in a joined effort is not only remarkable with respect to the very tight schedule, but also with respect to the form of cooperation being the first of its kind for both companies. A key element for success was undoubtedly the close involvement of Berner & Mattner as a development partner in the entire development process, beginning with the system definition and specification. At this point, I would like to express my thanks once again for the very good and close cooperation with the project management and technical experts of DB Netz.

Our technical paper on page 6 also deals with the development of software-intensive control systems. We present a model-based approach, systematically implementing essential requirements of the CENELEC standards such as function-based development, modularity, and traceability.

Enjoy reading!



Thorsten Hiebenthal
Head of Transportation

IMPRINT

Publisher:
Berner & Mattner Systemtechnik GmbH
Erwin-von-Kreibig-Str. 3
D-80807 Munich
Phone +49 (0)89 608090-0
Fax +49 (0)89 6098182
www.berner-mattner.com
marketing@berner-mattner.com

Editorship and Layout:
Stephanie Herbst, Thorsten Hiebenthal
with thanks to the authors of the papers

TABLE OF CONTENTS

Deutsche Bahn

Mixed operation along the railway line Fulda-Burgsinn

Due to safety reasons, encounters of passenger and freight trains in multi-track tunnels on high-speed tracks are not permitted without restriction. Usually, this can be achieved by restricting the usage along the affected sections during operational phases to trains of the same type (only passenger or freight trains). But what if mixed operation is inevitable due to capacity constraints or construction works? During a three-week construction project, passenger and freight trains were redirected via the railway route Fulda-Burgsinn. A technical assistance system (conflict alert system) helped avoid encounters, amongst others.

Authors: Roland Herzig (l.), Head of I.NVT33 Interlocking Systems, DB Netz AG, and Cengiz Genc (r.), Project Manager, Berner & Mattner

To date, freight and passenger train encounters in tunnels have been eliminated by suitable operating procedures avoiding encounters of passenger and freight trains by defining time windows (day/night operation).

Construction works along parallel routes, however, forced DB Netz to find a new solution along the section Fulda-Burgsinn for the fall of 2009. Due to construction works, freight trains had to use the tunnel-rich section for a defined time during the day, in addition to passenger trains. The task was thus to reliably prevent tunnel encounters between passenger and freight trains, also for short-term schedule changes. DB Netz approached uncharted territory developing the technical protection against tunnel encounters.

Tight schedule

Work on the project "mixed traffic" started in December 2007. The railway-internal analysis and requirements description was followed by a call for tender for the technical implementation concept. Partial contracts of DB Systemtechnik were assigned to various partner companies to cover train detection and interlocking systems.

The development of the operating system and the central conflict detection – an IT system for track sensor evaluation, identification of potential tunnel encounters and communication to the traffic controllers along the way – was assigned to the system developers of Berner & Mattner.

"The development was launched in August 2008, mixed traffic was planned for the period of November and December 2009. In terms of the required testing, approval and acceptance process alone, this was an ambitious schedule. Therefore, it was important to involve a competent partner who not only has the required know-how in system technology but who is also familiar with the special procedures and organization of Deutsche Bahn," recounts Roland Herzig of the client DB Netz in retrospect.

Complex architecture

The analysis of the central conflict detection developed by Berner & Mattner is based on a total of 24 measuring points (ID locations) equipped

