Transactions on the Built Environment vol 34, © 1998 WIT Press, www.witpress.com, ISSN 1743-3509

Safety, availability and capacity of electronic interlocking

S. Ricci
University of Rome "La Sapienza" - DTIS - Transport Area
Via Eudossiana 18 - 00184 Roma - Italy
Email: SRICC@DTIS.ING.UNIROMA1.IT

Abstract

In the paper a large range of projects and realisation in the field of electronic interlocking are analysed. Specific tools are developed with the aim of allowing the systematic comparison among different systems and of checking them on the basis of IEC and CENELEC standard rules. Further results are represented by the evaluation of plants capacity and the definition of the best field for the application of the different interlocking technologies.

1. Introduction

The typical feature of electronic interlocking is the possibility to grant safety conditions by means of computer logic (hardware and software) where the relay systems act in case of traditional interlocking. Electronic command and control systems, not performing, anyway, safety functions, have been developed before proper interlocking systems. After the first electronic interlocking developed by Ericsson all the main signalling companies developed projects and implemented plants on the basis of a various range of requirements and very often aimed at the resolution of specific operating problems (little modular stations on long lines, big stations with a large number of merging lines, etc.).

2. Common logic of electronic interlocking

Behind different technological equipment it is possible to recognise in nearby all electronic interlocking systems common basic logic and structures, due to the need of performing the basic safety and reliability requirements, which are typical of every railway approach.

Differences are introduced in order to perform specific requirements stated by railway companies and/or to attempt the optimisation of the components in performing requirements.

The common logic of an electronic interlocking (of every signal box in a wider framework) is based on four functional levels (figure 1):

- operating level: interface with human operator, receiving his commands and transmitting controls coming from the lower level of the system (input-output);
- input-output level: capable to deal with informative flows coming from or directed to operating level and open-line installations in order to make them elaborated by the safety system;
- safety level: performing the actual interlocking function, involving states of open-line installations and routes to be run and exchanging informative flows with input-output level only;
- open-line installations: receiving commands and sending controls to an upper level (input-output).

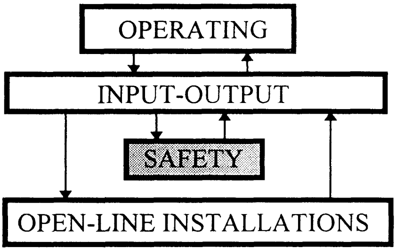

Figure 1: typical logic for electronic interlocking

In this framework, safety functions are performed only within the safety level and in the communication systems used for exchanging data with other levels. The safety level is typically characterised by redundancy, which is generally carried out on the basis of one of the two following main hardware-software interaction architectures:

- a *hardware redundant* architecture, in which the same software runs on different hardware;
- a *software redundant* architecture, in which on the same hardware run different software versions.

In both architectures the redundancy make necessary a comparison of results in order to assure the correspondence of outputs before transmitting them for the execution of related commands. In figures 2 and 3 previous architectures are shown referring to a triplicate redundancy.

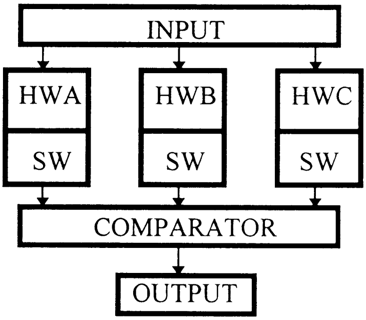

Figure 2: hardware redundant architecture

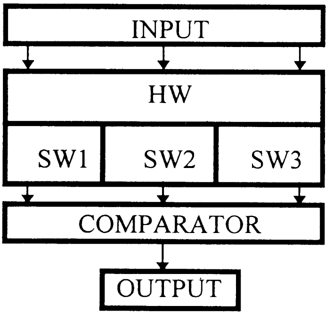

Figure 3: software redundant architecture

The introduction of redundancy is requested by safety in a probabilistic approach to the problem. In fact the fail-safe concept, employed since the origin of railways, is based on the use of components with established failure modes, on the existence of a safe condition in case of failure of one of its parts and on the arrangement of components in such a way that conditions more permissive than without failures cannot be reached. This concept has a limited applicability for complex systems employing microprocessors, where the number of failure combinations is very high and the probabilistic approach is the only effective solution.

