Tailored Solutions for Safety-Installations in the Loetschberg Tunnel - A Project with Importance for the Trans-European Rail Traffic

Walter Fuß, Thales Rail Signalling Solutions GesmbH, AU

Abstract

The Loetschberg base tunnel was the largest project for the Swiss railway infrastructure in the last five years. With a length of 34,6 km it is the third longest tunnel in the world at present. The maximum speed allowed to drive is 250 km/h. The project comprised four interlocking stations, ETCS Level 2 and additional automatic functions to handle the traffic through this tunnel in an optimized way. To fulfill all the safety requirements and the challenges of reliability and maintainability of this very long tunnel a lot new functions were to be realized in each of the mentioned systems. Following a unified approach using certified hardware and middleware and enhancing the scope of test to a total system simulation these demands were met. This article focuses on the challenges for the interlocking system LockTrac 6131 ELEKTRA.

1. Introduction

Thales Rail Signalling Solutions was contracted to deliver and install the signalling systems for the line from Frutigen to Visp in May 2003. The tunnel shown in figure 1 comprises one tube spanning the whole length and another one that is equipped with rails only for a length of 13 km in the south and 1 km in the north.

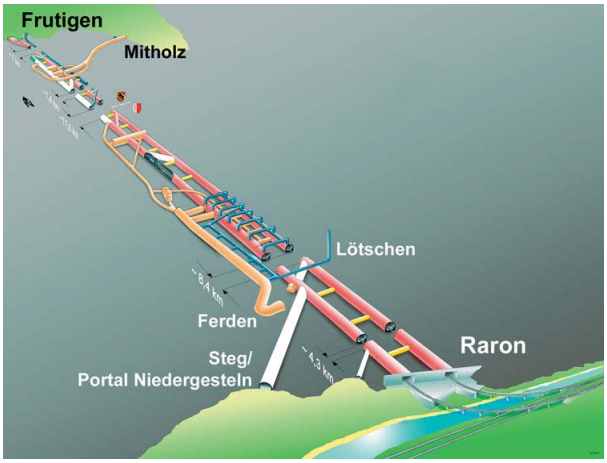

Figure 1: The Loetschberg base tunnel

The rail connection in the tunnel is realized as a high-speed point that allows the speed of 250 km/h along one branch and 180 km/h along the other one. To permit such high velocities it is not possible to use conventional optical signals but cab signalling must be used. The customer decided to install the train protection system ETCS Level 2 where the information of train routes coming from the interlocking stations is collected by the RBC (radio block centre) - the core component of the system ETCS Level2. The RBC sends to each train in the considered area the specific movement authority via GSM-R. This information is received by the on board unit OBU which displays the currently allowed maximum speed in the driver's cabin continuously.

Most of the customer's requirements came from safety considerations and from the high availability demanded for commercial operation as well as from the challenge to maintain all the equipment and railway installations in the tunnel. These requirements had to be realized basically in the interlocking systems. Fundamental assumptions concerning the safety relevant issues were scenarios of disturbances or dangerous situations like fire in the tunnel. In these cases it is requested to evacuate the tunnel as quick as possible. For this reason e.g. backward driving was demanded as an interlocking feature, an action which usually is strictly forbidden for train movements.

The automatic functions are considered not to be safety relevant by system design. All safety requirements have to be enforced by the interlocking and by ETCS. The tasks of the automatic functions are to control the traffic by requesting train routes from the interlocking stations for the trains traveling through the tunnel and to avoid conflicts like traffic jams.

The correct and effective interaction of these systems is of crucial importance for smooth execution of the traffic management and of the maintenance activities. Due to the fact that the development of ETCS took place in Germany, the realization of the interlocking functions was carried out in Austria and the automatic functions came from Switzerland this issue was a great challenge.

978-3-9810801-3-1/DATE08 © 2008 EDAA

2. Overview

The architecture of the whole system of safety installations (see figure 2) contains two interlocking stations for the tunnel (FRO and FRW) without optical signalling, one for each tube, and the interlocking for the station Frutigen (FR) in the north and another one for the station Visp (VI) in the south of the tunnel. The RBC is connected with all four interlocking installations. The automatic functions (AF) as the third part of this architecture are connected to the two interlockings of the tunnel and to the RBC. The operating personal is situated in the remote central station in Spiez (LS) where the railway stations between Bern and the boarder to Italy near Brig are controlled. The control system there was installed by Siemens. The interfaces between the interlocking and the control system are standard in Switzerland.