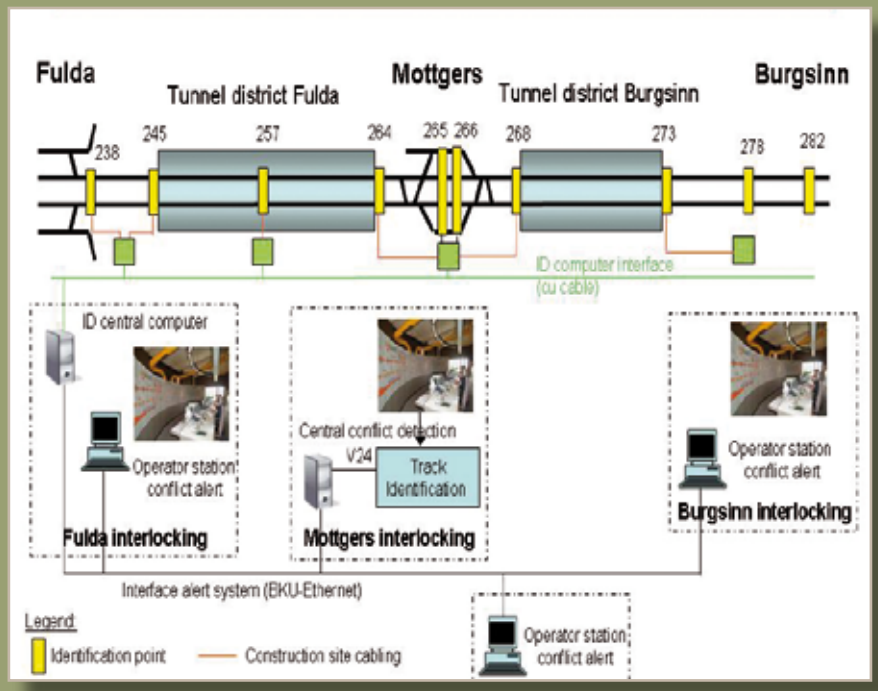
with wheel sensors along the section between Fulda and Burgsinn. The sensor data collected with the measuring points, which are placed at different positions of the high-speed line, helps recognize whether the tunnel areas are occupied by trains. Train identification means reliable detection of direction, speed, acquisition time and number of axles – and therefore the train type – through measuring points along the tracks. Sensor data is collected in various computers along the track and equipped with uninterruptible power supplies, and is finally transferred to a central collection point (ID collection computer). At the same time, the train number is evaluated as additional information from the train tracking bus.

All data converges in the central conflict detection computer system through an Ethernet network located in the Fulda interlocking. The central conflict detection then calculates if there might be inadmissible tunnel encounters. Hence, while these inadmissible encounters are already excluded from the regular schedule, with technical support they are also eliminated in exceptional situations such as delays.

Conflict warning via the operating station at the train controller

If the central collision detection recognizes potential inadmissible tunnel encounters, it generates visual and audible alerts. They are activated at the operating stations located at the workplaces of the train controllers in the interlockings Fulda and Burgsinn. Additionally, due to redundancy reasons, there is another operation station at the dispatcher in Frankfurt. He has to react only if the warnings and countermeasures taken are not acknowledged by the responsible train controllers.

"Technically, it would be possible to allow for countermeasures to be directly taken by the central collision detection. But due to legal and license reasons it was decided to start with an assistance system – after all, it was only for a period of three weeks," says Roland Herzig.



System setup

Benefits:

- Technical elimination of inadmissible tunnel encounters
- Flexible response to short-term schedule changes
- Individual solutions for various infrastructures
- Possible subsequent inclusion of additional requirements
- Short project times

Unique in the network

The central collision detection is still a unique project in the network of Deutsche Bahn and not yet approved for use with safety responsibility. There are many indications, however, that the challenges of the technical assurance of a mixed operation will be faced more often in the future. In particular, freight traffic from the seaports and through the bottlenecks from north to south plays a central role. On many new routes, the track runs mainly in tunnels or on bridges requiring correspondingly customized solutions. The developed system architecture and the lessons learned for the route between Fulda and Burgsinn, however, could be replicated.

"Against the background of long-standing experience in the development of railway systems, the experts have designed the central collision detection in a configurable way. It was thus possible to react on and include additional requirements even in later phases of the project, for example to satisfy permit authorities. In addition, automated test procedures have contributed significantly to the relatively short project times," comments Roland Herzig.

Embedded Software Architecture

Solid basis for the entire system life cycle

The only constant is change, even for products. Software architecture is crucial for continuous changeability, thus making complex systems ready for the future. Improper software architecture runs the risk of expensive subsequent adjustments, rapid technological obsolescence of the solution and lack of scalability. Early investment in the explicit design of software architecture leads to long-term cost savings in development and maintenance.

Software architecture is the structured arrangement of system components, indicating the communication relationships between the components and their mapping on hardware or software resources.

In fact, each software system has a certain architecture, even though it may not have explicitly been modeled. If it is the accidental result of the components' development dynamics, a functionally complete and accurate application may emerge all the same. Problems appearing later during maintenance, scaling or porting, however, are inevitable.