Nevertheless it is usual to find some plants still performing all or a part of the safety level functions with traditional relay technology. They can be considered as a heritage of the first developments of electronic systems, which performed only command and control functions.

Recently the *numerical assurance* concept arose as an alternative to redundancy. It is a single processor architecture in which each element is represented by large numerical values and the vital safety functions are performed by a *deterministic pseudo-random combination of numerical parameters*, so that the correctness of results can be numerically verified. Vital functions are represented in data structures, vital decisions are not to be made in the executable software and the correctness of numerical results and input-output circuits does not depend on the correctness of this software. Quantitative check of data structures and of interfaces among hardware, software and input-output level are required. The major advantage of numerical assurance is that it can be quantitatively evaluated by calculating the probability, or its upper limit, of an unsafe failure leading to a falsely permissive output; its major advantage is the necessity of relatively powerful processors.

3. Overview of realisations

Twenty years after the first electronic interlocking was carried out in Sweden (Ericsson plants in Goteborg, 1978, and Malmo, 1980), many railway companies chose to develop similar realisations.

Fourteen stations equipped with DSI electronic interlocking systems, controlling up to 170 open-line installations and allowed up to 230 routes, were soon set up in Denmark (1980). In Japan the first electronic interlocking, acting on 25 points and 36 track circuits and allowing 106 routes, was experimented in 1981 by RTRI in the Ishiuchi station. In 1983 the first Siemens systems were installed in Germany on local traffic lines (station Uhlandstrasse on Berlin underground and station Leitstrasse on Duisburg local EH network, controlling respectively 28 and 64 installations) and in South Africa on the Arthur Taylor Colliery line. 1985 was the year of the first French system (Chateauroux station with 25 points, 27 signals, 85 track circuits and 82 routes), the first Dutch system (Hilversum station with 64 open-line installations) and the first DB station in Germany (Murnau). In 1986 Siemens systems were extended to other 4 DB stations (Detmold, Springe, Essen Kupferdreh and Overath Roesrath). In 1987 the first Alcatel SEL systems (stations of Hockenheim, with remote-control of 8 minor stations on a 50 km line section, and Neufahrn, with 22 points, 26 signals and a level crossing) and an AEG system (station of Dieburg) were installed on DB network.

In the last 10 years the electronic interlocking technologies have been strongly developed, a large number of stations have been equipped across all main railway networks. During this period Austria, Switzerland, Italy, Finland, United States and Poland too implemented their first electronic interlocking and the dimensions of stations grew up to more than 800 open-line installations (first in Chiasso and more recently in Hannover) and 5000 routes (Hannover). An overview of the main realisations in this period is summarised in table 1.

Table 1: some electronic interlocking implemented in years 1989-1997

Year	*Country*	*Station*	*Firm*	*Dimensional data*
1989	A	Neumarkt K.	Alcatel	34 P, 37 S, 2 L, 1 C
1989	CH	Chiasso	Siemens	172 P, 377 S, 295 T
1994	D	Dortmund Eis.	Siemens	28 P, 70 S
1994	I	Porretta T.	SASIB	10 P, 12 S, 15 T, 3 L
1995	D	Ingolstadt E.	Siemens	38 P, 40 S
1996	A	Salzburg	Alcatel	156 P, 238 S, 1 C
1996	D	Hannover	Siemens	800 P+S, 5100 R
1996	D	Schwedt P.K.	Siemens	48 P, 76 S
1997	D	Eppingen	Siemens	18 P, 35 S
1997	D	Hannover S.H.	Siemens	68 P, 28 S
1997	D	Reutlingen	Siemens	18 P, 23 S, 2 C

C = remote controls, L = level crossings, P = points, R = routes, S = signals, T = track circuits

4. Safety and availability concepts

Safety and availability of a railway system are attributes focused on service provision, whose achievement is supported by reliability and maintainability.

For an interlocking system, *availability* is based on knowledge of all possible system failure modes, the probability of occurrence (or the rate of occurrence) of a system failure, causes and effects on system functionality of each failure, an efficient failure detection and location, an efficient restorability of the failed system, a maintenance programme and an efficient direction and control of human factors.

