Testing and Commissioning Handbook

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

aIE	Advanced Industrial Engineering
CENELEC	European Committee for Electrotechnical Standardization
DMI	Driver Machine Interface
EMC	Electro-Magnetic
EN	European Norm
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
EVC	ETCS Vital Computer
FAT	Factory Acceptance Test
IL / IXL	Interlocking
INESS	Integrated European Signalling System
IOP	Interoperability
IRIS	International Railway Industry Standard
ISA	Independent Safety Assessor
ISO	International Organization for Standardization
HW	Hardware
LEU	Lineside Electronic Unit
LOPA	Layer of Protection Analysis
MMI	Man Machine Interface
NSA	National Safety Authority
OBU	On-Board Unit
PPE	Personal Protection Equipment
QA	Quality Assurance
RBC	Radio Block Centre
SME	Small and Medium Enterprise
SW	Software
TSD	Test Sequence Debugger
TVP	Track Vacancy Proving / Protection
UK	United Kingdom
UNISIG	Union Industry of Signalling
V&V	Validation & Verification

Section 1 – EXECUTIVE SUMMARY

INESS project has been formed to derive a new common European interlocking as part of the drive for interoperability in railways and a single market. The current view of the railway market is that the equipment is too expensive leading to rail being seen as an uncompetitive form of transport when compared with other transport modes. INESS is seen as a vehicle to help reduce equipments costs. To provide a cost effective solution the project has pursued a number of work-streams, each looking at a particular aspect of an interlocking, functionality, architecture, et cetera each topic contributing to an overall cost reduction estimate as part of a business case.

This Testing and Commissioning Handbook forms deliverable F3.M1 from Workstream F. It addresses the objective of providing a recommended method of optimised testing and commissioning of the INESS interlocking applications in a cost effective way. The ideas and methods proposed could be used for other interlocking types currently deployed on the railway infrastructure although some of the specifics would vary because of the differing technology.

In developing this handbook the work-stream has taken input from both industry and railways in an attempt to arrive at a position where both sides gain benefit through reduced costs, uncertainty and time scales. It has been recognised by the contributors that if we continue with current practices and methods nothing significant will change and costs will remain stubbornly high. Therefore the handbook contains what some might describe as radical ideas, taking note of how other industries approach the task.

The handbook analyses the current practices, 'state of the art' as a starting point to provide an assessed reference point for the rest of the work.

The notion of removing/reducing to a minimum the on site testing has been taken on board coupled with production testing techniques to improve the quality of the delivered product and reduce cost. A method is described within the handbook of how this can be achieved. Other influences have been taken account of by the work-stream such as the adoption of methods originating from the ERTMS arena of automating the testing; again conclusions are drawn from this area and opportunities assessed. The idea of simplifying the application data by not necessarily utilising all the complex functionality of the interlocking is examined as a possible method of 'productionising testing' and achieving a 'safe by design' state where testing can be radically reduced.

A method of assessing the cost benefits is put forward so that the various methods can be assessed by users and data can be provided by the work-stream to Work-stream B for the INESS business case.

Section 2 – INTRODUCTION

INESS project has been formed to derive a new common European interlocking as part of the drive for interoperability in railways and a single market. The current view of the railway market is that the equipment is too expensive leading to rail being seen as an uncompetitive form of transport when compared with other transport modes. INESS is seen as a vehicle to help reduce equipments costs. To provide a cost effective solution the project has pursued a number of work-streams, each looking at a particular aspect of an interlocking, functionality, architecture, et cetera each theme contributing to an overall cost reduction estimate as part of a business case.

A key determinant of the cost of overall ownership is the testing and commissioning activity associated with the application of an interlocking. Work-stream F has been formed to investigate this area. Testing and commissioning is important because inefficiencies in this process accumulate with each application of the interlocking and any subsequent alterations to the configuration of the railway. Costs arise from a number of sources, direct labour, safety arrangements and processes, testing practices, access to the track, and provision of alternative services to the public whilst the works take place.

This report forms a deliverable of Workstream F looking at the methodology of testing and commissioning and how to improve performance in this area.

The report starts with a review of current practices to attempt to identify best practice, however it is clear that there are wide variations in current practice that are partly driven by country specific requirements, partly regulatory and partly infrastructure manager driven. Therefore what is regarded as best practice by one country may not be viewed in the same light by another. The work-stream has taken an independent view on the merit of these practices to cut through the political considerations and arrive at a technically optimal solution.

This same approach has been taken with other parts of the work carried out to develop this deliverable very much focused on an optimal technical approach to deliver the objective of an optimal testing and commissioning regime which will reduce cost for both the suppliers and railways whilst maintaining the primary safety objective.

Novel ideas are put forward as part of the approach which takes as a reference point a testing and commissioning stance, looking back at an interlocking design, rather than the traditional view of a design based stance, looking down stream to a testing and commissioning process. As a result some of the common practices are challenged such as the notion that testing has to be done on site. This practice does not happen in other industries so why are the railways different? Another area examined is the notion that applications have to use all the complex functionality provided by an interlocking product, which dramatically complicates testing. The report sheds some light on these areas and resultant opportunities.

Finally there is a conscious effort to provide information that can be used by Workstream B as part of the business case analysis.

Section 3 – TESTING AND COMMISSIONING METHODS

3.1 State of the art in Testing & Commissioning

Testing is an essential part of the development and commissioning phase of an interlocking. The efficiency of the testing phase has a large impact on the costs associated with an application. Traditionally, electronic interlocking solutions have been bespoke to national railway administrations and have been designed by manufacturers in concord with the national signalling rules and standards reflecting their current state of evolution and also with the aim to address specific requirements of the local railway administration in order to comply with the local track layout specialities and with legacy signaling systems to which they interface. As a result of this bespoke approach the methods of testing are currently diverse and act as one of the barriers to the introduction of a uniform interlocking product. In addition they tend to be inefficient because:

- many tests carried out on-site manually might be executed in lab or in factory – easier or even automatically,
- testing requirements are further subdivided into special / specific test processes or test procedures and test cases for each product,
- and because many test cases and procedures overlap and repeat the same or similar actions in different phases of testing and commissioning, thus testing the same functions of the interlocking repetitively.

