Report of a comparative analysis of the Interlocking Systems

“Rapporto di analisi comparata di Sistemi di Interlocking”

Imad Zaza

Attività svolta nel progetto RAISSS: RAILWAY SIGNALLING: SAFETY AND SECURITY

POR CReO FESR 2007 – 2013, LINEA D’INTERVENTO 1.5.a - 1.6, BANDO UNICO R&S ANNO 2012, cofounded by Tuscany region

Referente: Paolo Nesi

Distributed System and Internet Technologies Lab
Distributed Data Intelligence and Technologies Lab
Department of Information Engineering (DINFO)
University of Florence

http://www.disit.dinfo.unifi.it

19/04/2013

Version 1.0

Report of a comparative analysis of the Interlocking Systems

EXECUTIVE SUMMARY

Signaling is the keystone of the railway transportation system and besides it, the interlocking system acts a central role granting the key issues such safety of the overall system.

In order to develop a new Interlocking System, in addition to study the interlocking principles and to have a reasonable background in computer based architecture we have to learn from the state-of-the-art of the existent railways vendor's proposal.

To cover the topic, this report brings together all the main aspects which relate to a choice of ones of the most used Interlocking Systems in Europe.

This include the overall architecture, fault resilience policy, software used to implement the main functions and to interact with railway operators.

Being SIL4 classified systems, they have some commonly features such as:

- the development process have to follow V&V model;
- formal methods to specification, validation, verification is mandatory.

It is also noticed that the interlocking logic – the core issue - is generally an abstract model of the relay circuit due the well-established railway's engineering knowledge. Indeed the main dialect is the ladder diagram or one to one translation from Boolean equation to code.

Conversely some newer systems use the new paradigm of object oriented design which leads to use an object model diagram (and relative tools to generating code) such as Harel's statecharts or proprietary language like ObjRail.

The document is structured in three major section with relative subsections:

- Railways vendor's Interlocking
    - Signaling solutions SSI
    - Siemens (Ex-Invensys) Westrace
    - Invensys Westlock
    - Alstom Smartlock
    - Ansaldo STS Acc
    - AZD Praha Esa 33
    - ECM HRM9
- Other systems
    - Thales Elektra
    - Prorail Movares
    - Bombardier Transportation Ebi-lock
- Final considerations

Moreover the SSI uses a 16 bit cisc cpu and dedicated engineering procedural language that is GDL . Its failure resilience policy is exploited by the Triple Modular Redundancy. The human man interface is implemented by a keyboard and a printer to enter routes or to show status respectively. As it is the one of the first it has a dedicated component to interact with a control panel used with the relay based systems.

The Westrace uses a PowerPC microprocessor and it is developed by the ladder diagram language. Its failure resilience policy is exploited by 2oo2 architecture using diverse programming.

Being further evolution, the system control facilities rely on modern control system facilities as WESTCAD and could use a WESTRONIC for remote signaling control.

The Westlock it is not only a technology advance of the above cited SSI but it also has a fundamental improvement in the architecture that permits to be configurable in decentralized manner.

The Smartlock SML400 is the newer systems of Alstom and in addition to use last microprocessor technologies it is developed via statecharts through commercial IDE such SCADE. Its failure resilience policy is exploited by 2oo3 architecture.

The Ansaldo ACC has the possibility for the zone controller to take over the operational management in the event of failure of the central communication system. Its reliability reaches unprecedented levels, for example by virtue of the support for redundancy 2 of 4.

The ESA 33 system is fully computerized that is compressive of the CTC to the actuator belong to the physical devices. Its failure resilience policy is exploited by 2x2oo2 architecture.

The HRM9 is a new generation system that was engineered by full object oriented design. Its failure resilience policy is exploited by 2oo2 architecture.

Suddenly the information gathered it is not homogenous and this lead to dedicate a separate section for systems which it wasn’t possible to be fully exhaustive.

This is the case of Thales Elektra, Prorail Movares, Bombardier Transportation Ebi-Lock.

Since the lists of the system proposal is time-ordered (from the oldest to the newest), by reading this report it will be noticed the evolution of the intra-components communication by the use of serial links to the Ethernet link of today.

The report ends with some guidelines summarizing the following analysis such that an Interlocking system have to be modularized, expandable and easy to configure by a railway authority point of view meanwhile have to have a high system capacity and a good simulation and maintenance degree by a railway vendor point of view.

Keyword lists

Railway signalization; Interlocking system design; SIL4 systems;

Summary

RAILWAYS VENDOR ‘S INTERLOCKING

It will be proposed the following keys to study the interlocking system which will be described further on:

- System architecture
    - Logistic layer
        - System Control Facilities;
        - Diagnostic Facilities;
    - Functional core layer
        - Central Unit Interlocking and System resilience policy;
    - I/O layer
        - Peripheral Facilities;
    - Intra layer
        - Communication Facilities.

- System software

At a first glance, it will be notice that each vendor has their own terminology of the core part of their system while there is a silent agreement on the other elements like the trackside interfaces or human man interfaces.

Also, newer CBIs like Invensys's Westlock and Alstom's Smartlock use the same trackside hardware, and very-slightly-modified software and data preparation language.

SIGNALLING SOLUTION (EX-WESTINGHOUSE LTD) SSI

The following survey is mainly founded on [1].

Short background

Solid State Interlocking (SSI) was one of the first microprocessor based system, designed for use in railway signaling installations to compute and execute the signaling interlocking functions.

It will be discussed here for historical reasons and because some equipment's terms it is used in other systems. Despite the fact that it was introduced officially in 1985 at Leamington Station, some installations are still under use in some countries.

The development of SSI was undertaken jointly by British Rail, GEC Genera1 Signal Company Limited and Westinghouse Signals LTD in the United Kingdom.

British Rail has been responsible for the basic design of hardware and software, safety validation (manually executed by signal engineers) and for overall project management, GEC and Westinghouse Signals have translated the British Rail design concepts into fully engineered production equipment.

The interlocking is centralized in a single housing with true distribution of its i/o made possible by the provision of a data link and standard, nonprogrammable, slave object controllers.

The application of SSI to the existence railways (based on relay) was very flexible due the fact that SSI could be interfaced to conventional control panels or to VDU(Visual display Unit), line side signals and paints remained as before, the signaling principles of interlocking requirements of different railway authorities could be totally performed by SSI.

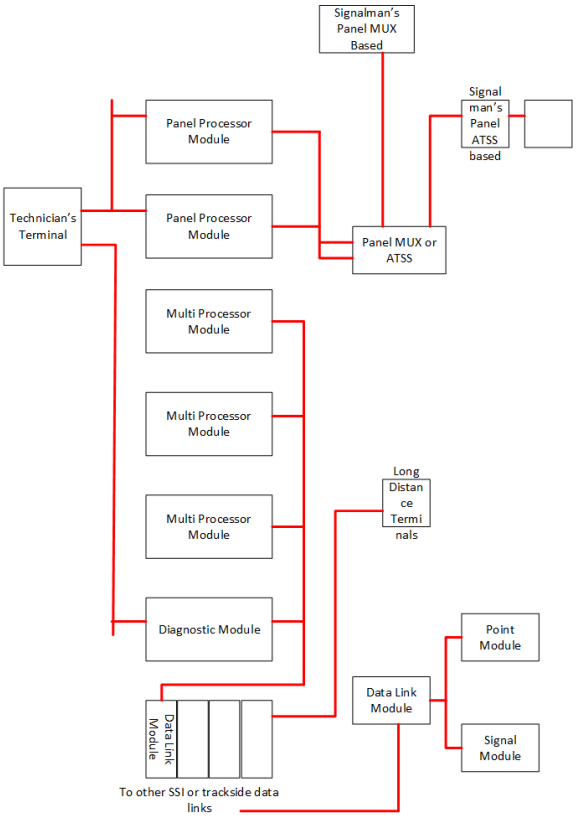
System architecture

From the above cited paper it is possibly to identify clearly the elements in the three layers:

- at the logistic layer it will be found the technician terminal and signalman's panel that could be of two type depends of the panel ones (MUX or Automatic Train Supervision System);

- at the functional core layer it will be found the central interlocking which contains:
    - two panel processor modules for communicating with the operator interface system (e.g. panel multiplexer, control panel);
    - three interlocking processors;
    - one diagnostic multi-processor modules;
    - two external data link modules for communicating with the trackside equipment;
    - If required, two internal data link modules for communicating with other SSI central interlockings in the same room.

- At the I/O layer it will be found the trackside equipment which interfaces with railway objects.



System Control Facilities

The panel processor modules perform the functions associated with the operator controls and indications. The panel processor modules are duplicated for availability and communicate over serial data links with the operator interface system which can be a panel multiplexer for interfacing to a control panel or a sophisticated control system.

The technician's terminal comprises a printer, keyboard, dedicated computer, tape cassette data recorder and modem. The technician's terminal receives information from both panel processor modules and the diagnostic multi-processor module of up to six central interlockings. It uses this information to print the status of the central interlockings connected to it. The keyboard is used to interrogate the system for specific status information and to apply route, and aspect barring etc.

The tape cassette data recorder logs all changes of state within the system providing a record of operation while the modem is for connecting a remote keyboard and printer to the technician's terminal.

The panel multiplex is used when a parallel interface to the operator control system is required such a control panel. The panel multiplexer is a duplicated system for high availability and communicates via a serial data link with the panel processor modules. Operator controls are received in a parallel form, the multiplexer converts them into a serial message and send it to the panel processor module. Operator indications are transmitted on a serial message by the panel processor module to the panel multiplexer, the panel multiplexer converts this information into a parallel form suitable for driving indication lamps or LED'S.

Diagnostic facilities

Diagnostic multi-processor module listens to the transmissions on the external and internal data links to detect faults with the interlocking multi-processor modules, the external data links or the trackside function modules connected to the data links.

This diagnostic information is then passed on the technician terminal. The external and internal data link modules convert the electrical characteristics of the data link transmissions used by the interlocking multi- processor modules to a level suitable for use external to the central interlocking cubicle.

Central Unit Interlocking and system fault resilience

The Motorola 6800 microprocessors used in SSI have a 16-bit address space:

- 60–80k bytes are EPROM which hold the generic program (about 20k bytes), and the Geographic Data;
- 2k bytes are RAM
- The rest is used for input and output devices.

The modest RAM is used, mainly, to hold the system's record of the state of the railway—generally referred to as the image of the railway, or the internal state in the sequel.

Alstom, also, developed a 'Turbo' upgrade for SSI. 'Turbo' SSI features a processor that operates at twice the speed of conventional SSI. The faster processor delivers twice as much data processing in the same elapsed time as 1MHz SSI interlockings. In addition, 'Turbo' SSI enables support for a greater number of trackside functional modules (TFMs).

The safety interlocking functions are performed by the three interlocking multiprocessor modules configured as a triplicated redundant systems.

Each subsystem is identical, and runs identical software. All outputs are voted upon, redundantly in each interlocking processor, and the system is designed so that a module will be disconnected in the event of a majority vote against it (i.e. due a failure), SSI will continue to operate as long as the outputs of the remaining modules are in agreement.

The output of the interlocking multiprocessor modules consist of command telegrams transmitted to the trackside data links from two of the communication processors in each multi-processor module.

The interlocking multi-processor module takes turn to transmit one telegram each, although each interlocking multiprocessor module calculates the content of every telegram. For each telegram the two non-transmitting multi-processor modules listen to the outgoing message, checking the validity of each bit as it is sent, and either multi-processor module can inhibit the data links immediately in the event of disagreement.