In retrospect, it has fatal consequences to quickly decide on a particular communication technology, an interface, or even a programming language under time and cost pressure in the development process, often without any documentation. Considering the life cycle of the product and the changeability needed for long-term success, this decision then simply has been wrong.

Architecture – an integrated element

In modern, agile development processes, the solution design takes place continuously, leading to new architecture requirements across the entire development process. Without continuous monitoring and correcting, a system will be very different from the documented architecture. Moreover, it will not adhere to prescribed approaches ensuring scalability. Well-designed software architecture minimizes the efforts for any necessary design changes at late stages of the project.

The ideal software architecture for your system

Do time pressure and high expectations for results force your developers to concentrate their capacity on the functional requirements of a system? By involving experienced software architects already at the early stages of development, key non-functional aspects can be considered as well.

The benefits are obvious:

> Clear structures, professional documentation

> Life cycle prediction

> Integration of state-of-the-art technologies

> Deliberate design decisions based on objective criteria

> Adaptable, future-proof products

Service portfolio of Berner & Mattner

> Software architecture development and project support

> Analysis of existing software architecture

> Coaching and moderation

For more information please visit: www.berner-mattner.com/en/sw-architecture

Complete Technical Paper for Download:
www.berner-mattner.com/en/technicalpapers

CENELEC Safety Standards

Challenge and opportunity

In the face of the growing complexity and networking of railway systems, the requirements concerning the development of safety-critical control systems are getting more and more challenging. For this reason, the legal requirements of the safety standards should not be perceived as unnecessary costs but as a tool for optimizing the development. This article presents an approach to model-based development of safety-critical systems, mainly derived from the V-model of the CENELEC standards family.

Author: Dr. Alexander Harhurin, Consultant at Berner & Mattner in Munich

Challenge and opportunity

The share of electronic and software-intensive control systems in railway engineering has increased significantly in recent years. Due to the growing complexity of these systems and the legally required evidence of product safety, the application of safety standards is essential, helping manufacturers provide evidence of the compliance with safety requirements. The standards requirements should not be perceived as disagreeable additional expenses but as an opportunity for optimizing the development. The standards describe methods and techniques that in practice have proven to be suitable tools for quality improvement and cost optimization during the development of safety-critical systems.

Requirements concerning the modeling technique

The following development process requirements can be derived from the standards:

> *Function-oriented development*
The technology must support the modeling not only of components but of system functions as well.

> *Modular development*
The technology must be able to decompose a system into its subsystems.

> *Traceability*
The technology must be able to manage links between functional requirements, components, and ECUs.

Model-based development

This article presents a modeling technique for developing software-intensive control systems as applied at Berner & Mattner. For a detailed description of this technique, please refer to the full version of this article in Eisenbahntechnische Rundschau (ETR) no. 10. The basic idea behind this technique is a model-based system development along the system life cycle of the CENELEC standard. In this way, the basis is created for a systematic

development process of safety-critical systems and tool support.

System interface

In a first step, a system is determined by defining the system boundary to its environment. All elements that are not within the system boundary belong to the environment. Afterwards the system interface for the overall system to be specified is determined.

Function-oriented specification

Based on the previously defined interface, the system functionality is specified. The functionality of a system results from the combination of individual system functions. The functions only specify the external behavior of the system and avoid preliminary decisions regarding the system design. Functions are modeled using interaction patterns in order to make the complexity of the functions manageable and comprehensible for all participants. An interaction pattern is a sequence of messages between the system and its environment, observable at the system boundary and in a timely order.

Subsequently, individual functions are integrated into an overall model taking their interactions into account. Interactions between functions describe how the independently modeled functions interact with one another to provide the desired overall behavior. To get an overview of a variety of functions, they are structured hierarchically.