On the other hand, those many testing methods have evolved into several main approaches which tend to be similar among many European manufacturers. Some of the smaller manufacturers have not faced the problems of the explosion of route variations, numbers of different interfaces to various signaling elements and legacy electromechanical and relay systems, but large manufacturers cope with similar problems and challenges. Therefore all of those large companies need to apply laboratory testing with automatic test beds and simulators, factory testing using mock-ups and dummies and, finally, on-site test methods which must at least follow national standards which typically define a list of mandatory test procedures. Also, different approaches focus differently to both technical and functional safety and to the overall functionality of the supplied interlocking. But the fact is that variations in the scale and ratio of those three basic approaches differ substantially among all manufacturers but with considerable influence coming from the railway network (and the associated signalling standards, infrastructure manager requirements and the relevant railway authority rules and customs) where the interlocking is installed.

To provide an introduction to the actual current methodologies and ‘state-of-the-art’, this chapter will summarise the previous work in this Workstream of the INESS project. The outcome of this work was reported in the deliverable [1].

In the previous work package the state of the art in testing and commissioning was examined through a series of structured interviews with manufacturers and railway administrations. These interviews were supported by a questionnaire provided to the partners before the interview.

An examination of the raw data has been carried out and supplemented by further enquires to provide a considered view on the state of the art. The information has been split into the following sub-headings for consistency with the later sections of the handbook.

- Factory and/or Laboratory testing
- On-site testing

The subsections describe the current testing and commissioning processes of the suppliers and the railway administration on a general and qualitative level. A quantitative evaluation of the efficiency of the process will not be made, because the basis of the data gathered by the interviews is not detailed enough to prepare such information.

3.1.1 Factory / Laboratory Testing

This section provides a summary description concerning a qualitative approach to factory testing. The main data was obtained from the interviews held at the beginning of the project in tasks F1 and F2 and from deliverable D.F.2M 'State of the Art Report'. This information has been enhanced with the expertise of the industrial partners involved in this task.

The questionnaire was divided into three sections to address three different process areas within test and commissioning:

- Part 1: Accreditation process of a railway signalling system.
- Part 2: Requirements from the railway administration in order to acquire a signalling system.
- Part 3: Description of the steps once a signalling system is approved by a railway administration until it is installed in a railway line and it is accepted by the relevant authorities.

Information was obtained from 12 suppliers through interview. The transcripts of these interviews have been re-read and re-evaluated with a different point of view from the original analysis. Instead of trying to obtain quantitative results, a qualitative approach has been adopted to understand the testing processes that are carried out in the factory or laboratory.

A summary is presented in the following paragraphs of the results of the reanalysis.

3.1.1.1 Accreditation process of a railway signalling system

This section summarises the data gathered concerning the process of designing a new interlocking and the process of getting a 'compliant label' according to the prevailing standards.

CENELEC standards (EN 50126, 50128, 50129) are followed by each supplier. These standards and the procedures implemented in order to follow them are well established and some suppliers choose to follow these CENELEC procedures even when they are not required to do so; usually as part of projects outside Europe.

The V model referred in the standards is widely used as well as the definitions of 'generic product', 'generic application' and 'specific application'. It is also common to engage an independent assessor to assess safety related issues. Most companies (8 out of 12) have their own Independent Safety Assessor (ISA) department that is independent from the rest of the company and they hire an external ISA when requested by the client or safety authority to increase the level of independence.

Regarding test facilities, most of the suppliers carry out their tests in their own facilities but also perform field tests; mostly with a safety related background. Environmental tests (like EMI) are sometimes outsourced to specialist companies mainly by small companies that don't have their own specialised EMI facilities.

For many of the suppliers interviewed, testing processes are defined in the standards as verification and validation processes according to CENELEC standards. The definition of these two words, according to the standards (e.g. EN50129), is:

- Validation: the activity applied in order to demonstrate, by test and analysis that the product meets in all respects its specified requirements.
- Verification: the activity of determination, by analysis and test, at each phase of the life-cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements.

For other suppliers, testing is only related to verification as defined in the standards.

Finally, referring to the Quality Assessment (QA) procedures, each one of the suppliers interviewed implements their procedures according to one QA being ISO 9001 and IRIS (International Railway Industry Standard) the most mentioned. All of the suppliers answered that in order to obtain the 'compliant label' they have to follow a quality assurance process.

3.1.1.2 Requirements from the railway administration in order to acquire a signalling system

This section of the questionnaire is intended to obtain information regarding which other requirements apart from fulfilling the CENELEC standards are required in order to become an authorized interlocking supplier for a Railway Administration.

A supplementary aim of this subsection is to understand the role testing in these additional requirements.

Apart from those CENELEC requirements that are mandatory in EU, there are specific national standards that have to be fulfilled like EMC regulations or environmental regulations, which are local interpretations of EU wide directives. In almost every case, the standards and procedures that have to be followed are well defined and Railway Administrations state these norms in contract documentation order to establish a guideline for its suppliers.

Tests are performed in order to provide evidence of functionality, safety and reliability of the interlocking. Most tests are related to CENELEC standards. There are some special occasions, i.e. a new high speed line, in which equipment is thoroughly tested beyond the standards as a special requirement from the Administration.

Most of the tests performed in this phase of the development are performed in the premises of the suppliers. Some of them can be carried out in the Railway Administration premises if required, or in other laboratories, mainly for environmental or EMC testing, but this is an exception. Some outsourced personnel can be hired for these testing processes, but they are managed according to the internal procedures as if they were hired directly by the company.

There are quite a few in-house developed software tools dedicated to testing processes. There are also some commercial applications used for software checking and software quality assurance as part of the test and commissioning process.

Tests are normally required to demonstrate the fulfilment of the functional requirements of the supplier's equipment and for verification of safety requirements. Suppliers have to give evidence to the Railway Administration of the standards, procedures followed and fulfilment of requirements.

Cross acceptance is not usual. Sometimes safety evidence can be used for cross acceptance, but since most of time new functionality is required by the different Railway Administrations which usually affects the safety case, the evidence has to be obtained afresh in order to give the specific safety evidence for the product.

The Railway Administrations supervise the delivered information, procedures and evidence and sometimes take part in some testing procedures.

3.1.1.3 Description of the steps once a signalling system is approved by a railway administration until it is installed in a railway line and is accepted by the relevant authorities

This phase comprises those activities that take place once an interlocking system has been acquired by a railway administration until it is fully installed and brought into use to control trains and the role that testing has in this whole process.

All interviewed suppliers follow a CENELEC process for the specific application, from engineering through development, installation, acceptance, commissioning and operation & maintenance. V&V sup-

port can be required for all phases. The main difference between them is where they put the border between generic product-application and specific application and this can vary from project to project.