The changes of configuration from triple to double to triple are achieved without any degradation in system operation.

The operator and train driver are unaware that there has been a change in system configuration.

Failure of two interlocking multi-processor modules would result in a controlled and safe shutdown of that central interlocking, as this failure would remove any safety redundancy to protect against error developing in the third multi-processor module.

Peripheral facilities

The SSI trackside equipment is composed by:

- Signal Trackside Function Module;
- Point Trackside Function Module;
- Data link module.

The trackside equipment is designed to be mounted in location cases adjacent to the trackside. Each trackside function module uses two microprocessors configured as a duplicated redundant sub- system thus if there is a disagreement between the two microprocessors the trackside function machine shuts down in a controlled and safe manner.

The signal trackside function module is primarily for use when driving signals but it can be used for other applications. It has eight outputs, two current sensing inputs and six contact sensing inputs.

The signal trackside function module outputs de-energize when the signal trackside function module shuts down but two of these outputs can be independently programmed using wire links in the trackside function module lug coupler to the "red retaining".

These outputs then energize when the trackside function module shuts down and are used for the red signal aspect. Two of the other outputs can also be programmed to flash and this is used when a signal requires a flashing aspect. The two current sensing inputs are used for lamp proving the signals driven by the signal trackside function module. The six contact sensing inputs require voltage free contact s of the functions to be monitored as a special coded signal generated by the trackside function module is fed via the voltage free contacts to the inputs**.** The signal trackside function module receives commands from its associated central interlocking, via the external data links, to switch ON or OFF each of its outputs. The signal trackside function module immediately sends a reply telegram containing the state of its inputs and status of itself.

The point trackside function module has been designed to interface directly to the British Rail clamp lock point machine. If other types of point machines are to be driven then suitable interface relays/contactors may be used between the point trackside function module and point machine. The point trackside function module has two normal valve outputs, two reverse valve outputs and four pump motor outputs, and can drive up to two independent sets of points. The point trackside function module has four point detectors contact input s and four contact sensing inputs. All inputs require voltage free contacts of the functions to be monitored as per the signal trackside function module. The point trackside function module is designed to de-energize its valve/pump motor outputs when the relevant point detection is made, also, an out feature is provided to cut off the drive to the vale/pump motor outputs if the point detection fails to make within a predetermined time.

Communication facilities

The data link modules convert the electrical characteristics of (data link) transmission used by the trackside function modules to the level of external data links.

Each data link module can drive six trackside function modules and two are required, one for each data link.

The internal and external data links are duplicated for availability. If both external data links fail, the trackside function modules connected to those data links will shut down is controlled and safe manner, i.e. all red retaining outputs energized and all other outputs de-energized. The external data links can extend to 10km without amplification and can extend to a maximum of 40 km with amplification. Amplification is performed by connecting two data link modules back to back on each data link at each amplification point. The consistency of the data transmission is ensured in AC and DC traction areas due to the use of the following techniques:

- Hamming Coding
- Manchester Coding
- Message Protocol
- Date Rate
- Electrical characteristics of data link transmissions.

System software

The software, developed in the Geographic Data Language (GDL), of the panel processor module is designed to receive commands from the operator interface system, convert them into suitable messages for the interlocking multi-processor modules and then pass the messages to the latter at the appropriate time and to deduce the correct state of the route, track, points detection etc. and send this information to the operator interface system.

The safety software employed in the interlocking processors is sub-divided into programs providing initialization, redundancy management (i.e. performing hardware safety checks ad comparisons, implement safety and availability strategies), interfacing with panel processors and communications links, data transmission and reception, and computing the interlocking functions.

SSI has been designed to be data-driven with a generic program operating on rules held in a ‘geographic’ database. These data configure each SSI installation differently, and define the specific interlocking functions (although the more primitive functions are directly supported by the software). The relationship between generic program and the data is one in which the former acts as an interpreter for the latter.

The software in each central interlocking is designed to support maximum of 63 trackside function modules, 128 signals, 64 sets of points, 256 track circuits and 256 routes. Also, the maximum number of central interlockings that can communicate with each other via an internal data is 30.

All SSI software is organized on a cyclic basis with the major cycle determining the rate at which trackside equipment receive fresh commands, and the rate at which the image of the railway is updated.

A maximum of 63 TFMs can be connected to one SSI, and the major cycle is consequently divided into 64 minor cycles. In the zeroth cycle data are exchanged with the diagnostic processor.

During one minor cycle the generic program:

1. performs all redundancy management, self-test and error recovery procedures;
2. updates system (software) timers and exchanges data with external devices such as panel processors;
3. decodes one incoming data telegram and processes an associated block of Geographic Data;
4. Processes the data associated with one outgoing command telegram.

The latter phase is the most computational intensive part of the standard minor cycle because it is through these data that the Interlocking calculates the correct signal aspects.

The SSI minor cycle has a minimum duration of 9.5 ms, and a minimum major cycle time of 608 ms However, SSI can operate reliably with a major cycle of up to 1,000 ms, with an individual minor cycle extensible to 30ms.

This flexibility is needed for handling panel requests. If the required minor cycle processes mentioned above can be completed in under the minimum minor cycle time, the control interpreter will process one of any pending panel requests (which are stored in a ring buffer). The data associated with a panel request must not require more than a further 20 ms of processing time—the data are structured such that accurate timing predictions can be made at compile time. If the minor cycle is too long the trackside functional modules will interpret the gaps between messages as data link faults, and will drive the equipment to the safe state in error.

The initialization software compares the internal state of each of the three interlocking processors to determine the required start up procedure. When power is first applied a *'mode 1' startup* is necessary: this sets the internal state to a (designated) safe configuration, forces all output telegrams to drive the track-side equipment to the safe state and disables processing of panel requests; after a suitable delay so that TFM inputs can bring the internal state up to date, the Interlocking can be enabled under supervision from the technician's console.

After a short power failure much of the contents of RAM will have been preserved and a 'mode 2' or 'mode 3' start up is appropriate. A 'mode 2' start up resets the internal state to the safe configuration but preserves any restrictions that had been applied through the technician's console—the system is disabled for a period long enough for all trains to come to a halt, and allowed to restart normal operation automatically. A 'mode 3' start up involves a similar reset but the status of routes is also preserved, and the system restarts immediately.

SIEMENS (EX-INVENSYS) WESTRACE SSI

The following survey is mainly founded on [2].

Short background

Westrace solid state signaling system is an on-going development of vital processor based equipment. The last model is Westrace MK2 (four times capable than the original Invensys ones) and is nowadays commercialized by Siemens as Trackguard Westrace Mk2.

System architecture

From the above cited paper it is possibly to identify clearly the elements in the three layers:

- at the logistic layer it will be found the WESTRONIC S2 interface;
- at the functional core layer it will be found Processor Module (PM), Vital Logic Equipment (VLE) and Diagnostic Module (DM);
- at the I/O layer it will be found up to 128 Input/output Modules (IOMs).

System Control Facilities

The following survey is manly founded on [3].

The interface between the operator via WESTCAD and the system is granted by WESTRONIC S2 interface.

As all ex Invensys (relatively new) products generally it is used MoviolaW as Human machine interface.

MoviolaW is a PC-based tool that provide real time and replay graphical displays of the system status, showing track circuits, points, signals and other equipment, so that the interlocking status at any given time can be easily understood.

The on-site MoviolaW automatically records every system input, output and internal change, using a high capacity log on the PC's hard disk.

Internal logic states can be examined in detail and changes of state monitored. Users can switch between real time and replay, to identify critical events and investigate incidents. MoviolaW can be played forwards or backwards, with plain text messages to help identify failures of trackside equipment, such as signal lamps and point detection.

Authorized engineers can have password-protected access via modem or WAN, to quickly diagnose problems from remote locations. MoviolaW has a Microsoft Windows ™ based interface and can be designed and edited with the same PCGE (PC Graphic Editor) tool used for WESTCAD.

Diagnostic facilities

In the first release there were a separate Diagnostic Modules that provided a non-intrusive interface to the Vital Modules, for fault diagnosis and event recording, and also ensure that the correct data has been downloaded to the system. The Diagnostic Module could be interrogated locally or over a modem link, giving the maintainer quick and easy access to system status information.

With the introduction of WNCM (described furthered on) diagnostic information can be accessed via both the network and serial interfaces, so a separate diagnostic module is no longer required.

Central Unit Interlocking and system fault resilience

Each PM comprises three interconnected PowerPC microprocessors - two form the processing core, performing the interlocking logic and cross-checking each other, whilst the third executes diagnostics and network communications functions.

It can also be operated in Hot or Cold Standby modes, with high speed optical links connecting adjacent sets of interlocking equipment, to provide a seamless transfer of control.

All of the modules incorporate ‘2 out of 2' architecture and have full compliance with CENELEC SIL4.

The Mk2 achieves its safety by diversity. Its fail-safe design uses two distinctly different methods to ensure correct functioning, with a health monitoring arrangement where the operation of each processor is checked by at least two other processors.

Each WESTRACE produces two drive signals. The first is to the Output Power Control Relay (OPCR), which switches all the outputs. If an output becomes unsafe, WESTRACE de-energizes the OPCR, all output drives are removed and (if necessary) all signal aspects return to red. The second drive signal enables the vital serial communications. If WESTRACE de-energizes this drive signal, all vital serial communications stop.

For the OPCR and the vital serial drive signals to be energized, WESTRACE’s Primary and Secondary Negation signals must be present. Primary Negation monitors the information passed between all the vital modules in an installation; it occurs if the central processor fails to operate, operates but determines that it has an internal failure or if it fails to exchange messages with a vital module, e.g. a vital module determines that it has an internal fault, and shuts itself down. Secondary Negation works differently, using bi-directional Health Monitoring links between adjacent vital modules.

Using these links, each module can check that the adjacent module’s microprocessor and timing reference are working. If a vital module detects a fault, it disables the Secondary Negation signal and stops communicating with its adjacent modules over the Health Monitoring link. As one module shuts down, all the other modules detect that the adjacent module has failed and consequently shut themselves down too. This means that Secondary Negation does not depend on a single module disabling the Secondary Negation signal.

Peripheral facilities

Devices known as Object Controllers (OC) provide the interfacing between the WESTRACE Input/output Modules and the trackside ‘objects' such as point machines, signals, track circuits and axle-counters. The OC concept is again modular, using basically the same core components as the interlocking itself. Each OC contains common components with direct connection with the objects.

Communication facilities

The vital processor systems are built up from a range of compatible modules which all communicate over a common parallel bus.

Conversely each interlocking system can be networked using standard Ethernet systems, to provide conveniently scalable versatility, with reliability and safety.

Since the first system it has introduced of a new vital logic module, the WESTRACE Networked Communication Module (WNCM).

The WNCM consists of:

- the VLM6 module, providing conventional vital logic module functionality;
- Network Communication Diagnostic Module (NCDM).

The VLM6 not only supports a larger number of logic rungs but, importantly, allows the use of the NCDM, which has one TCP/IP network interface and two further serial interfaces for vital and non-vital communications.

Another benefit of the NCDM is that it can accommodate up to 15,000 rungs of non-vital logic, freeing up vital processing space within the VLM6 module.

System software

WESTRACE is programmed in Ladder Logic, using PC based GCSS (Graphical Configuration Sub System) software, which allows signal engineers to easily enter, check and test each application in the office, before installation on-site.