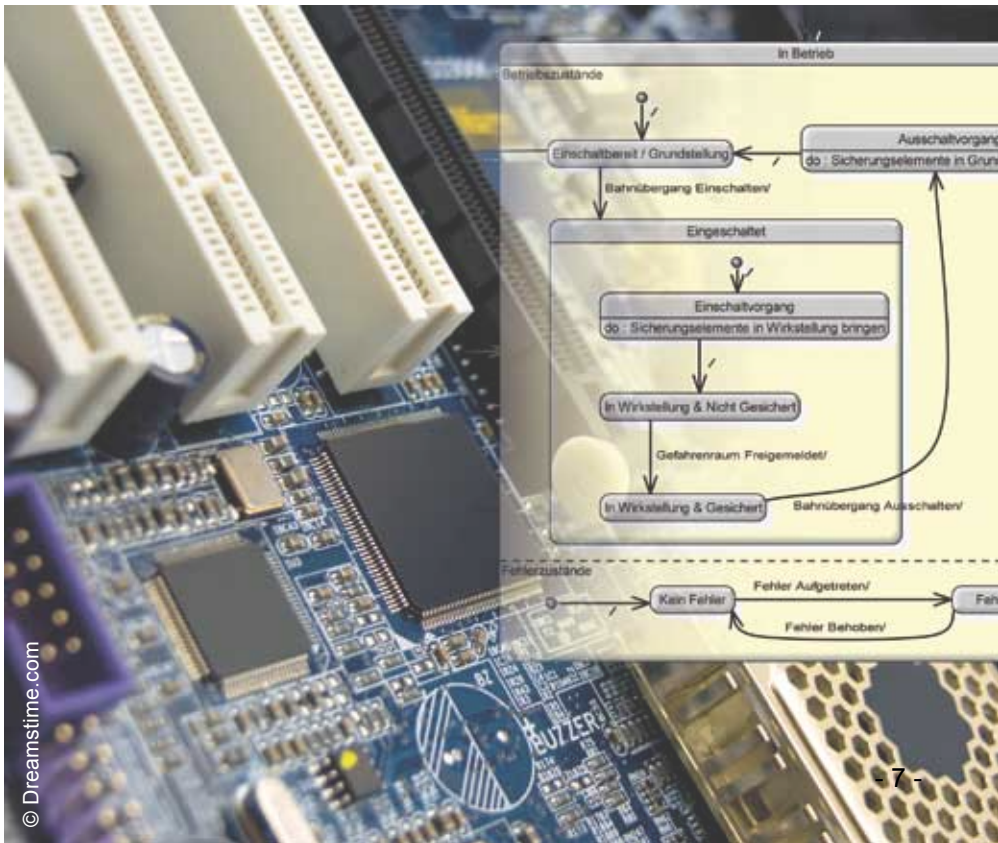
Logical and technical architectures

In the development cycle, the logical architecture of a system directly follows the function hierarchy. It provides a rough system decomposition into its subsystems and logical components. Compared with the functional hierarchy, the main focus of the logical architecture is no longer the specification of the functionality observable at the system boundary but rather the system structuring or splitting into logical, communicating units.

A logical architecture is essential for the successful development of a system. In this architecture, safety-critical functions are clearly differentiated from non-safety-critical ones as required by the safety standards. Moreover, this differentiation reduces the effort for providing a proof of safety for safety-related functions. A system is rarely developed by a single team. The development of complex systems is in fact characterized by the classic supply chain process. The structuring of the system into manageable subsystems with well-defined interfaces reduces the communication effort between developers and suppliers. The technical architecture describes the implementation consisting of hardware and software.

Traceability

In the development of complex systems, it is common that the requirements and the technical infrastructure of the systems to be developed vary continuously. For the maintenance of such systems it is important to be able to trace the impact of these changes. Therefore, the EN 50129 lists the requirement that the requirements traceability must be a fundamental idea regarding the validation of a system, and that there have to be funds available to demonstrate this in all phases of the life cycle. Individual elements of the presented model are interlinked by traceability links in order to fulfill the requirement concerning the traceability between all artifacts of the development process. These links define which requirements are implemented through which functions and ECUs, respectively.



© Dreamstime.com

Summary

The following summarizes the advantages of the presented model-based approach:

The function-oriented specification is clear and precise, being able to serve as a contract between principal and manufacturer.

System functions and not components are the focus of this approach, simplifying the required proof of safety for all safety-related functions of a system.

The logical architecture structures the system into logical units. The structuring of the system into manageable subsystems with well-defined interfaces reduces the communication effort between developers. In addition, safety-related functions are differentiated from all other functions in the logical architecture.

All models are linked to one another by traceability links. This is necessary for a consistent proof of safety of individual system functions and reduces the effort of system maintenance.