Regarding the testing activities most of the suppliers perform tests in the laboratory and onsite. There are also some formal tests performed with the Railway infrastructure manager to accept the system, known as factory acceptance tests (FAT).

The tests performed for this phase mainly include functional and safety tests. More than half of the suppliers interviewed also perform HW and SW tests at this stage while the others consider them as part of the FAT (generic product tests).

HW and SW tests performed in the laboratory generally include the use of tools developed by the supplier with different degrees of automation depending on the supplier.

The functional tests consist mainly of testing the control table and the incompatibilities in the laboratory. Further, tests are done onsite normally together with the Railway administration.

3.1.2 On-site testing

The on-site testing is an important step during the commissioning phase of an interlocking. Currently this takes place throughout the installation and commissioning phase of every interlocking project. Generally there are two forms of testing logical and connectivity to demonstrate that it has been connected correctly and the internal logical relationships are correct for the application. This means, that every railway administration and each supplier is involved in on-site testing during their interlocking projects.

The amount of required testing varies considerably. Testing depends on the size of the interlocking project, as well the development processes of the supplier. The answers from the interviews about the state of the art in testing and commissioning suggest that there are differences in the testing process.

Railway administrations are involved in the testing and commissioning phase of an interlocking as well as the supplier. Whilst the physical testing is inevitably undertaken by the supplier the railway administration maintains an active oversight of the process as the body that is accountable for the safety of the operation of the asset.

3.1.2.1 SME supplier

During the first tasks of the Workstream F, three SME suppliers were interviewed about their methods and processes for testing and commissioning an interlocking system. All three companies are situated in Germany, dealing with international, mostly European interlocking projects.

The smaller suppliers do their testing in the own laboratories, on-site only the connection and the cables are tested. Functional tests as well as safety tests are performed only in the laboratories. The same can be said for the hard and software tests. The smaller suppliers have optimized their testing processes by minimizing on-site testing, the way INESS intends it in the issues of this work stream.

The supplier builds up the complete interlocking connected with sample field elements, such as a signal, a switch motor, etc. in the laboratory. With this configuration all functional, software and safety tests can be performed. The testing is supported to some extend by in-house tools, which were developed with a few exemptions by the supplier itself. Environmental tests are sometimes outsourced to engineering companies or universities, since these facilities are not available at the supplier.

After achieving the Factory Acceptance Test (FAT) and by this finishing the laboratory test processes, the three SME suppliers have nearly the same steps to be performed next:

- Delivery from the factory to the site
- Installation on-site
- Verification tests on-site, including Allocation Test
- System / Installation Acceptance by the Railway Administration

After completing the in-house laboratory tests, the interlocking is disassembled, packed and transported in pre-defined components to the site. There the interlocking is assembled again and connected to the field elements.

After the installation of the interlocking system the cable and allocation tests are performed.

The positive effect of this laboratory process approach is the reproducibility of the test conditions, especially for bug tracing. In addition, the number of persons needed for the tests can be minimized both for the laboratory tests and the on-site commissioning phase.

The on-site commissioning phase itself is very short and can completed in only few days for one interlocking system and extending to several weeks for a whole line with many interlocking systems. This very short time needed for commissioning of an interlocking systems based on the fact that virtually all

functional and safety test process is undertaken in the laboratory. Therefore those time consuming tests, are performed before the supplier's equipment leaves the laboratory for the site.

Looking at this, the testing process of the SME suppliers is optimized with respect to minimizing the effort and time spent on-site. But on the other hand this testing is only reasonable for smaller interlocking systems, since the system needs to be built up completely in the laboratory, which may not be possible for interlocking systems for more complex layouts. This conclusion is drawn from the answers given in the interview stating that a very short time period of two days can only be reached, when the interlocking consists of about 10 devices. When extending the interlocking system or installing an interlocking system for more than one station, as referred to by an interviewee citing a project with five stations, the time needed for the commissioning will grow up to two weeks.

3.1.2.2 Big supplier companies

In addition to the three SME suppliers, nine big supplier companies were interviewed.

In contrast to the above described testing process, the bigger suppliers do most of their testing work on-site. In the laboratories mostly only the interlocking software is tested. The whole procedures of testing functionality, safety, etc. are done on-site.

This could be due to the size of the interlocking projects, which do not currently allow or make it possible to build up the whole interlocking including sample field elements in a laboratory. Therefore only a small part of the testing is done off-site and supported by tools, because most of the on-site processes are not supportable by tools.

The most used "tool" on-site is the human, which means, the on-site testing is very skilled human intensive activity and therefore highly expensive. Whether it was a railway administration or a supplier, both give a total number up to some hundred persons that are needed to test and commission an interlocking system on-site. This is due to the fact, that for the functional tests, every field element - signal, switch or other movable elements – needs to be manned by one person, which can give feedback during testing. Mostly the needed personnel came from the suppliers - directly or indirectly by subcontracting other companies.

The time that is needed to conduct the on-site testing varies highly from one weekend, as said by one German and one Spanish supplier, up to four months in the UK. This last value matches with the duration stated by NetworkRail.

An explanation for this variation in the duration of the testing process on-site was not given by the answers of the interviews.

3.1.2.3 Railway administrations

In the interview phase of the Workstream F six railway administrations were questioned about their state of the art methods and tooling with respect to the testing and commissioning of an interlocking. All the railway administrations explained that they take part in the testing of the interlocking. Most of the railway administrations test the majority of the system in the laboratories. Only Deutsche Bahn (Germany) and Banverket (Sweden) – renamed now in Trafikverket – do only the half or much less than that of the testing in the laboratory.

The way of prescribing the testing processes also differs highly. In most railway administrations the amount of tests and the tests itself depends on the specification and the functionality of the specific interlocking; consequently the catalogue of test cases and sequences to be carried out differs from project to project. This is the case for the majority of the railway administrations, which were interviewed. Again the exceptions are Germany and Sweden. These two railway administration have a testing catalogue, coming out of regulation. In Germany the testing catalogue is defined in a company regulation (KoRil892). Trafikverket specifies the needed testing procedures by national regulations.

Through the specification mechanism, the railway administrations have a big influence in the cost structure of the testing and commissioning phase.