In [4] carried out work for Invensys, applying various SAT and model checking techniques to verify the correctness of a simple pelican crossing and two existing railway interlockings consisting of approximately 500 rungs [4] .

In [5], in particular his translation from ladder logic into propositional logic, and applied several model checking techniques in order to try and reduce the complexity of the problems. The relationship between a ladder logic program and propositional logic was discussed in great detail. A method for formulating such a ladder logic program as a formula in propositional logic was presented. This laid the ground work for all successive projects involving ladder logic.

As its programming logic is analogous to free-wired relay interlockings, this lead to ideally suitable for upgrades of existing systems.

The GCSS software has two main editors:

- Housing editor;
- Ladder editor.

The Housing Editor is used to select which modules will be configured in which physical locations in the housing rack. The Ladder Editor then allows the Ladder Logic to be entered. By default this uses a Ladder Logic view, but it can also display relay based representations which may be more familiar to some engineers. The software also enables access to certain system functions, allowing the engineer to instigate actions, such as a reboot or testing the Output Power Control Relay (OPCR). There are also between 200 and 300 internal timers (depending on the module), which behave in a similar way to relay timers.

INVENSYS WESTINGHOUSE WESTLOCK

The following survey is mainly founded on [6] , [7] .

Short background

WESTLOCK is a fourth-generation SSI interlocking that functions just like SSI and adds the major benefits of system capacity, availability and support tools.

It can use existing SSI application data and can combine data from multiple SSIs to eliminate cross-boundary, performance-constraining constructs. High-speed processing achieves fast object response and minimal route-setting time.

The CIP has a processor that is 25 times faster than the SSI turbo MPMs it replaces in terms of CPU speed alone.

It is uses Ethernet based communications for both vital and non-vital networks (which are each duplicated for availability.

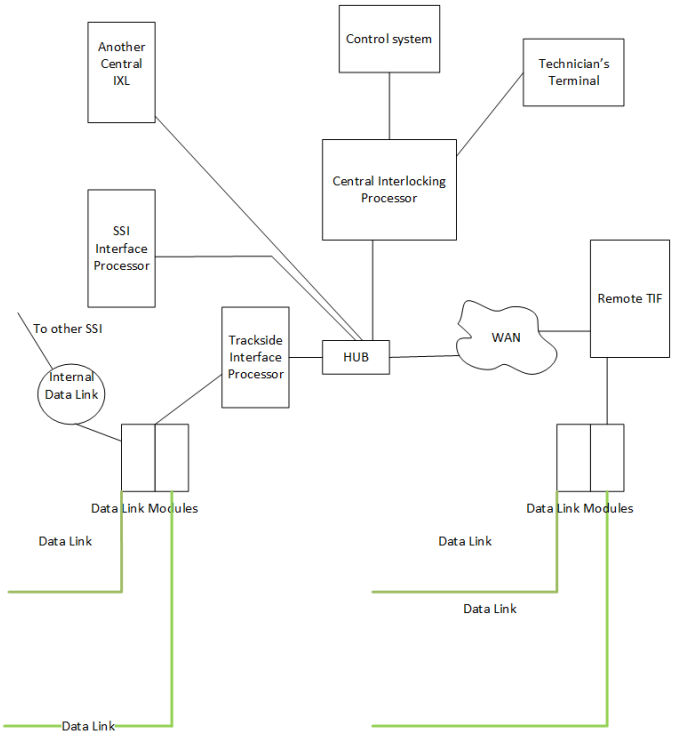
Unlike SSI there is also the ability to have a separate, vital, serial network link into the interlocking; this means that it could be connected to a Radio Block Centre (RBC) without the need for any additional equipment. This is something which is just not possible with SSI.

The SIL2 components of the WESTLOCK system (the CSG and TW (L)) are based on industrialized COTS PC equipment to ensure a future, supported source of hardware and to keep the equipment as cost effective as possible.

System architecture

From the above cited paper it is possibly to identify clearly the elements in the three layers:

- at the logistic layer it will be found a technician’s workstation and a pair of dual redundant Control System Gateways (CSGs);
- at the functional core layer it will be found the Central Interlocking Processor (CIP);
- at the I/O layer it will be found a Trackside Interface Function (TIF) for each Trackside Data Link (TDL) and a processor to communicate with the SSI data link.



System Control Facilities

The WESTLOCK technician's terminal is based on a Windows XP embedded operating system and runs on COTS industrialized hardware, thereby reducing costs and ensuring future hardware availability.

A new data preparation system is complemented by a new Simulator, and SSI experts will quickly benefit from the intuitive, automated features.

A similar interface is used for the Technician's Workstation, which now supports mnemonic names as well as numeric identification.

The graphical, multi-window interface shows a real-time track diagram and a fault log, and accesses all SSI interlocking, telemetry and TFM states displaying mnemonics. All data is logged and comprehensive replay using all workstation facilities aids incident investigation. Remote Technician's Workstations, with viewing facilities only, assist remote support.

Diagnostic facilities

Being an evolution of the SSI, it share the same diagnostic equipment discussed earlier.

Central Unit Interlocking and system fault resilience policy

The CIP consists of 3 main processor modules which perform the safety-critical interlocking functionality.

This system exploits the Trident Triple Modular Redundant modules that have been proven in the safety industrial protection (hydrocarbon processing, nuclear, etc.) environment where safety is a given and reliability is everything.

All modules are fully hot-swappable. Any single failure cannot impact on operation, and can be repaired with zero impact on train operation. Separate hardware is used for the Central Interlocking Processor (CIP), the safety brain that controls the railway, the Trackside Interface Processor (TIF) that controls the data links, and the SSI Interface (SIF) processor that talks to other SSIs.

The safety software—fully validated to Safety Integrity Level 4 (SIL 4)—uses two fully independent diverse processes within each vital module.

Even the application data is compiled diversely, to separate constructs for each safety process.

This system fully meets the SIL 4 industry standards of CENELEC (EN 50126, 8 & 9) and IEC 61508. The Tools a whole new suite of graphical tools makes design so much easier while retaining the flexibility and efficiency of the SSI data constructs.

The vital hardware used for the CIP and the TIF is a worldwide established product from the process control industry. It had been designed to meet SIL3 standards for high availability, with all modules being at least duplicated for redundancy. This means it came ‘readymade’ with hot-swap, hot-learn capability which allowed a massive step.

Up from SSI in terms of maintainability. A dual path, true and complement processing program architecture was introduced to allow the step up to full safety critical SIL4 rating as required by most railways now days.

Peripheral facilities

It can have multiple Trackside Interface (TIF) processors, each separately controlling a data link. The TIF is controlled by similar triple modular redundant processors as the CIP with a special triple modular redundant module for driving the SSI Data Link Modules.

Moreover it controls the railway using SSI Trackside Functional Modules (TFMs) connected to a SSI Trackside Data Link (TDL).

SSI TDLs use a relatively simple and now certainly considered slow, protocol. However the processing required driving such a vital link is intensive enough that it uses separate Trident systems to drive each data link.

These are separate from the CIP and are solely responsible for driving and monitoring the data link. These units are called the WESTLOCK Trackside Interfaces (TIF) s.

As the TIFs emulate how an SSI interlocking drives the data link, any existing SSI data link can be reused with it. This means all the existing DLMs and TFMs of an SSI installation could be retained and did not need to be modified at all.

Communication facilities

The dual-redundant Ethernet interface between the TIF and CIP are ideal for decentralization, and only require an industry-standard Ethernet link over any (and probably diverse) bearers between the two.

SSI Interface WESTLOCK uses an SSI Interface (SIF) processor to communicate with legacy SSI systems.

The SIF uses similar hardware and is also connected using redundant Ethernet links. Technician's Workstation A new PC-based Technician's Workstation uses dual Ethernet connections to the CIP.

This system has the ability to communicate to control centers using two different protocols.

The first option is the BR1921A protocol which is typically used to communicate with Panel MUltipleXers (PMUXs) on NX panels.

The second option is the protocol most commonly used by British Rail's Integrated Electronic Control Centre (IECC), BR1631, which is now known as the 17503 protocol.

System software

As the Westrace system, the IXL logic is programmed as Ladder Diagram with the MoviolaW human machine interface.

ALSTOM SMARTLOK SML400

The following survey is mainly founded on [8].

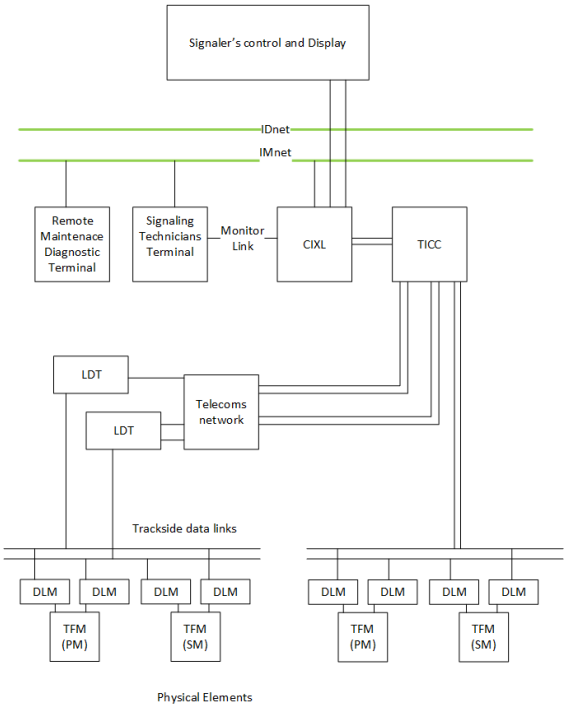
Short background

The Alstom Transport group supplies a family of interlocking systems, known as SMARTLOCK.

System architecture

From the above cited paper it is possibly to identify clearly the elements in the three layers:

- at the logistic layer it will be found the Support System Cubicle (SSC);
- at the functional core layer it will be found the Central Interlocking (CIXL);
- At the I/O layer it will be found the Trackside Interface Communications Cubicle (TICC).



System Control Facilities

The Support System is composed of a Support System Cubicle (SSC), one or more user interface PCs (client PCs) and printers. In addition to the local clients, a remote maintainer facility is available with connection via a Wide Area Network (WAN) using ISP ADSL links for example.

It provides all the necessary information and controls required by the Maintainer and Signaling Technician for monitoring and managing the signaling system during maintenance activities.

The support system is based on client/server architecture. The main elements of the support system are as follows:

- Redundant support system servers (support server A and B)
- Local support system client
- Time source
- Printer
- Remote client

The Support System employs a dual redundant configuration of the Support System's servers (SSer's).
In common with other parts of the SML400 system, this dual-redundant configuration provides a system tolerant to first failures.

The Support System includes at least one dedicated workstation for the Maintainer and Signaling Technician with a screen, keyboard, mouse and printer for one or more CIXLs.

Other workstation PCs may be distributed around the signaling control center as required.

A Local Client PC, mounted in the SSC, provides a user interface for the maintainer/technician to graphically view the state of the system and the equipment under its control. It is also the point of entry for the application and removal of technician controls.

It communicates via a LAN connection to one of the support servers, but automatically switches to the other if this connection is lost. Where remote client terminals are provided to allow distant maintainers to view the system via a WAN link, the remote users log into the client gateway via Windows TM terminal services.

The local client is a Commercial off the Shelf (COTS) rack mounted industrial computer. It is contained in a 2U high rack mount chassis. If remote maintainer access is provided, then this is replaced by the externally similar client gateway.