At the same time technical concept of *safety* is closely related to availability, but the severity of the consequences of a failure play a further important role. Consequently, safety concept (and risk as the complement of the probability of safe system functionality) is based on knowledge of all safety-related functions, all possible safety-related system failure modes and their probability of occurrence (or their rate of occurrence), the consequences of a hazardous event or a safety-related failure mode and the probability they will lead to an undesirable event or to an accident, the safety protective measures and the human factor influence on the safe operations.

For an electronic interlocking the sequence of the functional states which can lead to an absence of availability (service disruption) or to an absence of safety (accident) are summarised in figure 4. Hardware and software redundancy configuration and comparison among outputs act in order to allow faults and errors detection and to lead the system again to a regular operation state. The dotted line between service disruption and hazard is a consequence of external factors (in particular human actions) which substitute the interlocking in degraded conditions and can lead to a hazard states when they are not correctly performed. In this sequence reliability and maintainability are related to the minimising and detection of faults, errors and, consequently, failures during the whole system life-cycle.

From a normative point of view CENELEC rule EN 50127 covers the specifications of guided transport systems (GTS); in this framework EN 50126 defines reliability, availability, maintainability, safety (RAMS) and their interaction, a process for managing them, specifying requirements and demonstrating that these requirements are achieved (similar definitions and processes are included in rules IEC 300 and 1508); finally EN 50128 and 50129 deal with safety-related electronic systems, respectively from a software and a hardware point of view.

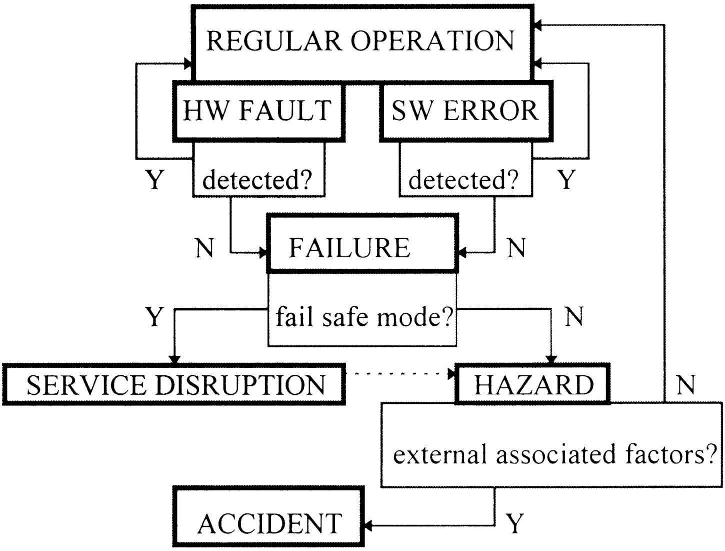

Figure 4: functional states following a hardware fault or a software error

5. Methodological tools for systematic analysis

In order to allow systematic analysis on different interlocking systems and technologies a methodological framework has been built. By means of this it is possible to carry out quantitative (both deterministic and probabilistic) comparisons and evaluations from safety and availability points of view. The basic tool is a matrix scheme, in which the phases of interlocking life-cycle are represented on the rows and the significant events of the functional states sequence on the columns. In table 2 an example referred to the evaluation of safety is shown; a similar scheme (with the same rows and some differences in columns) can be drawn with reference to the evaluation of availability.

Each value P(ij) in a matrix cell represents the risk (probability) of occurrence of the event j during the phase i [for instance P(7A) is the probability of a fault during hardware installation]. By analysing in each column the reciprocal links among phases (for instance some phases can cancel the risks of the previous ones), it is possible to evaluate the global risk for every event. The quantitative analysis shows that for electronic interlocking maximum risk values are related to phases of manufacture (6), installation (7), validation (8), acceptance (9) and maintenance (11).

Table 2: safety evaluation matrix

Life-cycle phases	*A. HW fault*	*B. HW fault detect.*	*C. SW error*	*D. SW error detect.*	*E. Fail unsafe mode*	*F. Ext. assoc. factors*
1. Concept						
2.System definition						
3.Risk analysis						
4.System requirements						
5.Design						
6.Manufacture						
7.Installation						
8.Validation						
9.Acceptance						
10.Operation						
11.Maintenance						

Concept and system definition (life-cycle phases 1 and 2) imply logic structure so that no differences exist between traditional and electronic interlocking system. Risk analysis (life-cycle phase 3) is a widely tested methodology in many application fields (for instance nuclear technology) and no particular problems arise for its application to railway safety systems. System requirements (phase 4) are well defined by CENELEC and IEC rules, while electronic design (phase 5) is today a strongly consolidated technology sector. The operational phase (10) is mostly similar to traditional interlocking too.