But the main parts of the testing procedure are nearly the same all over the six railway administrations. All expect to get evidence of the implementation by testing to validate

- the correct connection of the interlocking system with the field elements,
- the correct and complete functionality of the interlocking system (hard and/or software),
- the safety functions

The testing procedure is carried out without tool support, meaning that none of the railway administrations have given any detail in this. Only ProRail (The Netherlands) has given the explicit answer that no automated tool is used for performing the testing. For the railway administration, as well as for the suppliers, the human being is the most important “tool” for testing work on-site.

The time needed for the test and commissioning phase of an interlocking system varies from very short terms, such as stated by Trafikverket and ProRail, which need one or two weekends on-site, up to 4 months on-site work as reported for the UK by NetworkRail. An explanation for such a difference in the duration of the on-site works was not given in the answers of the interview.

3.1.2.3 Summary of the state of the art in on-site testing

The on-site testing plays an important role during the commissioning phase of an interlocking. All companies which were questioned perform testing work on the track before they put an interlocking system into operation, but the amount of testing varies considerably between the companies. There is a range of time for on-site testing between one weekend (SME supplier) and up to four months (UK). A partial explanation for this can be found in the approach to testing an interlocking system. SME suppliers do the whole functional testing in the laboratory within the Factory Acceptance Test. On-site only the validation and allocation tests were performed. The big supplier companies in contrast, do a lot of functional testing on-site, which is time consuming.

In the case of on-site testing the suppliers have not given any information of the usage of automated tools, this lack of information can be interpreted no automated tools are used during the on-site testing phase. The human is the most important tool on-site. This fact helps explain why the on-site testing is expensive.

In the end this leads to the conclusion that testing of interlocking systems on-site is not efficient with respect to the time and money as opposed to performing these tests in the laboratories/factories. The testing and commissioning process for interlocking systems offers many possibilities for optimization with respect to the assignment of personnel, tool support and implemented methodologies.

3.2 Testing methodologies

3.2.1 Reduction of field tests by increasing laboratory tests

In order to validate the interoperability of INESS interlocking components they could be tested on a real track but the costs and effort are very high, because a test train has to be moved to the track, the trips have to be arranged with daily traffic or the line has to be blocked for the regular traffic, etc. That is the reason why the main focus for assuring that new railway components i.e. interlocking, other trackside or onboard equipment, will work correctly is laid on testing beside the real railway environment. This could be done by using “hardware-in-the-loop” tests inside a test laboratory.

The benefits of using a laboratory for implementation of hardware tests are that it is possible to perform various tests under the same or equal conditions, tests are repeatable and the laboratory environment is flexible for different components. In order to save costs it seems necessary as a first step to check the conformity and inter-changeability of new INESS interlocking components in a laboratory as well as to check if they are in line with the requirements of the INESS specification.

3.2.1.1 Generic methodology for creation of laboratory tests

Before a technical system like the INESS interlocking environment can be tested the first step should be the generation of testable test cases and scenarios.

For each new technical system the specification must be summarized in a functional requirements list. This list of requirements is the basis for every test procedure. To prepare test cases a test case compiler needs to select the requirements from the reference list, extract them from a textual description and convert them into machine readable and executable form before transmission to the test machine as executable test cases.

It is useful to divide the requirements into functional groups or features. The benefit of using a traceability matrix is to ensure that each requirement from the list of requirements is covered in at least one test case.

The most complex problems of testing are

- the question of covering all possible combinations (usually of routes and signals) and the way to minimize the necessary test set,
- how to cover the prohibited situations/combinations to test the safety reaction. – the requirements not always cover this – so there is a question whether the test cases cover to 100% the requirements or whether it covers 100% of possible faults, or both, which has to be the main goal.

To convert the test cases into a dedicated test scenario it is necessary that the test cases are prepared by the test case compiler in a templated form capable of having parameters assigned. That means that it is possible to test a variable number of combinations within only one test case. For example a test case which includes the testing of a signal perhaps needs to be prepared for testing main signals and also for testing combined signals.

Additionally the possible position inside the test track layout of the test scenario must be selectable. Hence one test case template can cover similar requirements. With the combination of test cases of the test case catalogue it is possible to create different scenarios under usage of different test cases and different requirements. The following general figure depicts the dependencies between the functional requirements, the test cases and the test scenarios.

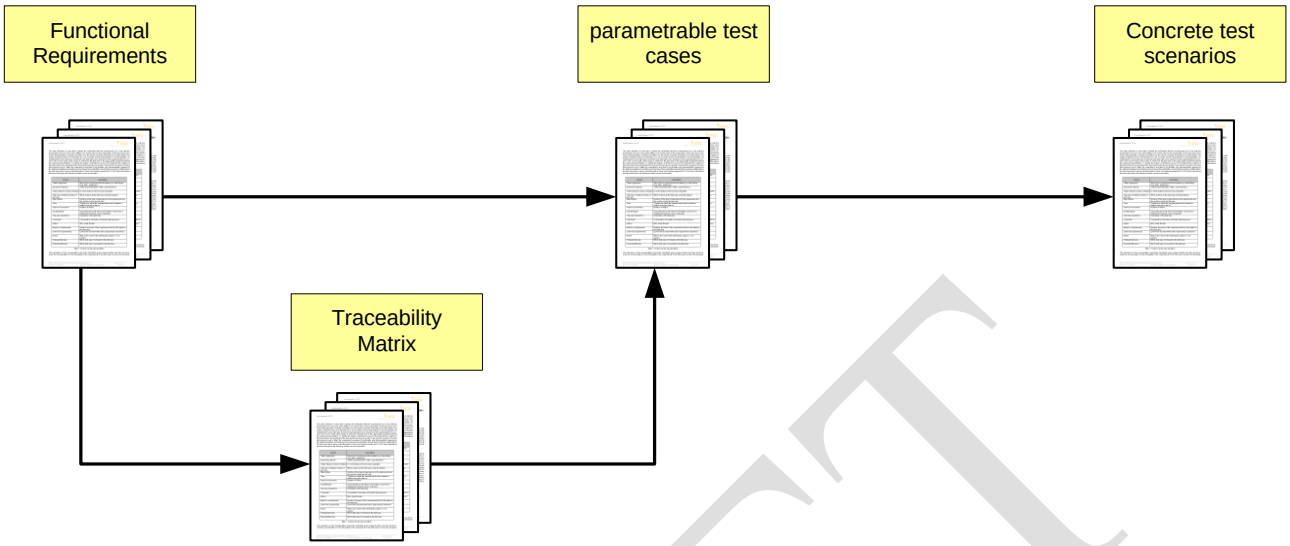


Figure 1: General creation of a test case

The main objective of every test is always the verification that the requirements are in line with the specification and also have been fulfilled. The formal rules for the preparation of the test cases must ensure that the description contains information for the clear coverage of test traces and test results.