The signaling Technician provides:

- Interlocking mode control: Allows the technician to change the operating mode of the CIXL and individual VIXLs including starting/stopping.
- Temporary controls: Provides commands for the technician to impose or remove temporary controls on the operation of the interlocking. Owing to potentially serious consequences of the incorrect setting and, in particular, removal of controls, the mechanism by which the commands are issued is managed to an appropriate Safety Integrity Level (SIL).

An external clock is provided to allow synchronization of time across the various servers and clients within the Support System, such that time stamps applied to logged events are against a consistent time frame linked to a common source that is synchronized to national time.

Diagnostic facilities

The support system provides also diagnostic as follows:

- Monitoring: Provides text and graphical information on the state of different elements of the interlocking such as the CIXL, trackside objects, communications equipment and links.
- Alarm Management: Performs fault diagnosis and provides text and graphical information on faults and important events detected by the system.
- Event Log Management: Logs and stores all events in the exact order of their detection and provides access to historical data.
- User Access Management: Controls user access to the different functions of the support system.

In addition to the local clients, a remote maintainer facility is available with connection via a WAN. Such remote terminals have the same operator interface as a local version, but without the facility to apply and remove Technician Controls.

Each support server logs all system activity on a pair of logging devices, one of which may be removed for analysis offline in case of incident/accident investigation.
Data logs may also be transferred to offline facilities for analysis via USB flash drives.

Central Unit Interlocking

The CIXL is at the heart of the SML400 and is based on Alstom's "2 out of 3 Platform". The CIXL manages the interface with either type of Traffic Control System (TCS) used in the UK that is it provides direct interfaces to Panel Multiplexers (PMUXs) required by an NX panel, and/or direct interfaces to an IECC, MCS – or similar system supporting the same interface.

This is a general-purpose safe computation system for railway signaling and control applications.

The CIXL contains interlocking memory that records the current state of the railway under its control; this includes functions such as signal lamp proving, point detection and track section occupancy. It also stores internal interlocking variables such as approach locking and timing functions.

The interlocking memory states are referenced by the signaling logic to determine when and which controls may be sent to the trackside devices: point movements and signal aspects etc. as determined by changes of input states from the trackside, or requests made by the signaler.

The CIXL contains the following components:

- I/O subsystem (one out of two architecture);
- Computing subsystem (This includes three redundant channels which implement the 2oo3 architecture);

As with SSI, only 2 of the 3 safe computing channels need to be operational for the system to continue in operation, a failed channel can be replaced without taking the system off-line.

In the event of internal failure the CIXL can change seamlessly, and without any required intervention by operators, to 2 out of 2 (2002) operation (whilst at the same time isolating the failed module).

An “Emergency Signals on Control” feature is provided by a circuit that, when the signaler presses a button dedicated to a specific area of control, removes power (both A and B supplies) from the CIXL and all TICCs used to control the data links in that area. As with an SSI ESOC circuit, a timer relay ensures that, once pressed, the power is removed for a minimum of 15 seconds, regardless of how quickly the button is released.

This ensures that the affected CIXL and sub-systems within the TICCs are all subject to a restart.

In the absence of controls from the Central Interlocking, all TFMs will assume the “red retained” state, and display their “most restrictive” aspects. Points will remain locked in their current positions. The subsystems in the TICC take approximately 10 seconds to recover once power is restored, but the CIXL takes between 2 and 3 minutes to restart, but then enters a 4 minute timeout to ensure that all trains that may have previously observed clear signal aspects have come to a stand. During this timeout period, signals will be sent controls for their most restrictive aspects and points will not be controlled by the Central Interlocking, hence remain locked in their current positions.
However in [9] it is described some features of the diverse process development of two Smartlock –referred as system A and System B- and also formally specified with Vienna development Model.

The interlocking logic is represented differently for each system. In system a, processes logic is expressed as Boolean equations, which are generated using a rule-based tool while the logic for the system B, takes the form of compiled procedural code.

The design of the logic generator tool was commissioned nearly twenty years ago to the University of Bologna by the SASIB Railway Group in Bologna (which later became Alstom Ferroviaria S.P.A.), as part of a research project to investigate the use of rule-based techniques for interlocking data configuration. An early prototype of the tool was produced in the late 1980s using Quintus Prolog. The Prolog program was developed further within the Alstom group in the early 1990s, and has evolved over time to its current state. The program has been used since on numerous interlocking applications for different operating companies.

The program inputs files containing a given interlocking logic schema and files containing Prolog facts denoting the properties and layout of a given signaling area.

In the early years, the logic was validated by manual inspection of the Boolean equations output.

This practice, being time consuming and error prone, could not be sustained in the long term, especially with the increasing size and complexity of the new interlocking applications to come, and so new validation approaches were evaluated, and, in 2001, a decision was made to develop a diverse logic generator.

The second tool was to be developed independently from the first tool, using a different team and alternative techniques and tools as suggested in CENELEC.

Given that the only documentation on the first tool, available at the time when the second tool was conceived, consisted of a user manual and the Prolog program itself, in order to understand the nature of the schema meta-language and how it was to be interpreted, it was considered necessary to begin the development with a precise specification written in a suitable notation, for which VDM++ was chosen.

The main purpose of the specification was to:

- construct a model of the circuit diagrams used to describe the interlocking logic;
- formalize the conversion rules used to generate Boolean equations from the logic;
- construct a model of the schema definitions embodying the templates and rules
  Used to construct the interlocking logic;
- Formalize the reasoning mechanisms used to apply the schema to the facts.

So as not to be influenced by the design of the first tool, the specification of the second tool was created from first principles (based on prior knowledge of formal logic and rule-based systems), using the first tool as a black box in order to analyze the required behavior, by observing its results when applied to example scenarios.

Although the formal specification was used initially as an aid to understanding the requirements, in the end, it served as an alternative representation of the metalanguage.

The System B interlocking system has been developed in recent years to replace the Solid-state interlocking system (SSI).

Using the same design as SSI, the System B system interprets binary code representing the interlocking logic. The code is interpreted on the contents of reserved areas of memories used to record the states of the signaling functions controlled by the interlocking.

Iterating in cycles, the interlocking receives indications of the current states of the signaling functions, updates the memories accordingly as the logic demands, and sends commands to control the signaling functions to their new states.

The interlocking logic is defined using a procedural, object-centered language, introduced in [10] is a rigorous approach to capture functional requirements of classical planning domains , which has been designed to be backwards compatible with the language used for configuring SSI applications.

The logic is organized into blocks of code containing tests and commands that access the signaling object memories, which are combined together in conditions and statements, using typical imperative language constructs, to be evaluated and executed by the interlocking.

The logic is prepared as source code. The source code syntax of the memory tests and commands uses mnemonics oriented to signaling engineers.

The source code is compiled to Motorola S3 object code, which is programmed on a memory device to be installed on the interlocking system.

Following the design of SSI, the object code instructions are derived directly from the source code syntax.

Because Alstom has no access to definitive reference material on the SSI language, and because the language was to be extended to exploit features provided by the new interlocking system, a decision was made to formally specify the new language, in order to understand its semantics, i.e. how it is interpreted by the interlocking, and, as a result, clarify its syntax. The formal specification was constructed in VDM++, based on a formal model created previously using the Fusion notation.

As with SSI, it is assumed that the System B object code is generated using a compilation system approved at a SIL4 safety integrity level. SSI ensures this level by using compiler and decompiler tools. For System B, this proved inadequate, owing to the difficulty of decompiling back to the pre-translated source code. Instead, it was

Considered necessary to compile and decompile to an intermediate representation of the logic, for which the abstract syntax of the formal specification proved ideal.

Peripheral facilities

The Trackside Functional Module Gateway (TFMGW) Subsystem provides the functional interface between the CIXL and the TFM through the TFM Network.

Trackside Functional Modules (TFMs) are the local interface with vital signaling equipment at the trackside. These are the same modules that are employed by SSI. Two types are currently in use in the UK as follows:

- Signal Module (SM) which is designed to provide the power interface with color-light signals, and is sufficiently flexible to handle other signaling loads as well. It provides inputs for current proving and for general purpose signaling inputs such as track circuits.

- Points Module (PM) which forms the power interface for direct drive of clamp lock type point motors. Other types of point machine such as the Alstom Type HW are driven via interface relays. The PM provides inputs for point detection and general purpose signaling inputs such as track circuits.

Moreover, the TFMGWs, formed by the combination of the Front Ends (FEs) and Gateways (GWs) provide the interface between the CIXL and the communications modules (DLMs or LDTs) providing the Trackside Data Links (TDLs).

They are responsible for managing communication, via the TDLs, with the TFMs on their networks (including setting the cycle time and dealing with any reply messages that might be missing because of a TFM failure, noise, damaged cable etc.).

Separate GWs are provided for the ‘A’ and ‘B’ TDLs. Normally, both links are in operation but a TFM will respond if it receives a telegram on one link only. The TFM sends its reply messages simultaneously on both ‘A’ and ‘B’ networks.

Each TDL (same of SSI ones) communicates with up to 63 TFMs and can employ Data Link Modules (DLM) to provide baseband links between the interlocking and the trackside part of the link, or they can use a Long Line Link (LLL) as provided by LDTs over a telecommunications interface.

The only difference, when compared to an SSI data link, is that a Smartlock system has the capacity to drive every TFM in a fully loaded interlocking, whereas SSI interlockings are typically limited to 55 of the theoretical limit of 63 to avoid breaching the SSI’s capacity limit.

Two levels of coding protect the information sent on the data links. They are also fully duplicated for high availability with separate ‘A’ and ‘B’ links.

The baseband link uses a dedicated twisted pair cable over which data is transmitted in half-duplex mode at a rate of 20 Kbits/s by the DLMs. Separate cables are provided for the ‘A’ and ‘B’ links and they can, if required, be run over different physical routes in order to increase availability. The maximum length of the baseband link, including any spur up to 1 km in length, is 10 km (but it can be extended to 40 km by using repeaters at intervals of up to 8 km).

Communication facilities

The support system's servers are linked to the CIXLs by the Internal Maintenance Network (IMNet); a pair of redundant networks that link:

- the CIXL to the support servers
- The clients, printers and the NTP time source to the servers.

The redundant networks are linked together at the central switches to allow the two support servers to communicate.
WAN links may be provided to allow clients at remote locations to access the system but with restricted functionality.

A separate network may be used to link remote clients to "local" client (nominated as a client gateway) using Windows TM terminal services software.

A version of the Support System Cubicle also includes switches for an independent duplicated LAN to allow multiple CIXLs to pass safety related data between each other.

In addition to the diagnostic information received via the IMNet, each CIXL Extended Adaptation Unit (XAU) is connected to the support system servers via a synchronous serial RS-422 Monitor Link.
This link enables 'snooping' to be performed by the support system on the trackside communication data passing between the CIXL and TFMGW. This information is logged and incorporated into the live databases on the support servers.

The TICC houses the equipment responsible for:

- Managing the external trackside communications networks
- The protocol for communication with TFMs.

There will generally be 1 or 2 TICCs per CIXL, depending on the number of Trackside Data Links (TDLs) required; however, this can vary depending on the overall size of any given system.

A TICC can support 2 or 4 data link pairs, depending on the model used. The TICC contains pairs of Gateways (GWs) and their associated Front Ends (FEs), together forming what are referred to as TFM Gateways (TFMGWs). The FEs handles the interface between the CIXL cubicle and the GWs and conduct the polling as the bus master, whilst the GWs act as protocol converters.