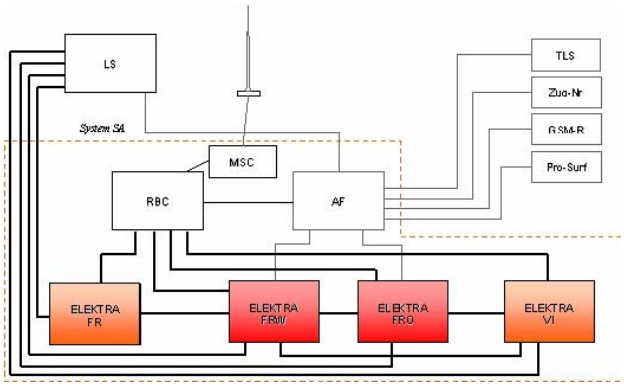

Figure 2: Global architecture

2.1. Initial situation of Thales

At the time of contracting the ETCS Level2 system was still under construction and operating on a pilot line in Germany, the automatic functions were a completely new development to be started within this project and the interlocking system ELEKTRA has been established in several stations in Switzerland since 1998, meeting all requirements of standard railway operation. In addition to this a lot of work was spent to extend the functionality up to the needs of this complex project.

2.2. Safety principles

As trains transport people and high property values all installations providing train routes – tracks, points and signals as well as the interlocking and the train protection system – are safety critical. The most recent standards in Europe (and even in the world) to define safety related issues for software based railway systems are the standards of CENELEC [1, 2, 3]. These standards define Safety Integrity Levels 0 (non safety-related) up to 4 (very high). SIL4 as the highest level means that among 100 installations at the utmost once in 1000 years a safety critical failure might occur.

2.3. New features for ELEKTRA

The new features to be realized in the interlocking system ELEKTRA involve different aspects for the development. There are new functions to be implemented in the application software as well as a new type of interface to the RBC and another type of interface to the automatic functions both affecting basic parts of the system. For the high-speed point machines the interface hardware had to be extended and last but not least the communication among the interlocking systems was enhanced by supplying a generic interface for train routes starting in one station and ending in another one.
For operating purposes the features are grouped in three classes:

- Functions for normal operation
- Functions for maintenance activities
- Functions for cases of disturbances and emergency

In particular the new features contain five new types of train routes supporting maintenance and evacuation scenarios, the new feature Maintenance-District which is a special operating state for several zones providing maintenance activities, three new “elements” (“Bahntunneltor”, “Schiebetor” and Direction Dependent Locks) and the new types of interfaces to the RBC and to the automatic functions. All those features are safety relevant. How the SIL4 is achieved in the system ELEKTRA will be explained in the next chapter.

3. System ELEKTRA

The interlocking system LockTrac 6131 ELEKTRA was introduced in Austria in 1989, in Switzerland in 1997 and in Hungary in 1998. A system upgrade to the next generation ELEKTRA2 was done from 1998 to 2002 when the first ELEKTRA2 was set into operation in Neuhausen, Switzerland.

3.1. Architecture

The fundamental approach to achieve safety with the system ELEKTRA is the two-channel architecture and diverse programming (see [1]). Strictly apart of that there are redundant system elements to enhance reliability and availability. For architectural and maintainability reasons the system is split into three levels, HMI, central controller and field element controller that comprises the element controller EC and the interface controllers IC.

In addition to the three levels shown in figure 3 there is a component for long distance communication and external interfaces respectively. This Remote Control Unit (RCU) has also a two-channel software architecture and provides the interfaces to RBC, to the automatic functions and to the neighbouring interlocking as well as to a remote control system.

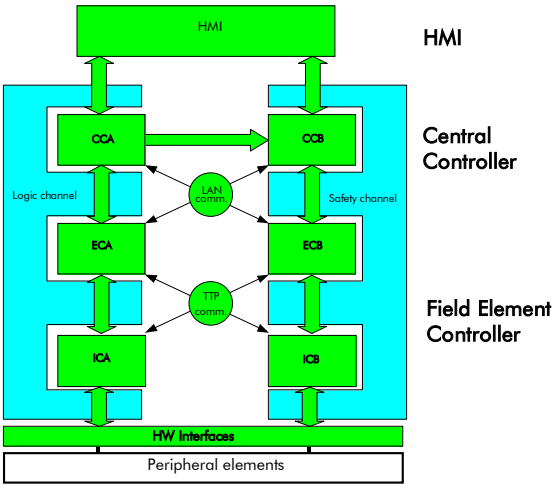

Figure 3: SW-Architecture of ELEKTRA

In opposition to the two-channel architecture of the CC the HMI contains only one software channel. The safety relevant information items – display information or operator commands – are handled according special methods providing the safety via two-fold and three-fold communication with the safe central layer and acknowledgment of each step by the user so that SIL4 is reached. This concept is called the method safe HMI.
The complex customer specific requirements are implemented in the application software of HMI, CC and EC. Contrary to the shrinking hardware life cycles the customer expects a product lifetime of 25 years including availability of spare parts and maintainability of the system all the time. So in order to achieve independence of the application software from the actual used hardware the TAS control platform is used.