It is necessary that in every test case document each test case has a reference to the requirement to be covered. This can be assured by a link from the test case to the appropriate requirement inside the referenced specification.

To handle the system verification process for the trackside the creation of test cases is required. They should be used to show the test purposes of how to attain the requirement coverage of functionality and inter-changeability. Agreeing to the defined objectives, manufactures should have the possibility to specify test procedures additionally to the test cases which allow conducting tests for their own trackside equipment.

For the INESS interlocking test case description the following content can be documented:

Column	Description
Tested equipment	Sort of equipment which will be tested (e.g. Interlocking, LEU, RBC, Switch etc.)
Operator (Optional)	traffic superintendent or 'RBC' superintendent
Tested feature/ number of feature	features the test case is separated in
Test case of feature/ number of test case	number of the test case inside the feature
Step number	number of the step in dependency of the requirement and the position inside the test case
Time	the time on which the requirement should be tested or fulfilled during the test run
Version of document	number of version
Inputs/Outputs	inputs (IN) which will influence the tested component or outputs (OUT) which can be evaluated
Test case description	description of the test case
Comments	comments for the tester of the test case/sequence
Author	creator of the test
Based on requirements	number and name of the requirement which is the basis for this test case
Link to the requirements	link to the document where the requirement is described
Result	result of the test, e.g. 'passed' or 'not passed'
Followed test case	test case which is followed by the test case
Preceded test case	test case which is preceded by the test case

Table 1: Content of a feasible test case description

This description of the documentation should be formalized under usage of tables. They should include the documentation for the traceability of the requirements to the test cases as well as the traceability of the tested features to the test sequence which is the summary of a set of test cases.

Functionalities which are often tested in the same constellation in different and similar features/test cases should be merged into own features/test cases. The advantage of this method is that the features need to be tested only once and every requirement is covered. These features can be used to implement them into other test cases of other features.

There is a reference needed to the other features which allows the usage of a complete feature with a complete test case procedure as a 'sub-feature' within another feature. If a test sequence is prepared with this methodology during the test run the 'sub-feature' will be covered automatically within the feature where it is included. The following figure shows the dependencies for this process.

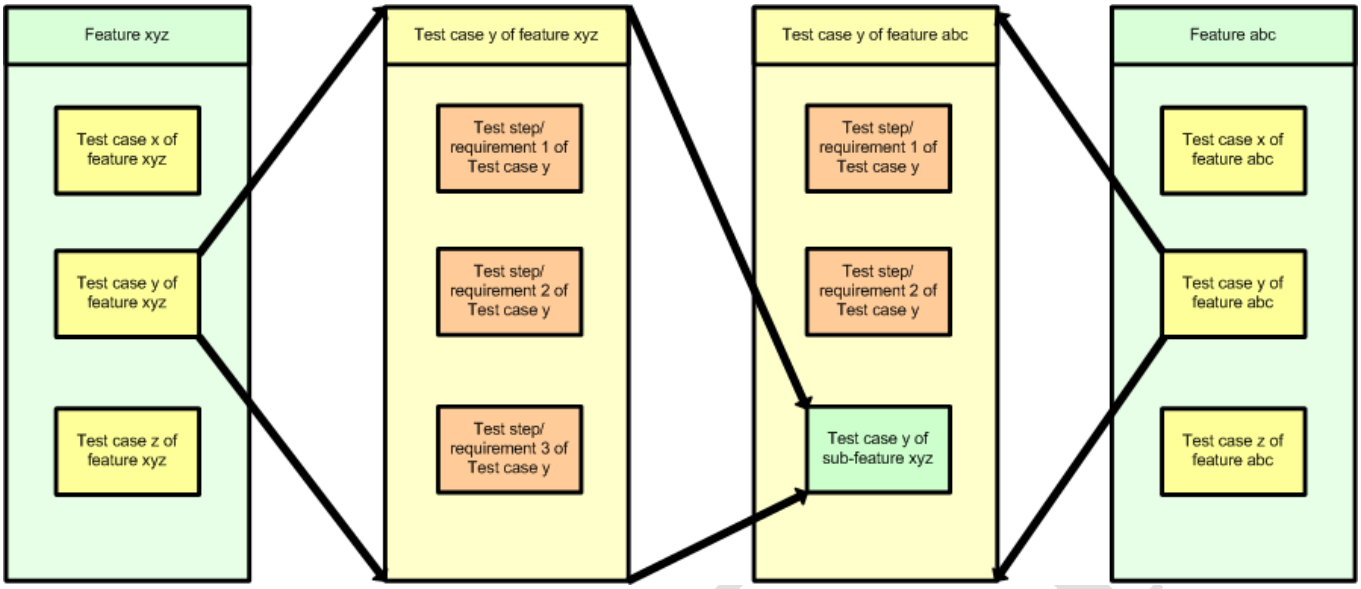


Figure 2: Feature and Sub-Feature

On this basis test features within the test cases can be combined to complete test sequences or for real tests on a real track to test trips. The whole set of test sequences cover each test case at least once to ensure that each requirement is fulfilled.

3.2.1.2 Interoperability based testing

Interoperability is a main topic for the implementation of a European-wide rail transportation system between the different European countries which are using different components from different suppliers. To ensure the interoperability, test cases must be implemented which are created focussing on the assurance that the formal rules of the European railway operators are well conceived. A formalisation of the process ensures that a unitary and matchable basis for the creation of test cases will be implemented. It is also a tool to generate automatically performable tests and to ensure that test results will be available in a unified format for the test evaluation.

To ensure that different components of different manufactures work with each other and do this in a correct manner (e.g. trackside component of manufacturer A with onboard unit of manufacturer B) the members of UNISIG created the IOP (Interoperability) test specification.

The features of the specification are:

- The track and train side components are produced by different manufacturers.
- There are only the interfaces between the systems which are testable for a tester.
- The test is only at the interfaces to the system e.g. the DMI to the driver or the button surface for the signal man and the logging of the interfaces.

The tests are not created to test only individual components of the manufacturers or to test only completely equipped tracks of the operators as individual items. They are used to check the integration process between them. The focus is on the correct interaction and the correct behaviour of the used components (train- and track side). Thus, it is guaranteed that the test cases will be consistent and at the same time minimizing the testing effort as well as maximizing the benefit avoiding overlapping and repeated tests of contents.