The FEs is fully duplicated internally with normal and reserve cassettes. The TICC also contains a pair of SSI communications modules (either Data Link Modules (DLMs) or Long Distance Terminals (LDTs)) for each pair of GWs, which provide the communications with the TFMs at trackside (where the signals are received by further DLMs and LDTs respectively, which then relay the data to and from the TFMs). The TFMs are either Signal Modules (SMs) or Points Modules (PMs), dependent on what equipment is required to be operated.

System software

The language used for this is a superset of that used by SSI, making it possible to import legacy SSI data if converting an existing SSI scheme to use Smartlock. The additional language features offered by Smartlock are summarized below.

SML400 allows the CIXL to be partitioned into a number of "virtual interlockings" (VIXLs) that may either be:-

- Independent of each other functionally yet communicate via a simulation of the SSI's internal message mechanism;
- Capable of testing and writing to each other's memory in a controlled manner.

Each VIXL has its own links to the Signaler's control and display system, so these systems see a Smartlock as identical to a set of SSIs. Two or more VIXLs can process requests at the same time, independently of each other, such that a CIXL is able to work with more than one signaler at any one time.

The maximum number of VIXLs in a CIXL is 64; but in practice it is limited to 6 Panel/TD or 8 IECC/MCS type VIXLs by the number of links available for trackside and control system connections.

Many CIXLs can intercommunicate allowing a Smartlock system to be extended to cover a large and complex area.

CIXL-CIXL data transfers must use the same internal message structures as SSI, but the boundaries between CIXLs can be chosen with more freedom (given the size of area that a single CIXL can cover) such that the interfaces occur at places that keep the inter-CIXL transactions simple.

When replacing an SSI scheme, each VIXL would be made equivalent to one of the replaced SSIs. The internal messages between VIXLs are equivalent to the SSI's Internal Data Links (IDLs) and can use the original SSI data to do so.

The CIXL is configured with three memory devices (USB keys), one for each channel, loaded with the specific application data and the interlocking software.

Additionally, each computing channel has its own identity device. The information (scheme name, CIXL identity and VIXL data version) loaded from the identity devices is checked against the USB memory devices content – providing protection against the accidental use of unapproved data or software.

The interlocking software is general-purpose but can be configured for:

- Network Rail's Generic Requirements;
- The specific requirements of each signaling scheme, via the application data.

Application data is prepared in accordance with the scheme plan, control tables and other relevant input information using the Smartlock 400 application engineering system.

Smartlock data language is backwardly compatible with the SSI syntax described in SSI 8003-91, but provides some useful extensions for time delays and inter-VIXL communications.
The Alstom uses the SCADE Suite to develop safety-critical software of some of their IXL systems.

Briefly, the above suite allows the interlocking principles to be specified rigorously as communicating automata and to be translated into executable code with a certified translator. Thus at the level of individual IXL units it is possible to guarantee that software of a basic IXL principle implements the specified behavior of that basic IXL principle.

ANSALDO STS ACC

The following survey is mainly founded on [11] and [12].

Short background

The ACC systems use computer technology to implement route control, interlocking and clearing functions with high reliability.

It, also, performs automatic diagnostics, operator assistance and data logging functions to improve the operating efficiency of both signaling operators and maintenance engineers.

The availability of automatic tools design, testing, troubleshooting and maintenance contributes to reducing system implementation times and overall plant costs.

ACC safety logic can be configured to match it to different signaling context including:

- Large and medium sized mainline stations;
- Marshalling yards and multipurpose terminals;
- Railway lines with small and medium sized stations, automatic or axle counting block, grade crossings etc…;
- Metro lines.

System architecture

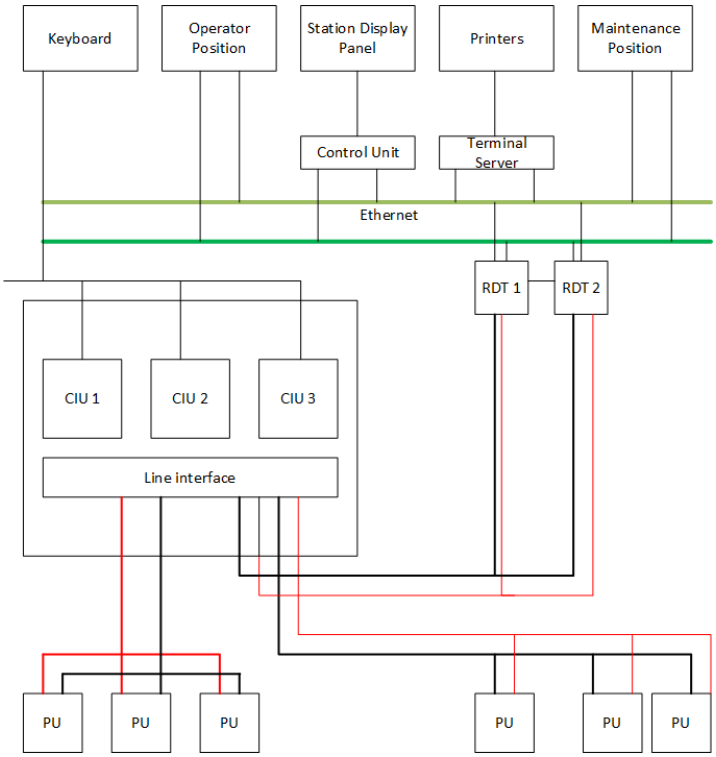
ACC is based on a distributed and modular architecture including different redundant processing nodes connected through serial lines. Two basic subsystems can be identified:

- the safety subsystem, processing all vital functions (interlocking logic and process interface)
- The non-vital subsystem (RDT - Recording Diagnostic Telecommunications -), including operator interface, data logging, diagnosis and remote control functions.

The safety subsystem also is composed of two parts:

- a central section called Safety Nucleus (NS) or Central Interlocking Unit (CIU) performing the interlocking logic and controlling the vital input keyboard ;
- A peripheral section called Peripheral Unit (PU) including a number of Trackside Units (TU), managing the input/output functions required to control the station field equipment.

The central Safety Nucleus, the Trackside Units and the non-vital subsystem are connected through a vital communication link based on optic fiber high speed serial lines.



System Control Facilities

The operator interface comprises two types of working places:

- Signal operator
- Maintenance Engineer

Both working places can be duplicated if the station is very large and operation complex.

Signaling operator Work place comprises:

- graphic station with 1 or 2 colors video screens, keyboard and mouse, used to display station panel to issue commands and form alarm/warning display;
- a functional keyboard with display for emergency controls and safety information display;
- A printer for service forms and other documents.

The functional keyboard and the display are controller by the CIU, while the other devices are controlled by the RDT.

The RDT subsystem is based on commercial computers (PC or workstations) in hot stand-by continuation. Special proprietary boards are used to connect it to the CIU through the dedicated high speed link.

The RDT subsystem is also used to provide a connection to a standard LAN to exchange information with a variety of related system such as traffic information, traffic optimization etc.

The external keyboard is based on failsafe *2oo2* hardware (device) and is connected to the three sections with a dedicated fail safe link. Through this keyboard all kind of commands can be entered:

- the ones requiring safety operation (e.g. emergency command) and the ones with no critical attribute such as route setting commands;
- The latter kind of command is normally received from the non-vital: subsystem or from a remote control system.

Central Unit Interlocking and System fault resilience policy

The Exclusion Logic is fail safe and composed of three sections based on 2oo2 microprocessor boards. Each section is connected through a safe link with a couple of safety nucleus sections, and controls their agreement in order to decide whether to enable or shut down operations.

The Safety Nucleus is based on Triple Modular Redundancy architecture (TMR). Three computer sections independently perform the same functions in the same hardware and software environment. Software diversity is used on the three safety sections with regard to the application software.

Peripheral facilities

Each Trackside Unit includes a processing computer called Area Controller (AC) and a series of electronic field interfaces called Field Controllers. The Area Controller computer contains the following elements:

- main unit, based on 2 out of 2 hardware configuration with fail safe watch-dog unit
- optional backup unit in hot stand-by to increase the availability
- Two line interfaces to manage the redundant high speed optical link connecting the Area Controller with the Safety Nucleus.

The Area Controller is interfaced by means of an electrical redundant serial bus to a number of Field Controllers. Each Field Controller is based on a 2 out of 2 fail safe microprocessor board and a field interface specific for each type of device to be controlled.

General purpose field interface are also available to control electromechanical relay when needed. Through external conditioning modules the final interface with the field device is obtained together with galvanic insulation.

The Area Controller units, together with the Field Controllers, implement field equipment control functions on the basis of the command issued by the central Safety Nucleus. They also monitor the operating states and transmit the relevant data to the Safety Nucleus.

Communication facilities

A line interface is used to connect the NS with the Trackside Units and the non-vital subsystem. A series of modules is used to convert the electric signal into an optical one, to drive the fiber optic safe high speed link.

System software

ACC safety subsystem software can be divided in the following:

- System and application software;
- Interlocking logic data;
- Station layout data.

The logic management program is unchanged regardless of the application due to the particular data driven structure of the interlocking logic: a set of logic operations including verifications and assignment statements define the behavior of the logic program.

This data base together with the station layout data base is accessed and interpreted by the logic management program to perform the interlocking logic.

For this reason all the fixed software is verified and validated once and needs no more testing when new logic or layout data is introduced.

If needed, new rules can be defined and tested using automatic tools for entering and verifying the new data.

The station layout database is entered with the aid of a completely automated graphic tool. This CAD system, based on commercial computers, can be integrated with a simulation tool to allow off-line testing of the configured software.

AŽD Praha ESA 33

The following survey is mainly founded on [13]

Sort background

Station interlocking ESA 33 is a full computer based interlocking system that serves for safety operation of railway traffic in stations with track branches or without them.

It is the next stage of development of computer based interlocking produced by AZD Praha s.r.o. and meets SIL 4 safety integrity level in accordance with EN50129.

ESA 33 is computer based interlocking at all levels – commanding, control and executive ones. Coupling outdoor equipment is done electronically, i.e. by means of electronic modules that have been specially developed for different outside elements (for example modules for signal, point machine, track circuit and so on), possibly by relay interface if there is requirement to control non- standard outdoor element in station. ESA 33 can work with cold or hot standby at commanding level and at control level. A processor unit and power supply unit at executive level can work with hot standby feature as well.

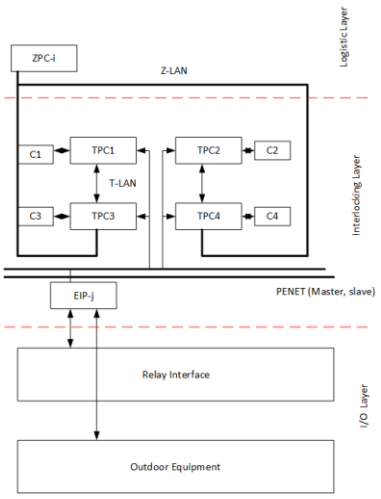
System architecture

From the above cited paper it is possibly to identify the elements in the three layers:

• Commanding level

• Control level

• Executive level



System Control Facilities

At the logistic layer it will be found the signalman workstation termed (Z)PC, which can work in in cold standby or hot standby mode, that are connected through communication link to the Interlocking layer termed control level.