Higher values of risk are related to manufacture (life-cycle phase 6), in which production quality-control procedures are involved and a definitive choice between specific and commercial hardware has not been made yet. Installation procedures (phase 7) are at a not normalised state either, while only in the last years some criteria for validation and acceptance (life-cycle phases 8 and 9) of electronic safety systems have been defined at a early stage. Finally maintenance programme (phase 11) can not be planned because of the still restricted number of observations on functioning systems available, not allowing the construction of a well defined rate for faults and errors frequency.

Hardware faults and software errors come mostly from manufacture and installation and they can be minimised by means of an effective maintenance, software errors can be reduced by effective validation and acceptance tools too. The detection of both faults and errors depends on validation, acceptance and maintenance success. The fail-safe mode, as underlined above, is not a peculiarity of electronic interlocking so that the probability of unsafe mode is always fairly high (cause-effect relation are not clearly defined like in relay interlocking). Finally the action of external associated factors is not typical of the interlocking technology but it is related to other surrounding conditions like traffic density, human factors, etc..

6. Systems capacity with different technologies

In the first period of electronic interlocking technology development it has been accompanied by the growth of their capacity: 170 open-line installations in 1980 (Danish stations) became about 844 already in 1989 (Chiasso). Later the research was particularly addressed towards costs reduction with constant capacity and safety levels.

The number of open-line installations, which a system is capable to control, is widely considered the main parameter for the evaluation of the capacity of an interlocking system. A deeper analysis has been carried out in order to consider only the installations controlled by means of safety input-output links. On these basis the present situation regarding the capacity of the main systems available on the market and operating in medium or large plants has been defined.

The results are summarised in table 3. The highest capacity is reached by Siemens and Alcatel systems, widely implemented in Germany, Austria and Switzerland; they are able to be applied for the control of large junctions, comprehensive of a certain number of minor stations. EBILOCK and SSI systems balance the lower capacity with more distributed information flows leading generally to lower realisation costs and higher availability rates in degraded conditions. Westrace and VPI allow the lowest costs by means of the minimisation of processors number (redundant hardware are never foreseen by these systems).

Table 3: capacity of main interlocking systems

Systems	Firms	Controlled Open-line installations (up to)
EL S	Siemens	1000
L90, ELEKTRA	Alcatel	1000
Westrace	Westinghouse,Safetran,Dimetronic	440
VPI	GRS	320
EBILOCK	Adtranz	300
SSI	GEC,Westinghouse	200

References

[1]Rutherford D.B. - L'evoluzione dei sistemi di segnalamento ferroviario - Incontri CESIT, 11.1997

[2]Giger A., Nowak K.H. - Prüfung der Software-Projektierung beim ESTW L90 - Signal+Draht, 10.1997

[3]Maschek U. - Elektronische Stellwerke: ein internationaler Überblick - Signal+Draht, 03.1997

[4]CENELEC - Draft prEN 50126: Railway applications: the specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS) - Bruxelles, 11.1995

[5]Steindl H. - Entwicklung und Einsatz elektronischer Stellwerke bei den ÖBB - Elektrische Bahnen, 08.1989

[6]Bimmermann H. - Mit Mikroelektronik sicher in die Zukunft: moderne Zugsicherungssysteme - ETR, 07-08.1989

[7]Gianinazzi A. - Il nuovo impianto di sicurezza elettronico di Chiasso Viaggiatori - Rivista Tecnica della Svizzera Italiana, 06-08.1989

[8]Walther H., Lennartz K. - Einsatz von Elektronischen Stellwerken bei der Deutschen Bundesbahn - ETR, 11.1985

[9]Savarzeix R., Auclair J.P. - Le poste à commande informatique de la SNCF - Revue Générale des Chemins de Fer, 10.1985

[10]Jonasen A.A., Siggard N. - Microcomputers take over the interlocking function - Railway Gazette International, 12.1981

[11]Okumura I. - Electronic interlocking to be tried in Japan - Railway Gazette International, 12.1980

[12]Berg Von Linde O. - Computers can now perform vital functions safely - Railway Gazette International, 11.1979