The following figure illustrates the suggested stepwise methodology and approach for testing technical, line-specific and operational requirements and the interaction and collaboration of the different components.

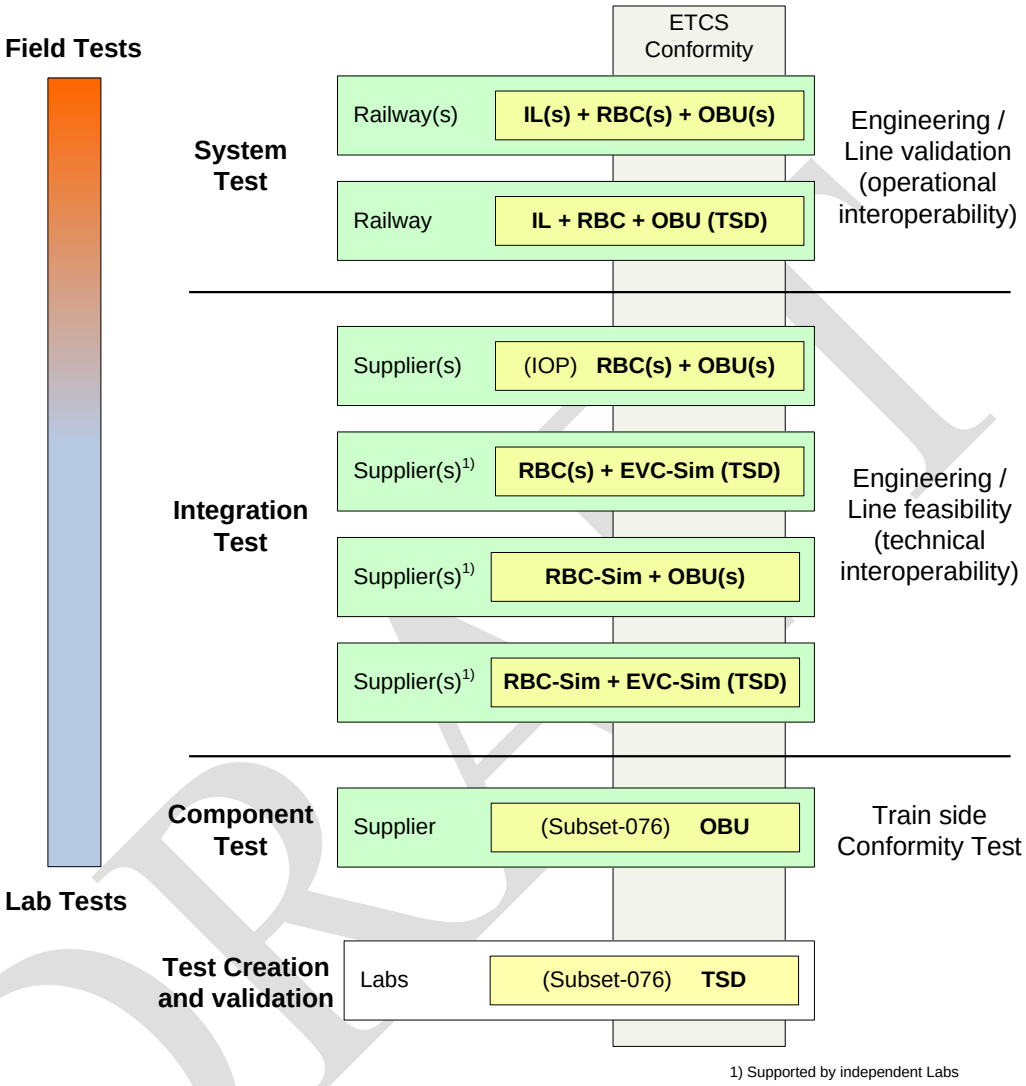


Figure 3: Proposed test phases and levels of detail in the development process

For instance an ETCS onboard unit (OBU/EVC) will be tested on component level using the conformity and interoperability test standard for ETCS onboard units (Subset-076) and Reference Test Architecture with the Test Sequence Debugger (TSD) in order to approve the compliance and conformity against the SRS for ERTMS/ETCS.

The technical interoperability of train- and trackside components, i.e. EVC and RBC, will be checked also in a laboratory on the integration level. At least operational line-specific tests can show the feasibility and suitability on system level including all parts of the whole system also in a laboratory.

The EVC and ETCS conformity approval on component level and its use through the different layers will ensure compliance and consistency between the operational requirements of the railway undertaking and the technical requirements of the SRS. With the different levels of the ETCS conformity as basis it is guaranteed that ETCS is inside all the other levels above.

3.2.1.3 Common Methodology of testing for operational tests

Beside the defined technology, operational tests also define the interaction between technology, operational actors (e.g. dispatcher, interlocking or train driver) and operational rules (guidelines and regulations) as extension to the technical test.

The technical test cases deal with the functions of the train side (RBC; Interlocking; OBU etc.) but even though technical functions of the trackside are defined, there are also operational procedures needed and tested.

In the following picture the context between operational and technical documents is illustrated. The operational level is based on the technical level.