The ZPC recall common pc as they are assembled by a keyboard, mouse, LCD monitors for displaying rail yard, and so called technological monitor for displaying pages with operational status of different parts of ESA 33 and text messages to operating staff.
It is possible to connect up to 12 commanding computers to the control level and theoretically unlimited numbers of computers, that don't allow operation used for displaying controlled yard on a large screen display.

It is also present technological monitor that were used for displaying of a list of non-fulfilled conditions in case of processing risk functions. The risk functions are those that function that involve cooperation with operational staff as setting calling on signal aspect or switching a point machine to opposite position when the track section is occupied and so on.

Displaying the list of non-fulfilled conditions is vital. After reading the list of non-fulfilled conditions by the operational worker, he has to confirm or reject the list.

Required action is processed in sub level (Interlocking layer) after confirming the list of non-fulfilled conditions by special confirmation sequence.

It follows, from above, that ESA 33 has vital commanding procedures in case of risk functions - it is guaranteed that ESA 33 will not generate and confirm risk function by itself.

Commanding level can be installed even in more than one station. In these cases the commanding level is connected to the control level similarly as groups of decentralized EIP object controllers.
It is possible to connect ESA 33 interlocking to the system of remote control. Remote control of DOZ-1 type is an integral part of ESA 33.

Theoretically, it is possible to connect unlimited number of stations. Practically it depends on the ability of the dispatcher, how many stations and what density of traffic with he can control. Up to date there are apart from several section control (typically dispatcher controls 3 or 4 neighboring stations) two central traffic control (CTC) centers installed in the Czech Republic. The CTCs covers approximately 100 km and 80 km of line with 15 and 8 controlled stations. Workplace of the CTC is fully equipped commanding place. It is possible to set all functions including risk functions (e.g. setting a calling on signal aspect) from the CTC workplace.

It is possible to define functional or geographical restrictions for each CTC workplace similarly as for regular commanding place used for controlling one station.

It is allowed to hand over control from CTC to local control as well as take over controlling the station from local control to the remote control by the CTC workplace. Graphical and technological layer (GTN) can be connected to the ESA 33. GTN is a telematics layer of the interlocking equipment. This layer from AZD production allow in connection with ESA 33 following functions:

- automatic recording of traffic documentation
- graphic displaying of a train traffic diagram
- building of prospective plan of traffic
- transmissions of information from/to other sources (for example systems for train position monitoring)
- building of statistics of traffic
- recording of operation of operational staff and interlocking activity

Diagnostic facilities

Data archives are stored to the RAM disk, which are part of each technological and commanding computer.

EIP object controller has diagnostics archive too.

All archives can be stored to the portable media and browsed on the other computer with installed special program later on. However, it is possible to connect diagnostic server, marked as LDS.

This server is connected to the control and executive level and server program saves all archive data to the server hard disk automatically. Moreover, it is possible to connect modules for measuring analogue values, such as voltage, insulating resistance, throwing current, temperature and so on. These data are stored as well. Access to the data stored in diagnostic server is possible through the computer with installed client program and connected to an access point of the diagnostic network.

Central Unit Interlocking and System resilience policy

The CUI of ESA 33 consists of a pair of active and a pair of standby - termed technological - computers TPC, which are interconnected by local network. The standby pair can work in cold or hot standby mode.

A concept of safety of the interlocking is based on the principle of composite safety in case of faults in accordance with EN 50129. The control level is configured as 2 times 2oo2 with the same hardware and diverse software.

Pairs of computers TPC1 – TPC2 and TPC3 – TPC4 exchange the data required for verifying of right function through T-LAN.

Moreover TPC1 – TPC3 and TPC2 – TPC4 exchange data required for mutual changeover between states “active” and “ standby” in case both pairs work in hot standby mode.

Hardware comparators, termed as C1 to C4, are used to switch of a faulty pair of technological computers. If technological computer works all right it transmits to its own comparator six signals.

The next condition for transmitting these six signals to the comparator is the correct functioning of the second technological computer in the pair. The comparator compares the received signals in the preset shape. If there is a discrepancy between the received and the preset signals, power supply to the particular TPC is switched off. Because switched off TPC cannot communicate with the second TPC in a pair, it stops transmitting signals to its own comparator and consequently power supply to the second TPC in the pair is switched off too.

By a performance point of view, the ESA 33 can control station with 1200 logical elements that is railway station with approximately 300 physical interlocked points.

Because there are not many such “big” stations around the world, typically there is one control level with decentralized (remote) EIP object controllers to more stations (especially neighboring stations).

Physical connection of decentralized groups of EIP object controllers is realized by fiber optic cable and optic modems. In this case it is possible to move each group of EIP object controllers away up to 40 km from previous one.

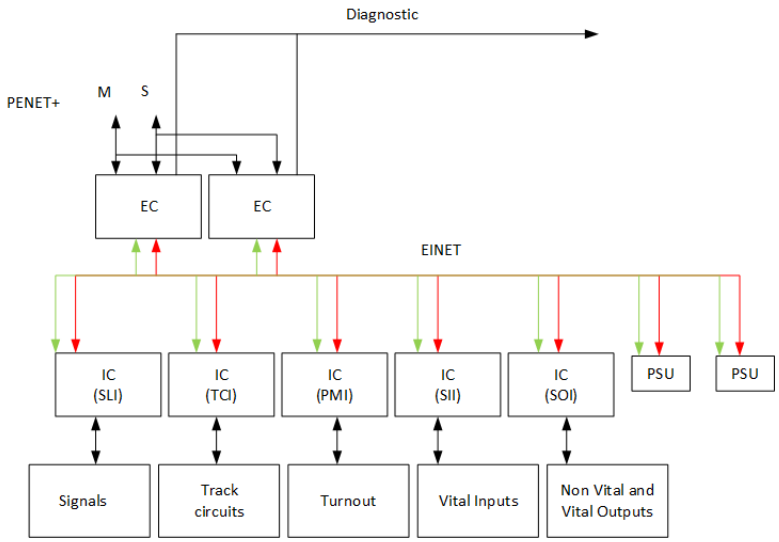
It is not necessary to have commanding level located at the station where the control level is installed.

Peripheral facilities

At the I/O layers it will be find the EIP object controllers.

A block diagram of EIP object controller is presented in figure below. From the point of view of architecture the EIP object controller is designed as “two levels” object controller:

- level of Element Controller – EC
- level of Interface Controller – IC
- Power Supply Unit



EC are processor units that arrange vital communication between functional core layer units on the one side and units IC on the second side.

It works as multiplexer and de-multiplexer and modifies transmitted data on base of the state of IC units. The EC units collect diagnostic data for local and remote diagnostics. It is possible to use one EC card in one EIP object controller; in this case the EC unit has no standby, or two cards EC. In case when two EC cards are used in the EIP object controller, they work in hot standby mode. Each EC unit works in 2oo2 mode.

IC units are designed as the units with inherent safety. They are intended for straight control of elements. Because of concept of safety 2oo2, they are designed for working in such system. Both branches are placed on the one module.

There are types of IC units:

- SLI
- TCI
- PMI
- SII
- SOI

SLI unit provides contactless control and detection of lighting of signals. The unit can control 8 signal lights at the most (the number of controlled lights is subject to configuration), 4 lights out of these 8 can be prohibitive lights. Independent replaceable switching modules are used for switching on/off the lights.

TCI reads contacts of track receivers and transmits additional code of continuous automatic train protection system to a track circuit. The unit can control 8 coded spots at the most, i.e. for example 4 track sections without branches. The coding is carried out by external (independent) high power switches.

PMI unit provides contactless control and detection of position of point machines. It is possible to control 2 point machines by the one PMI unit, whereas each point machine is powered independently. Each output can control two physically coupled points, i.e. points with consecutive switching on of electric drive. If needed, relays detecting position of the point machine can be connected to the unit too.

SII unit provides contactless reading of inputs. One unit has 32 inputs at the most.

SOI unit is designed for contactless controlling of interlocking elements. The unit has 8 vital outputs and 8 non-vital outputs.
The control level has relatively huge computing capacity. In this time, one control level, i.e. four TPCs,
Data including train numbers that are necessary for function of such telematics application, is get from the Z-LAN of the control level. Example of graphic displaying of the train diagram is at the fi g. 4.

Communication facilities

Communication network of control level is divided to three physically separated networks:

- T-LAN;
- Z-LAN;
- PENET.

Z-LAN network works on the principle of THERNET IEE 802.3 with TMNET protocol (own communication protocol of AZD). This network connects the logistic and functional core layers. Physical connection is realized by fiber optic elements.

T-LAN network works on the principle ETHERNET IEE 802.3 as well. All four functional core computers are interconnected by this network.

PENET network works on principle RS485 with communicating protocol PENET+ with transfer rate 115, 2 kids. PENET+ is again the own communication protocol of AZD.

PENET network connects functional core and I/O layers.

PENET network is “two branches” network, i.e. the first branch, called master, connects executive level with TPC1 and TPC3, the second branch, called slave, and connects executive level with TPC2 and TPC4.

EC unit communicates with IC units by communication protocol EINET. This communication protocol is used on interface RS485 similarly as protocol PENET+. This is power supply unit. If two PSU pieces are used, they work in hot standby mode. Input and output voltage is isolated from each other.

System software

The software is separated to mutually cooperating parts. One part is so called general software that includes program code for communicating processes and partially program code of some traffic safety algorithms, which don't differ from application to application on the lines operated by one railway administration, for example algorithm of switching of a point. Second part is called application software that includes information about shape of the rail yard of factual railway station, dependencies defined by an interlocking table and so on.

ECM SPA HRM9

The following survey is mainly founded on [14].

Short background

With the conception of an architecture contemplating HMR9 technology as the core of the signaling system, ECM has developed a completely integrated, flexible, scalable and modular solution. By analyzing working models and the operational requirements ECM has implemented the key requirements of a high modular signaling system.

Based on the fundamental requirements of simplification and standardization of engineering solutions for the standard practices and customer requirements, ECM has developed a signaling solution that is both future proof and cost-effective, the system is all about enhancing the infrastructure and it can be delivered and put into service very quickly.

The ECM HMR9 system is compatible and able to operate with ETCS (European Train Control System).

By implementing the multi-station concept it is now possible to control an entire railway line from a central post with one interlocking, making it possible to make changes to single station layouts without having to reconfigure and retest the entire system.

Unlike the old single-station concept the multi-approach allows each signaling device to be configured as if it were physically connected with a specific station.

This brings with it enormous advantages:

Additional stations can be added when needed, making it easier to carry out a staging approach without having to create a blockade and closing down lines for long periods.

- Significant reduction in the amount of testing: only the added parts of the system need to be verified and tested.
- Reduction in hardware.
- Changes to the system have almost no impact since the interlocking is data driven.