3.2. TAS control platform

The TAS control platform is a vital computer platform, which is designed to support computer-based railway safety installations such as electronic interlocking, axle counters or train protection systems like RBC and on board units. It separates the railway specific applications from the hardware and system software technology and serves as a common base for these applications.
The TAS control platform is an open, scalable software architecture oriented towards established industrial computing standards. Its core incorporates software components such as a Portable Operating System Interface (POSIX) compliant operating system, a fault tolerance system and a communication system.
The fault tolerance system offers configurations like 2-out-of-2, 2-out-of-3 or even the non-redundant variant 1-out-of-1. For example the Thales axle counter uses the 2-out-of-2 and the 2-out-of-3 configurations, the RBC and the OBU are 2-out-of-3 systems. ELEKTRA is in terms of the TAS control platform a 1-out-of-1 system, where redundancy handling is part of the product specific features.
At the hardware level the TAS control platform uses commercial standard components, which are supplemented by added-value services for railway systems. For example the RBC and ELEKTRA uses the same controller boards though both have totally different software architectures.
The TAS control platform offers a layered architecture to take advantage of the rapid evolution in hardware and software technologies. It deals with different component lifecycles and the integration of third-party software and commercial standard components. Figure 4 shows the structure consisting of an application layer, middleware layer, operating system layer and hardware layer. The orange areas show the application domains, the blue areas show the parts of the TAS control platform and the yellow areas represent the third party and commercial components.

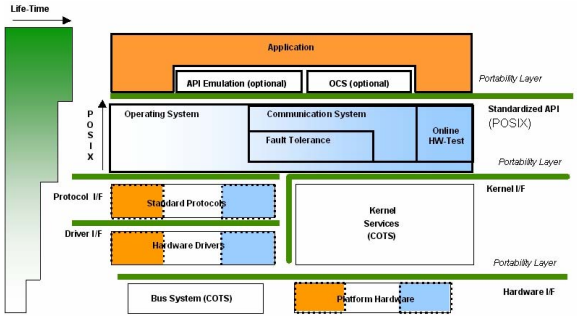

Figure 4: Architecture of TAS control platform

The application layer represents the product providing the functionality requested by the customer. A standard Application Programming Interface (API) insures the independence of the application software from the underlying system.
The middleware layer contains application transparent communication and fault tolerance mechanisms to deal with the redundancy, fault tolerance and communication requirements.
The operating system layer includes a real-time kernel and protocol stacks, consisting of standard commercial components. The TAS control platform also supports the

integration of drivers and protocols developed in the application context as loadable modules.
The hardware layer has the shortest lifetime because of rapid technological evolution.
So the TAS control platform introduces strict separation between the hardware, operating system and the application software, thus ensuring that it provides the long lifetime required by complex railway applications while benefiting from the rapid progress in computer technologies. All terms of safety, reliability, performance and certification concerning hardware and software layers below the application software are handled by the certification of the TAS control platform.

3.3. Two-channel-approach

The main characteristic of the ELEKTRA system design is the two-channel architecture. Each channel processes its specific software in the sense of diverse programming. Defining coding rules that differ between the two channels, use of different algorithms and different roles like master/slave the differences between the application software of the two channels are forced. However, in the central layer the channel B (CCB) is written in a rule based programming language called PAMELA, which was developed by Thales and follows the algorithm of RETE networks. So the CCB is working as an expert system. Additionally each channel has a separate team of engineers designing and coding the application. Due to these efforts it is possible to run both software channels on one controller board still meeting SIL4.
This architecture produces some constraints for the development process. The contradiction of the independence of the software running in different channels and the demand of the close and synchronous interaction of the two channels is solved by splitting the development process in phases with common and phases with separated development activities. Conjoint work is done in the phases of requirements specification, architecture and design but disjoint work while module design, coding and module test. Nevertheless discussions and peer meetings are possible, necessary and therefore welcome all the time.

4. The realization

The time frame given by the customer in May 2003 included a development phase till middle of 2005 followed by a lot of different test activities together with the customer accompanied by reworks if necessary. The circumstance that 50% of the whole time frame was spent for operational tests was the result of the experiences of the customer gathered in previous projects with ETCS (Olten-Luzern 2000-2002, Mattstetten-Rothrist 2002-2004) where the tuning of the operational processes and the training of the staff were the most critical issues to achieve the optimal performance.
The date to set the line through the Loetschberg base tunnel into operation was defined by May 2007 when a restricted commercial usage would start. Full commercial operation was planned on December 9th, 2007.
Under these preconditions the time frame for the development concerning the interlocking functions was rather narrow and led to a high number of parallel executed activities. There were roughly three main parts in the workflow, requirements specification, software development and tests.