Conclusion

The presented approach provides the basis for a systematic development process as well as a model-based tool support.

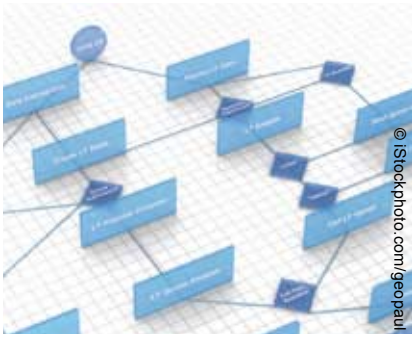
In addition, the legal requirements to provide a proof of safety for all safety-related functions can be fulfilled.

Proof of Safety

> Safety and validation plan
> Hazard and risk analysis
> Safety assessments along the process
> Process consulting on development and validation

Software Engineering

> Specification techniques
> Architectures
> Model-based development
> Development according to SIL 2
> Test engineering
> Assessment according to EN 50128



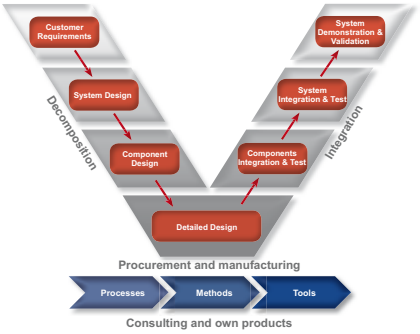
© iStockphoto.com/geopaul

Systems Engineering

> Understanding of the system functions
> Modeling of the system behavior
> Deriving of the system architecture

Processes and Standards

> EN 50126, 50128, 50129
> IEC 61508
> V-Model XT
> Requirements engineering
> Quality assurance
> SIRF, VVIBG, TSI, CSM



SCORE Student Contest: B&M Student Konrad Reiche in the Winning Team of FU Berlin

Students of the Institute of Computer Science at Freie Universität Berlin have won the international contest on software engineering – in short "SCORE". A member of the winning team was our student trainee Konrad Reiche (Transportation Systems, Berlin), who prevailed with his four teammates against 83 teams from 22 countries.

The Software Engineering Contest "SCORE" was organized as part of the prestigious ICSE (International Conference on Software Engineering) in Honolulu, Hawaii, from May 21 to 28, 2011. It takes place every two years and is organized by a worldwide group of computer science professors with the aim of challenging the world's best student teams in software engineering. The green light was already given in spring 2010. From then on, the students of FU Berlin adopted the most advanced software engineering methods in an exemplary form and used genetic algorithms to develop a web-based planning system for lectures and courses at universities and schools. In addition to features such as the course catalog, the software "SceTris" allows to automatically generate schedules and display scheduling conflicts. The room usage is thus optimized, since it already indicates during the planning phase if, for example, a tutorial takes place at the same time as a lecture of the same semester.

The 20-page summary report and the submission of the entire project, including design documents and source code, have convinced the jury. Among the world's top five teams – from Germany, Croatia, Sweden, Singapore and Spain – the Berlin students were invited to the conference in Honolulu. With three presentations in the form of lectures, poster and demo sessions, the students of Freie Universität Berlin were able to convince in the finals and ranked first.

Dr. Matthias Grochtmann, Team Leader Transportation Systems, Berlin (r.), compliments the awardee Konrad Reiche (l.).

Manfred Heidegger Takes Over Team Management of System Engineering in Vienna

Since July 2011 Manfred Heidegger has been directing the newly formed team "System Engineering" at Berner & Mattner in Vienna. He is the ideal internal filling of this position. Previously, since the start of the Vienna subsidiary in 2009, he had worked as project manager for Transportation Systems at Berner & Mattner. He had successfully implemented projects, both in the railway infrastructure sector and the rail vehicle development, for major rail companies and rail vehicle manufacturers.

Manfred Heidegger is an electrical engineer with focus on energy technology and power electronics. Having worked in the automotive and traffic telematics environment for more than ten years, he looks back on a comprehensive cross-industry experience in the development of complex electronic systems. Over the past two years, he has broadened his range of competence mainly with the safety-critical development of mechatronic applications in the rail industry focusing on CENELEC-compliant systems and software development with standards-compliant functional and technical safety aspects. Professional project management is another expertise of Heidegger.

