Alister 2.0 - Programmable Logic Controllers in Railway Interlocking Systems for Regional Lines of the DB Netze AG

Reiner Saykowski, Elferik Schultz, and Joachim Bleidiessel

Funkwerk Information Technologies GmbH
Edisonstraße 3, 24145 Kiel, Germany
{reiner.saykowski, elferik.schultz, joachim.bleidiessel}@funkwerk-it.com
http://www.funkwerk-it.com

Abstract

Railway interlockings are dominated by highly proprietary systems. We present the development project Alister 2.0 – an interlocking system based on industry-proven standard components: Safety PLCs in distributed nodes communicate over safe network protocols. This enables a highly productive and highly maintainable fail-safe interlocking system for centralised traffic control.

Keywords and phrases electronic interlocking, PLC, regional lines, ESTW-R

Digital Object Identifier 10.4230/OASIcs.KiVS.2011.205

1 Introduction

About 1000 railway interlocking systems in Germany reach the end of their life-cycle within the next years, most of them controlling regional lines. Furthermore, the DB Netze AG as operator faces increasing cost pressure and wants to raise its competitiveness. Hence, it is the defined aim to perform the modernisation of these interlocking systems with cost-effective, standardised and modular components, while still meeting the requirements and the railway standard CENELEC EN 50126[1], EN 50128[2] and EN 50129[3]. Among other things these standards impose a development process and safety requirements for the hard- and software. Consequently the Functional Specification ESTW-R (Electronic Interlocking for Regional Lines) was published, which encouraged a strongly modularised structure that consists of industry-proven common off-the-shelf products (COTS). This implicates a new system architecture and at the same time offers the chance of opening the separated market to new competitors. In summer 2006 Funkwerk Information Technologies GmbH was commissioned to equip the regional line connecting the cities of Kiel and Flensburg with a new interlocking system. With this innovative approach, the development project entered the phase of safety approval at the end of 2009. This was the first time COTS products were deployed in a interlocking system using a distributed architecture.

2 System Concept and Architecture

Although the regional line between Kiel and Flensburg is more than 50km long, it is monitored and controlled by just one control centre. This overall architecture is depicted in Figure 1 and will be explained now. The distributed computing nodes at the stations are called local ESTW-R. They are redundantly connected to the control centre via standard ethernet connection over optical fibre. The signalman operates the line from the control centre with one technical procedure-protected workstation running under Linux. Supported by train describer and train routing functionality, the signalman sends commands to set the

17th GI/ITG Conference on Communication in Distributed Systems (KiVS'11).
Editors: Norbert Luttenberger, Hagen Peters; pp. 205–207

OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

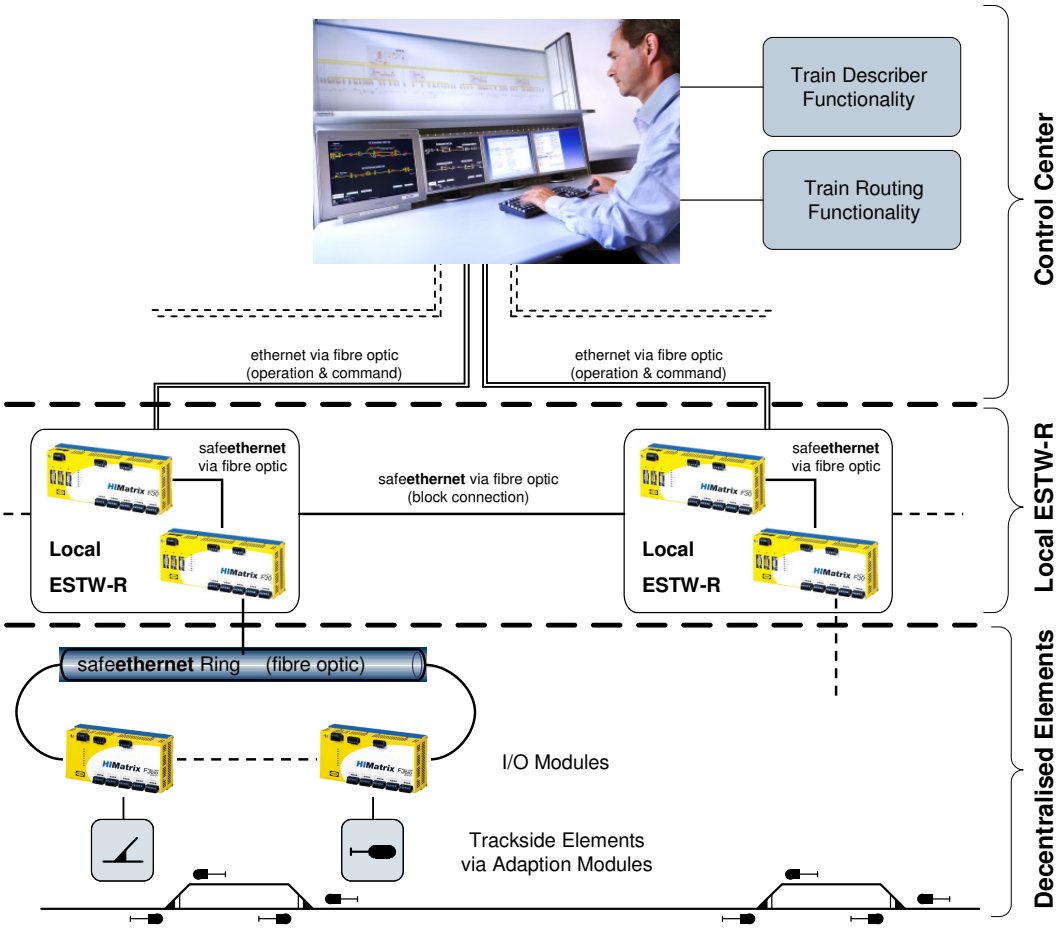

Figure 1 Network architecture of the development project Alister 2.0

train routes correctly. In the local ESTW-R computation is done by industry-proven safety Programmable Logic Controllers (PLC). PLCs follow a model of successive cycles, where each cycle consists of three sequential phases: read input, compute, write output. The PLCs communicate with so called decentralised I/O-modules via TCP/IP protocol over *safeethernet*. Safeethernet is a certified safety protocol, based on standard Ethernet technology IEEE 802.3. It is developed by the company of HIMA[1]. The I/O-modules drive the adaption modules, which in the end control the trackside elements, e.g. points, signals or level crossings.

2.1 Local ESTW-R — Interlocking logic with safety PLCs

A single local ESTW-R is composed of two safety PLCs, whereby every PLC is internally based on a 2oo2-architecture ("2-out-of-2"). Therefore, if one failure is detected by one of the PLCs, the PLCs will switch to a safe state – this is an integral requirement for safe railway operations. The PLCs are programmed in Function Block Diagram language (FBD), corresponding to the IEC 61131-3 Standard. IEC 61131[4] describes the standard use of PLCs, including general information, equipment requirements, communication and

[1] safeethernet is a registered trademark of HIMA Paul Hildebrand GmbH + Co KG, http://www.hima.de

standardised programming languages. Furthermore, to meet the requirements of the railway CENELEC standard only a subset of the FBD language is used, e.g. to avoid infinite loops. To set up train routes from one local ESTW-R to the next local ESTW-R, both communicate over safeethernet. Thus, data corruption, loss of data and data sequencing problems in communication between the nodes are detected. The decentralised I/O-Modules, which get their commands over safeethernet from the PLCs, are connected in a ring-structure, due to availability-considerations. The time to switch the direction of access in the ring-structure after a problem occurred is less than the minimum cycle-time of a PLC. Therefore, a switch in the flow of information will not interrupt the system. The I/O-modules drive the adaption modules. In turn these are not limited to actuate typically trackside elements. Because of their configurable and open communication interface, they can also actuate arbitrary digital in- and outputs, like axle counters.

2.2 Technically procedure-protected workstation

The complete route between Kiel and Flensburg is controlled by the technically procedure-protected workstation. At each point in time it presents an up-to-date process image on the workstation of the signalman. The integrity of the process image is secured by a patented image signal comparing system. The incoming image signal is received via two independent channels and compared twice a second. Single failures in communication or single components will be detected by the system and lead to a safe state. In this state only standard operations are allowed.

3 Outlook

With its maximum number of 10 distributed interlocking nodes already today the ESTW-R Alister 2.0 is based on industry-proven, highly maintainable COTS components and industry protocols. Hence, the railway interlocking market has been opened for innovation and sustainable components which are already proven and tested in automation and process industry. A new trend has started that will lead to further cost reductions and great efficiency enhancements.

References

1 European Committee for Electrotechnical Standardization (CENELEC). *EN 50126 – Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*. 1999

2 European Committee for Electrotechnical Standardization (CENELEC). *EN 50128 – Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*. 2001

3 European Committee for Electrotechnical Standardization (CENELEC). *EN 50129 – Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*. 2003

4 International Electrotechnical Commission (IEC). *IEC 61131 – Programmable controllers*. 2000-2007