System architecture

The HMR9 system consists of the following main components:

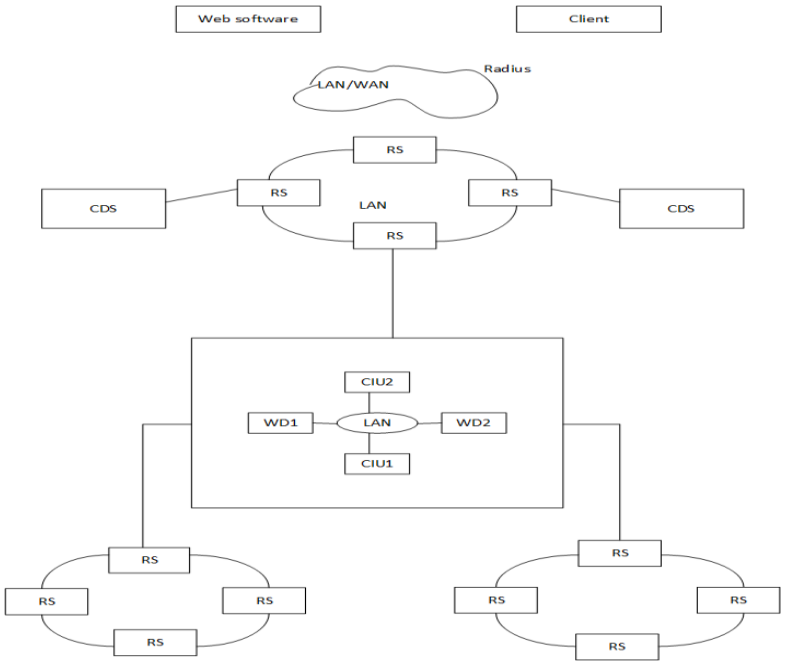
- Central Post – the central post consists of the central interlocking unit and the control and display system, which includes the signaler control terminals, alarms and fault reporting, and event recording.

- Multi Object Bay – Physical structure containing the Object Controllers for controlling the field devices (signals, point machines, track circuits etc.).

- Fixed Telecommunications Network (FTN) – a switched Ethernet network between the interlocking system and all of the FTN access points for the object controllers connected to the interlocking system by fiber-optic, existing copper cable or via a wireless connection

- PLC Object Controller – A PLC to interface other interlockings or other surrounding areas

- Remote panel control system – a control and display system which can be placed away from the central post (that is, situated in an operations office or on-site in the case of degraded mode).



System Control Facilities

The place Command and Control Center consists of:

- A PC;
- Watch Dog;
- Remote Graphics Units ;
- Monitors, keyboards and mice.

The bench consists of a control unit and related graphics quad 4 Monitors, keyboards and mouse and any voice alarm system.

The PCs are connected to an Ethernet LAN through CIU ring switched to 1 GB. The PCs are commercial HW and are controlled by a circuit Watch Dog. The Remote Graphics Unit is connected to the module's Remote Graphics Extension (residing on a PC) via point -to-point optical fiber. In case of failure PC the Watch Dog turns it off and activates the second system that was in warm standby that takes control.

The PC, the watch dog, and its network loops are contained in a cabinet which is located at a certain distance from the counter of command and control. The monitors are commercial products and replacement parts can be always kept available for a quick replacement.

Diagnostic facilities

Diagnostic Management System includes the maintenance terminals, alarms and fault reporting, event recording, diagnostics, archiving and retrieval facilities, and many other non-safety-related aspects for diagnostics control and supervision

Central Unit Interlocking and system fault resilience policy

The central interlocking unit is realized through a two-out-of-two redundant architecture. The two CIUs are connected over an internal area network. Connection with the field is through wide area networks, while the con trolls and display system is connected by a local area network. The CIU also has a watch-dog circuit that votes the validity of the processing and shuts down the faulty unit in the case of an error.

Peripheral facilities

The trackside devices are contained in several types of equipment such as multi-object bays, trackside functional modules and harsh environment location cases.

The multi object bay (commonly referred to as a peripheral post) consists of an open frame arrangement containing object controllers and conditioning modules.

The innovative approach of the HMR CBI means that the control equipment can be installed either inside a peripheral location (containing one or more multi-object bays), inside a case at the side of the track, or in a trackside functional module in the immediate area around the signaling equipment (on a signal mast or gantry).

Communication facilities

On the communication level, the HMR9 uses an IP protocol therefore allowing the possibility of using any type of device that supports an Ethernet system as well as wireless or dedicated fiber optic as physical support. Since the IP protocol is public, the ECM HMR9 architecture is able to integrate with other systems provided by other suppliers.

The data communications network is split-up into five separate communication rings:

- a wide area network (WAN – Primary); (WAN - Primary)
- a wide area Network (WAN - Secondary)
- a wide area network (WAN - Secondary); (LAN)
- an internal area network (IAN); and(IAN)
- a fixed telecommunications network (FTN).(FTN)

The WAN normally consists of a primary and secondary link, but certain applications may only need a primary link with redundant ring switches.

As the name suggests, the local area network (LAN) covers a small local area. This network is used to connect the control and display system to the central interlocking unit at the control center, and to connect with the diagnostics and maintenance system and related remote terminals.

The internal area network is the network which connects the components of the 2oo2 redundant central interlocking unit with the watch-dog circuit and communications with the outside world. The network is contained within the central interlocking unit module in the control cabinets at the control center.

The fixed telecommunications network provides a switched Ethernet network between the interlocking location and all of the FTN access points for the object controllers connected to the interlocking. This allows the use of Ethernet through fiber-optics, copper cable or wireless connection from the FTN access point so that the IP network is extended to a gateway in each signaling location which contains object controllers. Within the signaling location, each object controller has its own Ethernet connection and IP address.

System software

The logic manager is the invariant code that processes the interlocking controls by performing the safety checks and, if these are satisfactory, generates controls for the equipment out in the field.

From a software point of view, it is a ‘safe interpreter’ of a byte-code generated off-line from object-oriented language sources.

Object-oriented language is used to describe the signaling devices as objects belonging to a certain context class which, according to events (field indications, events from other objects, operator or automatic controls), develop their own state. The language also provides the possibility of defining, for each context class, several connections to the object controllers to make the safety logic for the signaling devices independent from the control and indication method. The peculiar characteristics of the ObjRail language, and types of variables in the context classes, are described in separate documents.

For each process cycle of the central interlocking unit, the logic manager processes the byte-code of the context classes, defined by the safety-logic software design engineer. The characteristics of each instance are always extracted during the execution phase from the configuration database.

Execution of the class byte-code produces an update of the class dynamic variables which represent the state of the logic entity, and an update of the interface variables which generate the control messages to the object controllers.

Two application-dependent databases – interlocking rules database and configuration database – are included in the central interlocking unit software. These databases are managed by the invariant code described in the previous section.

The interlocking rules database contains the specific application's safety logic which configures the HMR CBI so that it is in line with the signaling principles of the specific country.

The configuration database contains the site-specific data for a particular geographical application. This data defines the actual points, track circuits, signals and so on that are to be used with each of the processes defined in the interlocking rules database.

The data preparation process (DPP) includes all tasks needed to produce the central interlocking unit's data system files from source documents (the Signaling Scheme Plan and the Control Tables).

The scope includes preparing the safety logic and application-specific geographic data (all elements of application data used by the central interlocking unit). System file generation is a key step of the data preparation process in which the safety logic and geographic data are brought together to be loaded onto the central interlocking unit's independent processing sections.

The data translation tools used in the data preparation process for the generic application and specific application phases are:

- Plan Editor
- Control Tables Generator

The data preparation process is in compliance with CENELEC EN 50128 Norm Railway applications - Communications, signaling and processing systems - Software for railway control and protection systems, in separate documents.

OTHER SYSTEMS

In this section it will be presented some systems which it has not been possible to obtain complete information

THALES – ELEKTRA

The following survey is mainly founded on [15], [16] and [17].

Some background

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.

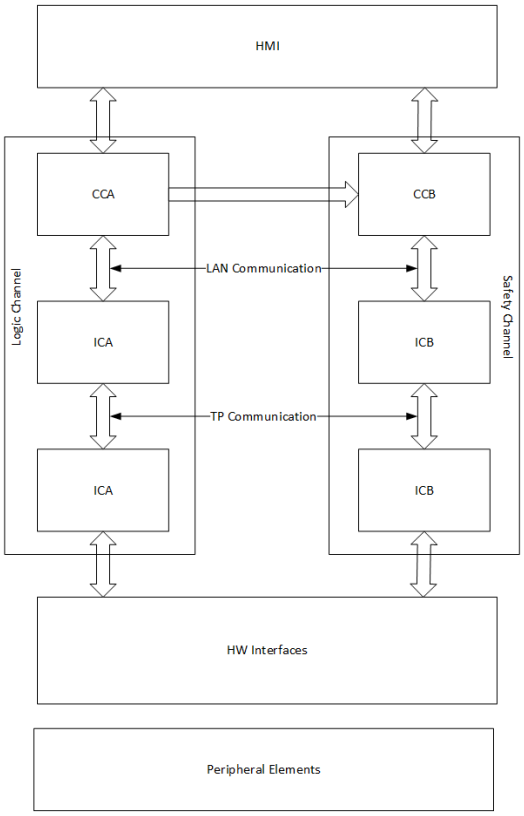
System architecture

For architectural and maintainability reasons the system is split into three levels:

- Human Machine Interface (HMI);
- Central Controller (CC) ;
- Field Element Controller that comprises the Element Controller (EC) and the Interface Controllers IC.

In addition to the three levels shown in the following figure there is a component for long distance communication and external interfaces respectively.

This Remote Control Unit (RCU) has also two-channel software architecture and provides the interfaces to RBC, to the automatic functions and to the neighboring interlocking as well as to a remote control system.



In opposition to the two-channel architecture of the above cited Communication Controller (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 threefold 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.

System Control Facilities

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.

At the hardware level the TAS control platform uses commercial standard components, which are supplemented by added-value services for railway systems.

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. The next Figure 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.

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.

System software

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.

To handle the requirements management process the tool DOORS was used, nowadays under control of TREK (Thales Requirements Engineering Kit).

The development process for ELEKTRA follows the V model. 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 phase’s 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 Clear Case 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 [18] 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.

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 Clear Quest 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 an efficient cooperation so that the requirements of the functionality as well as those of the time constraints were met.

System fault resilience policy

The fundamental approach to achieve safety with the system ELEKTRA is the two-channel architecture and diverse programming. Strictly a part of that there are redundant system elements to enhance reliability and availability.

The fault tolerance system offers configurations like 2-outof-2, 2-out-of-3 or even the non-redundant variant 1-outof-1. For example the Thales axle counter uses the 2-outof- 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.

PRORAIL MOVARES EUROLOCKING

The following survey is mainly founded on [19].

Eurolocking is a SIL 4 PLC interlocking completely based on Commercial of the Shelf (COTS) hardware components. Any (SIL 4) PLC can be used in this concept to engineer an open system. Only the logic inside the system is dedicated to the railway environment.

Eurolocking is developed according to the Cenelec EN50126, EN50128 en EN50129. The architecture follows the generic (modular) interlocking architecture.

The core of the system consists of the:

- SIL4 PLC CPU;
- Maintenance and Diagnostics system;
- Data logger.

The latter to be used in case of accidents to 'rewind' the status of the interlocking system. Digital I/O, both in the interlocking room and in trackside cabinets, can be connected directly to the outside elements such as signals, etc.

Besides safe digital I/O, various communication standards are supported such as Ethernet and Profibus/Profisafe.

Upon request, specific communication protocols can also be implemented to support, for example, existing dedicated CTC's. As the core of the (safe) system a safety PLC is used.

In the design of the interface to the trackside elements, a modular approach is implemented. Standard IRS (Interface Requirement Specifications) is implemented in modules (hardware and logic) and can be exchanged from infrastructure operator to infrastructure operator.

All standard interfaces are implemented. New interfaces can be easily added. New modules to communicate with LEU's (Line side Electric Units) for ERTMS Level 1 and an RBC (Radio Block Centre) for ERTMS level 2 are under investigation. In the PLC there is a possibility to implement (low level) customer specific communication protocols.