Manfred Heidegger
Phone: +43 (1) 585 1861-211
Email: manfred.heidegger@berner-mattner.at

Control at your Fingertips

Berner & Mattner and Centigrade present innovative touch interface software solutions

The Munich software experts and their partner Centigrade present approved process models and award-winning practical examples for the development of intuitive touch software for industrial device control systems. The solutions developed by both partners improve among other things the usability of human machine interfaces.

Berner & Mattner and its partner Centigrade show how manufacturers of machinery and plants can improve functionality and usability of human machine interfaces through modern, touch-sensitive interfaces.

"Intuitively usable human machine interfaces are competitive factors in today´s industrial device development. Very often, however, the resulting market opportunities are neglected in the development of new products", explains Dr. Klaus Wiltschi, Head of the Industrial Customers Department at Berner & Mattner. "High-quality touch displays are state of the art for industrial control units. Together with modern software platforms, they offer multiple options for efficient and effective interaction solutions. The development of intuitive touch user interfaces, however, requires specific expertise regarding usability, relevant HMI development processes and innovative GUI software technologies. Together with Centigrade, we have successfully broken new ground in the development of touch interfaces. We apply specialized development tools and processes and support manufacturers of complex industrial equipment who are interested in intuitively usable touch control solutions."

Award-winning touch operating terminal

The first success of this new approach to developing human machine interfaces is an award-winning touch operating terminal for an electrical engineering test device developed by Berner & Mattner and Centigrade in cooperation with OMICRON electronics. The UI design of Centigrade has been granted the iF communication design award.

Innovative touch interface for electrical engineering test device by OMICRON

For more information please visit: www.berner-mattner.com/en/touch-interface-software

News from other industries

Dr. Christian Hock, Head of Industry Division:

The user-centric development of HMI solutions has many advantages:

- Optimized user interaction
- Workflow-based user guidance
- Attractive look & feel
- User-verified with prototypes and mockups
- Flexibility in development

To further strengthen our teams of the Railway Division in Munich, Berlin, Braunschweig, Erlangen, and Vienna we are looking for (m/f):

Safety Engineers Rail Vehicles

System Engineers Rail Vehicles

Software Developers Transportation

We offer graduates and career changers (m/f), in particular, an intensive and individualized training program. Berner & Mattner provides attractive conditions, individual development plans, team support, freedom to build your personal career and the opportunity to take on responsible tasks.

No suitable position for you?
If you are experienced in technical software development and have skills in railway or automotive, aerospace, defence or industrial automation, we look forward to receiving your application. We will review your records and contact you as soon as we have an appropriate position to fill.

For detailed information about the company and the individual positions, please visit **http://www.berner-mattner.com**. We look forward to receiving your convincing application. Please use our online application form at **http://www.berner-mattner.com/bewerben** (German).

Ms Anja Ranft
Human Resources Manager
Erwin-von-Kreibig-Str. 3
D-80807 Munich
Phone +49 (89) 60 80 90-201
Fax +49 (89) 609 81 82
Anja.Ranft@berner-mattner.com

www.berner-mattner.com/de/jobs

berner & mattner
optimizing your development

berner & mattner
Systemtechnik GmbH

The previous issues of *Insight* Transportation (issues 1 to 5 are only available on our German website) can be downloaded at:

www.berner-mattner.com/en/download-center/newsletters

May 2011

>> Partnership – Rail Industry counts on Berner & Mattner

>> SysML Modeling – High-quality Interface Specifications

>> Internationalization – Berner & Mattner joins Assystem Group

October 2010

>> Framework Agreement - Development Services for Bombardier

>> CENELEC Conformity - Development of Rail Vehicles

>> Axle Counting Systems - Model-based Specification

April 2010

>> MERAN for DOORS® - Specification of Systems with Many Variants

>> E-Ticketing - Model-based SW Development for Embedded Systems

>> Quality Improvement - Automated Test of an Anticipated SW System

December 2009

>> Pioneer Work in Series - 30 Years of Berner & Mattner Systemtechnik GmbH

>> Model-based Methods - Key Factors for Modularization

>> Profitability Analysis of Projects - New Evaluation Tool