4.1. The requirements process

The customer had a quite clear idea of the new functions he needed but the detailed implications and the interaction of these features within the complex functionality of an interlocking system had still to be analyzed. So the requirement specification phase became perhaps the most important segment of this project where the combination of technical knowledge and understanding of customers needs were the key for the success of the project.
This phase started in September 2003 performing a biweekly meeting with the customer and most intensive analysis activities in each unit until December 2003 when the development phase was started. As a consequence 21 features ordered by the customer resulted in 392 system requirements were constructed.
To handle the requirements management process the tool DOORS was used, nowadays under control of TREK (Thales Requirements Engineering Kit).

4.2. The development process

The development process for ELEKTRA follows the V-model (see [1] figure 4 and [2] CENELEC: “Railway Applications: Safety Related Electronic Systems for Signalling", Ref no EN50129, February 2003
[3] figure 5). With respect to the high number of functions implemented in parallel running activities this process model applies to each development path organized as a subproject. Starting from the system requirements specification delivered by the requirements process each function development runs through the phases architecture & design, module design, coding, module test, integration and validation. Restrictive configuration management concerning software items as well as documents enabled this parallelism of activities. Using ClearCase it was possible to develop one software module for different features using different branches for each subproject. After finishing the development of a single function the modified software items had to be merged into the main branch. Though efficient tool support this is a critical action and therefore followed by another system validation phase,

which is performed independently as required in [1] for SIL4-systems.
The extension of the functionality of ELEKTRA is covered by an established process and is facilitated by the modularity of the software architecture. In the special cases of the new types of train routes the extension was done by broadening the functionality of existing modules whereas the features Direction Dependent Lock and Maintenance-District were introduced by the implementation of new software modules.
The most innovative enhancements from the technical point of view are the new external interfaces. Especially for the connection to the RBC the One Channel Safe (OCS) communication layer was introduced in the system ELEKTRA. OCS is a functionality provided by the TAS control platform to transmit safety critical information using one physical link. A second physical link can be configured for redundancy reasons. Originally designed for 2-out-of-2 and 2-out-of-3 systems the RBC possessed this communication technique from the very beginning. But for the 1-out-of-1 system (in the perception of the platform) and the two channel architecture of ELEKTRA this functionality was to adapt basically before implementing in the interlocking software.
Also the interface to the automatic functions lead to an additional technology for external interfaces using XML where so far X.25 with railway specific protocols was used. The development was performed in conjunction of three engineering projects, ELEKTRA, TAS control platform and the receiver systems RBC and automatic functions respectively.

4.3. Testing in five dimensions

Verification and validation of the system ELEKTRA is partitioned into three areas of tests containing module tests, subsystem tests and system tests which are performed according to the V-model of the development process. However, the prime challenge was the interaction and cooperation of the three systems ELEKTRA, ETCS and automatic functions. For this reason the test volume was extended by two further dimensions:

- The integration tests with all systems compound executed in the Thales lab in Zurich and
- The on site tests, partially defined and conducted by the customer

Each system had already sufficient test tools to perform all tests needed for one system alone. But integrating all systems together necessitated an overall test interface to coordinate and control the system specific test tools. With this additional layer of the test environment it became possible to simulate train movements synchronously for each subsystem and thus the interaction and cooperation could be tested in a huge number of scenarios.
The tests driven by the customer concerned the hardware installation as well as the functionality. The equipment to be installed in the tunnel was arranged in a set of containers and checked in a workshop outside the tunnel from February till September 2005. After the transfer of the containers to their places in the tunnel the functional tests began.
Executing all the test areas simultaneously and doing some rework at the same time the challenge was to coordinate all activities in a most effective way. For defect tracking e.g. the tool ClearQuest was used providing separate databases for each test area. The entries concerning the customer tests and the integration tests were the basis of the communication with the customer, which led to a efficient cooperation so that the requirements of the functionality as well as those of the time constraints were met.

5. Summary and Conclusions

The Loetschberg base tunnel project represented for Thales in general and for its interlocking system ELEKTRA in particular not only a commercial opportunity but also a considerable illustration of the leadership in the domain of railway protection systems and the chance to demonstrate the innovative power to define and implement new customers requirements within a challenging time frame. As planned full operation was started on December 9th, 2007. Especially the enhancements of the interlocking functionality and the performance during the operational phases recommend this product for further projects like the Gotthard base tunnel.

6. Acknowledgement

The author thanks the colleagues who provided information about the TAS control platform and all the reviewers who helped to improve this paper.

7. Literature

[1] CENELEC: “Railway Applications: Software for Railway Control and Protection Systems", Ref no EN50128, March 2001
[2] CENELEC: “Railway Applications: Safety Related Electronic Systems for Signalling", Ref no EN50129, February 2003
[3] CENELEC: “Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)", Ref no EN50126, September 1999