Movares are currently working on the implementation of a network based direct coupling to axle counting systems. As it is an open standard, the possibilities are infinite.

The logic programmed into the PLC defines the system as an interlocking. Here the railway specifics are programmed. In the Eurolocking solution, this logic can be set up and altered by any (certified) engineering company. For this, the operator specific signaling rules are converted in an engineering manual. With this engineering manual, new interlockings and changes in existing interlockings can be engineered.

To design more efficiently, standard building blocks are created. This principally creates an improvement in the verification and validation process of the specific application.

The selected CPU modules are internally a 2 channel SIL4 system. Additional modules can be inserted to improve availability.

Current system availability requirements state 99.9998% which can be translated as a system downtime of less than 2 hours every 100 years. Although this is quite a steep requirement, within the Eurolocking architecture, it is easily achievable. As the hardware modules are independent of the logic, redundant modules can be added (or left out for branch lines) without modification to the (railway) logic in the PLC.

For safety a THR (Tolerable Hazard Rate) of 3.0x10-9 per hour is required. This THR is defined as an interlocking system, controlling a station with a total amount of 15 (light) signals and its track circuits, switches etc.

BOMBARDIER TRANSPORTATION – EBI-LOCK 850

The following survey is mainly founded on [20].

System architecture

EBILOCK 850 consists of 3 sub-systems.

a) JZA 850. This is the interlocking computer system. In conventional terms this takes the place of the control, indication and interlocking circuitry normally located in the relay room.
b) JZU 840. This is the object controller system which covers all control of the wayside objects including the transmission of the data from the central computer to the location cubicles. In conventional terms this is equivalent to through circuits and location circuits.
c) GEN 285. This is a generating system for use on the EBILOCK 850. Basically it is a support system which contains all the necessary data for the complete system, e.g. obj6ct identities, station layouts, etc. In conventional terms this takes the place of signaling plans, typical circuits, etc. It is also capable of producing auxiliary information such as material lists, documentation, etc.

System Control Facilities

MAN 85 is a control system developed to work the interlocking direct utilizing 1 or 2 workstations or it can act as a standby system to the main control and supervisory system like the 715.

The operator commands are processed in the interlocking computer, which following a pretest routine allows the necessary control data to be transmitted around one of up to 13 possible loops.

Similarly status messages are received from the signals and points via these loops.

The technician has one or two personal computers and printers for typing in commands to the system and receiving printouts. A maintenance panel unit is provided for each computer and is used for hardware troubleshooting and some related software tests, Status indicators are provided on top of the computers showing whether the computer is running, halted or occupied for maintenance work.

There is also an operator’s panel provided for both the operators and technician for restarting and reloading of the computers as well as other functions and indications.

System software

The processing in the interlocking and transmission around the concentrator loops is cyclic. Cyclic time is approximately 0.6 seconds. During each cycle - all information concerning the status of the various objects is

collected the interlocking data is processed in two separate program 'sequences commands to the objects are compiled and transmitted information concerning the object status is transmitted as indications to 'the control and supervisory system Maneuvers from the control system are processed in a background program and not part of the fixed cycle.

System fault resilience policy

To ensure safety in both the online and standby computers the interlocking section in each computer, is divided into two parts, A and B. Each of these two parts uses its own data format, and produces its own commands which are issued to the Object Controllers.

Comparison of the A & B commands are made at the last point in the system i.e., in the object controller itself.

This technique is called diversified programming. The program sequence in A is independent of that in B. They fulfil1 the same function but the data is processed in different ways, to achieve this independence, and hence safety, the two programs are designed by two separate programming teams, working from a common specification. Relative to each other, the program sequences and data are reversed and inverted and stored in different areas in the computer memory. Any hardware faults are discovered using this technique. The data is updated every program cycle and time stamped to prevent the use of obsolete data.

Commands from the operator are processed for validity etc., via a pretest routine before entering the interlocking phase. Independent calculations are carried out in the interlocking processor resulting in independent A & B commands being transmitted to the object controllers on site.

FINAL CONSIDERATIONS

A modern electronic interlockings system must be highly flexible and scalable, to enable them to be adapted to different sizes, different hardware, different environments, different signaling principles and even different applications.

Also, all these systems have an important common feature: they are safety-critical and must therefore be developed according to the highest safety integrity level (SIL4), as defined in the standards applicable to the railway industry (CENELEC 50126, 50128, 50129, Railway Applications Standards [RAMS, software and electronics]). Apart from being suitable for safety-critical operation, railway systems must also be highly reliable and available, and in most cases must meet stringent real-time requirements.

Some of the key features to this flexibility are:

- Modular**:** Inputs and outputs are based on modules. The number of modules installed in the system is matched to the system capacity. The type of module is selected according to the function and voltage of the internal device.

- Expandable**:** Multiple systems can communicate on a peer-peer or master slave basis to either provide a larger system or to distribute the input and output.

- Easily configurable**:** The logic in the interlocking must be easily designed to suit different signaling principles. Fixed constructs make this difficult. The ability for a Signal Engineer to build standard circuits that can be inserted, modified if necessary, and meaningfully named according to the logic function are becoming a must in today's cost pressure environment. Easy to use design tools are required to support the logic configuration.

- High System Capacity**:** Processors are becoming ever more powerful, permitting larger systems and higher speeds. However, the vendors must be able to produce very small system using the same hardware and design tools at a competitive price, so a low base cost is important.

- Simulation and Maintenance Tools**:** These are important in testing and maintaining a system. They must also provide the flexibility to support different systems and principles.

Due to the increasing complexity of applications, it is also necessary that the platform be able to keep up with ever increasing demands for processing power, memory consumption and connectivity.

This trend can only be addressed by the use of off-the-shelf hardware and operating systems. In order to be able to keep up with the advances in hardware and operating systems, these components should be as interchangeable as possible, such that exchanging them does not compromise the system's safety integrity.

Further on is reported a summary for each aspects.

System architetture

IXL System	SCF	CPI	Peripheral facilities	Diagnostic facilities	Communication facilities
SSI	Light Panel, Terminal	Motorola 6800 (16-bit)	Different module for each trackside function	Passive External module	Serial link Separated module, drive up to 6 TFM
WESTRACE	Proprietary (Client/Server Application)	PowerPC	Different module for each trackside function	Direct information access locally or via modem link	Parallel bus between vital systems, Ethernet between different interlocking
WESTLOCK	Proprietary (Client/Server Application)	Motorola 6800 (32-bit)	Different module for each trackside function	Passive External module	Full Ethernet
SMARTLOK	Proprietary (Client/Server Application)	Motorola ColdFire (32-bit)	Different module for each trackside function	Incorporated in the Support System	IMNET, RS-422 WAN
ACC	Proprietary (Client/Server Application)	No data	No data	Incorporated in the Support System	Full Ethernet
ESA 33	Proprietary (Client/Server Application)	Unknown 32-bit	No data	Incorporated in the Support System	Full Ethernet
HRM9	Proprietary (Client/Server Application)	Intel Dual Core	Different module for each trackside function	Standalone system	Full Ethernet

System software

IXL System	Development	Engineered Language	Programming framework
SSI	Abstract model of Relay circuit	GDL	Direct code
WESTRACE	Abstract model of Relay circuit	Ladder Diagram	WESTCAD
WESTLOCK	Abstract model of Relay circuit	Ladder Diagram	WESTCAD
SMARTLOK	SCADE	State charts logic diagram	Unknown proprietary
ELEKTRA	V model Doors	CHILL/PAMELA	No data
ACC	V model	Ladder Diagram	No data
HRM9	V model	ObjRail	No data
EUROLOCKING	No data	Ladder Diagram	No data

System fault resilience policy

IXL System	Configuration Type	Stand by
SSI	TRM	HOT
WESTRACE	Single Processor with diversified software 1 out of 1 System	HOT
WESTLOCK	TRM	HOT
SMARTLOK	2 out of 3 System	HOT
ELEKTRA		HOT
ACC	1 out of 1 / 2 out of 2/ 2 out of 3/ 2 out of 4 System	HOT
MICROLOCK	Single Processor with diversified software 1 out of 1 System	WARM/HOT
EBI Lock 850	Single Processor with diversified software 2 out of 2	HOT

	System	
ESA 33	2x2oo2	HOT
HRM9	Multicore Processor 2 out of 2 System	HOT
EUROLOCKING	Single PLC 2 out of 3 System	HOT

BIBLOGRAPHY

[1] M.Williams - Westinghouse Signals LTD, «Adelaide Signalling Project Solid State Interlocking,» 1989.

[2] Westrace, «Westrace the flexible safety controller SYSTEM OVERVIEW http://www.westsig.co.uk/Repo/files/Westracel2.pdf,» Invensys westinghouse rail system, 2008.

[3] I. Rail, «Datasheet 10A-31,» Invensys Rail, 2009.

[4] P.James, «SAT-Based Model Checking and its Applications to Train Control,» 2010.

[5] K. Kanso, «Formal Verification of Ladder Logic,» 2008.

[6] Noel Burton, BSc MIRSE Westinghouse Rail Systems Australia, «How many interlockings does it take to signal a freight train?,» The Institution of Railway Signal Engineers Inc Australasian Section Incorporated.

[7] Invensys Rail system, «WESTLOCK Interlocking Datasheet 10A-9,» Invensys Rail system, 2008.

[8] Signalling Solutions, «Smartlok 400,» http://www.signallingsolutions.com .

[9] C. Minkowitz, «Formal Specification for Design Diversity: Two Case Histories, One Approach,» in *ADBIS (Local Proceedings)*, 2010.

[10] D. Liu e T. L. McCluskey, «The Object Centred Language Manual - OCLh -,» 1999.

[11] A. M. .Amendola, L. Impagliazzo, P. Marmo, Mongardi, G. Sartore(Ansaldo Trasporti), «Architecture and Safety Requirements of the ACC Railway Interlocking System,» IEEE, 1996.

[12] A. Anselmi, A. Fantechi, S. Gnesi, S. Larosa, G. Mongardi e F. Torielli, «An Experience in Formal Verification of Safety Properties of a Railway Signalling Control System,» *Safe Comp 95,* pp. pp 474-488, 1995.

[13] J. LECHNER, AŽD Praha s.r.o., «Computer-based interlocking,» *Archives of transport system telematics,* vol. 2, n. 1, pp. 43-47, 2009.

[14] E. SPA, «HMR9 - High modular redundancy,» http://www.ecmre.com/en/hmr9.xhtml.

[15] Walter Fuß, Thales Rail Signalling Solutions GesmbH, «Tailored Solutions for Safety-Installations in the Loetschberg Tunnel -A Project with Importance for the Trans-European Rail Traffic».

[16] G. Staffel e W. Bohm, «Alcatel Stellwerkstechnik,» *e&i,* vol. 3, n. 117, pp. 208-215, 2000.

[17] Thales Group, «Locktrac Elektra 6131,» https://www.thalesgroup.com.

[18] C. E. 50128, «Railway applications—Communications, signalling & processing,» 2001.

[19] Michiel Blaauboer MSc Technical Manager Movares, «SIL 4 Interlocking based on COTS hardware,» The Institution of Railway Signal Engineers Inc Australasian Section Incorporated.

[20] MR. B. STEELE FIRSE EB SIGNALS PTY. LTD. BRISBANE QLD, «Computerized Interlocking - 850 Systems,» IRSE, 1989.