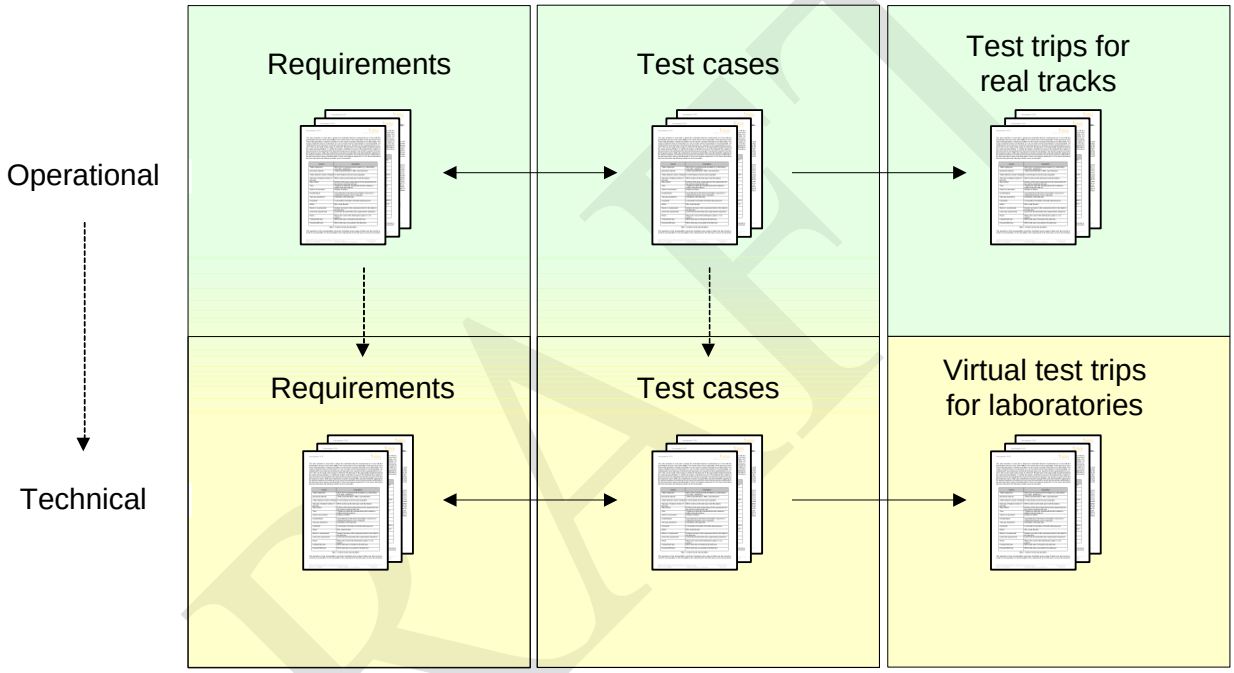


Figure 4: Generation of operational tests

The figure shows the method for the generation of operational tests. There is a split between the operational (requirements, test cases and test trips) and technical side (interlocking requirements, interlocking test cases and virtual test trips). The technical test cases are used as basis for the operational test cases due to fact that the requirements for operational test cases are complementary to technical requirements. The operational requirements can be used to create test cases including and extending the technical test cases. Based on those operational test cases test trips for real tracks can be prepared. It is also possible to prepare operational test trips according to the specific aspects of a newly equipped track, like the usage of ETCS levels (e.g. Level 1, 2 or Level 1/2) or modes (e.g. Shunting, Non leading) and functionalities.

The advantage of the technical basis of the operational test cases is that the operational test cases can be compared with

- technical test cases,
- technical features and requirements and
- operational test cases

of other railway undertakings. Thus, a safe operation without deviations between operational and technical requirements is ensured and inconsistencies can be found, e.g. if there is an operational test case that does not fit to include and extend any existing technical test case using it as underlying base.

3.2.2 Modularised Interlocking

In the last chapter it was pointed out that interoperability as one of the important goals of the entire European railway system depends on two key issues

a. ensuring the technical and operational interoperability of railway subsystems, i.e. ensuring the conformity and consistency of the requirements related to the specifications and requirements on component, integration and system level and
b. managing the different line specific and operational requirements.

The methodology to create test cases and test scenarios was explained in the last section, whereas this section will show what types of modularisation could be beneficial and how module testing can look like.

3.2.2.1 Benefits of a modularised interlocking with respect to testing

The main focus of INESS is to test or to perform the test methodology for an interlocking system. Interlocking systems can be divided in different sub systems like the equipment outside at the track e.g. point machine, signals, track occupancy detector, wires to the components and the RBC.

A modularised interlocking system could be based on the following schema of components:

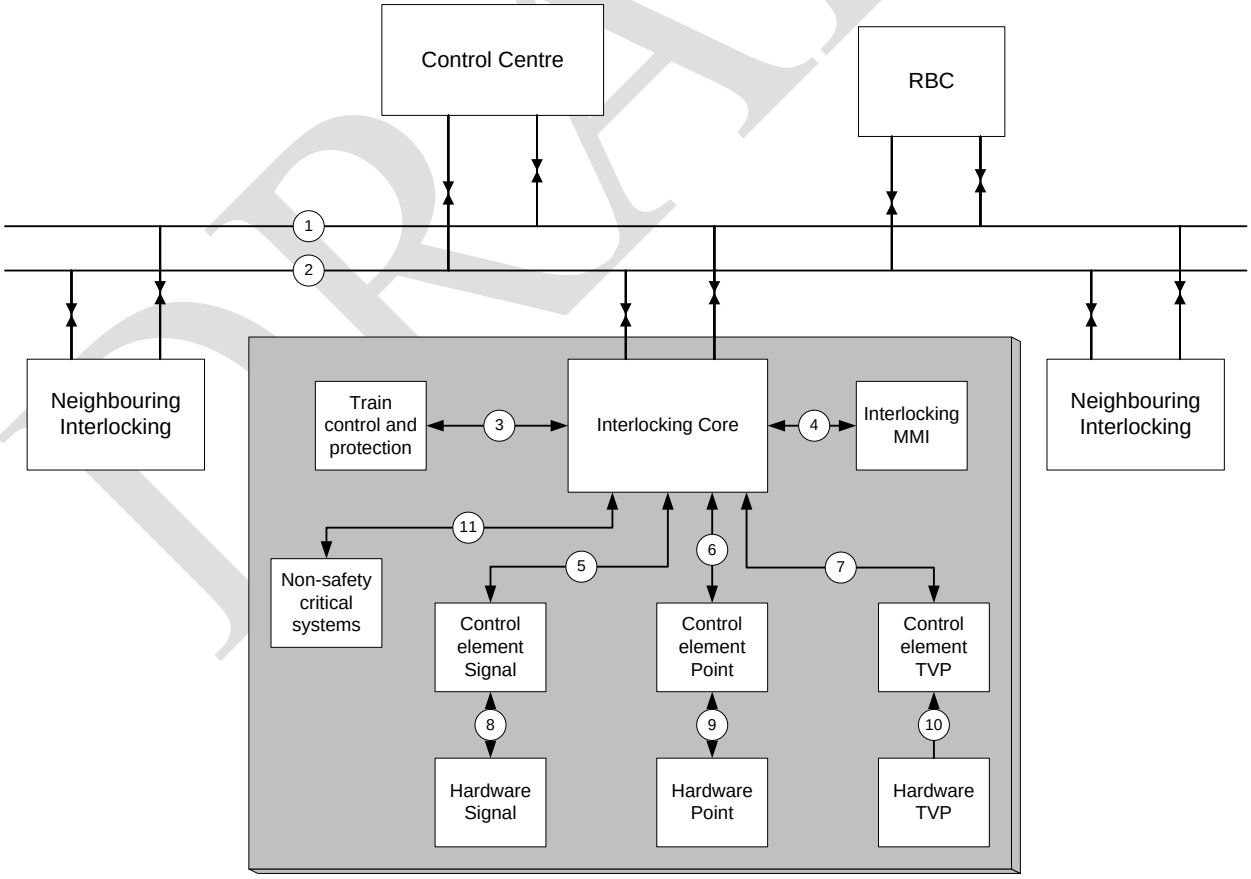


Figure 5: Generic structure of a modularised interlocking system

The displayed components are described as followed:

Element	Description
Interlocking Core	The core element of the interlocking system, in which the safety and security relevant functionalities are processed. This can be designed by using the specifications of the INESS interlocking core system developed by Work-streams D and E.
Interlocking MMI	Display and operation interface of the interlocking system. This can be either a regularly used interface within the interlocking environment or an interface only used in degraded situations in an environment where the regular operation of the interlocking is done in a Control Centre.
Control element x	Controlling unit for translating the signals coming from the interlocking core into a protocol or values transferrable to the respective field element. The Control Element also provides the status and diagnostic information of the respective field element to the interlocking core.
Hardware x	Hardware of the respective field element, for example for the signal: signal post, signal lamps, etc.
Train control and protection	Element containing all parts and systems needed for realising the train control and protection, such as balises, track circuits, magnets, etc.
Non-safety critical systems	Element containing all systems of the interlocking system, which are working without any safety relevance, such as train number information systems, announcement systems for platforms, etc.
Control Centre	Control centre for a number of interlocking systems in a centralised control and command structure of a railway administration
Neighbouring Interlocking	Next interlocking system on the line which is connected to the INESS interlocking. This interlocking can either be an INESS interlocking as well or a conventional interlocking system.
RBC	Radio Block Centre as part of ETCS.

Table 2: Caption of the Generic structure of a modularised interlocking system

In addition to the described modules a number of interfaces are included in the generic modularisation structure as well. The interfaces of a sample generic structure are displayed in Table 3.

Keeping testing in mind, the modularisation of an interlocking system is beneficial due to the fact that the modules are standardised elements and represent each a kind of a generic sample.

The generic samples are specified and developed ideally using standardised requirements, for example the Interlocking following the INESS Requirements Specification developed by Workstream D and the INESS architecture created by Workstream E. These standardised elements need be tested for a special project on a generic level only once. After successful testing, the modularised elements can be integrated in the dedicated interlocking system as often as needed without any further functional and/or safety related testing effort. By using such an approach the testing effort for an interlocking system can be decreased significantly.

Interface number	Description
1	Interlocking Core ⇔ Control Centre / Neighbouring Interlocking /RBC (safe functionalities)
2	Interlocking Core ⇔ Control Centre / Neighbouring Interlocking /RBC (non safe functionalities)
3	Interlocking Core ⇔ Train Control and Protection System
4	Interlocking Core ⇔ Internal Interlocking MMI System
5	Interlocking Core ⇔ Control Element Signal
6	Interlocking Core ⇔ Control Element Point
7	Interlocking Core ⇔ Control Element Track Vacancy Proving (TVP)
8	Control Element Signal ⇔ Hardware Signal (Field Element)
9	Control Element Point⇔ Hardware Point (Field Element)
10	Control Element TVP ⇔ Hardware TVP (Field Element)
11	Interlocking Core ⇔ Non safety critical systems

Table 3: Description of the interfaces used in the generic structure of a modularised interlocking system

Keeping testing in mind, the modularisation of an interlocking system is beneficial due to the fact that the modules are standardised elements and represent a generic sample of each type of unit.

The generic samples are specified and developed ideally using standardised requirements, for example the Interlocking following the INESS Requirements Specification developed by Workstream D and the INESS architecture created by Workstream E. These standardised elements need be tested for a special project on a generic level only once. After successfully tested, the modularised elements can be integrated in the dedicated interlocking system as often as needed without any further functional and/or safety related testing effort. By using such an approach the testing effort for an interlocking system can be decreased significantly.

3.2.2.2 Modularisation scenarios for adapting the testing effort

The above described generic modularisation structure is a first step towards a standardised and cost saving approach for the development of interlocking systems with respect to testing efforts.

A further step in the direction of cost efficiency in testing will be done by selecting the modules in line with the needs of the respective project's plan. As a result different single modules are combined into a module block for a particular application. The adaption of the functionalities and the special circumstances of the interlocking project can be taken as the basis of the application's modularisation scenario.

There are different scenarios possible, reflecting the different designs of the interlocking system. For example controlling many field elements located close to each other like in the entrance section of a station (see section 3.2.2.2.1) or the control of decentralised field elements, such as the equipment of a line (see section 3.2.2.2.2). These two exemplary modularisation scenarios are described in the following two sections. The section 3.2.2.2.3 then will provide a comparison of the two scenarios with respect to the number of interfaces, which need to be tested. This allows a first qualitative assumption of potential effort savings.

3.2.2.2.1 Modularisation scenario A – Combined Control Elements (CCE)

The first scenario represents a schema with combined control elements. The scenario is shown in Figure 6.

All Control elements needed for controlling the part of the line are combined into one module. This combined module is connected with the interlocking core by only one interface on two channels (see number 12 in Figure 6) due to safety related protocols.

The different hardware elements at the track are directly connected to the combined control element by special interfaces as it is shown in the generic structure of the modularised interlocking system. This modularisation scenario is a schema well suited for the control of a station, where various points, signals etc. are located.

With respect to the testing effort this modularisation scenario will reduce the effort due to the minimisation of interfaces between the interlocking core and the control elements. In this scenario only one interface between the interlocking core and the control elements needs to be tested instead of three in the generic structure of the modularised interlocking system. This reduces the effort for the testing of this scenario by two interfaces.

To reduce the effort further, the standardisation of the protocol for this interface is recommended. By standardising this interface and its protocol the functionality and the safe design of the interface needs only to be tested once. This statement is valid for both positive as well as negative testing.

The different hardware elements at the track are directly connected to the combined control element by special interfaces as it is shown in the generic structure of the modularised interlocking system. This modularisation scenario is a schema well suited for the entering situation of a station, where various points, signals etc. are located as represented by the blue boxes in Figure 7.

With respect to the testing effort this modularisation scenario will reduce the effort due to the minimisation of interfaces between the interlocking core and the control elements.

In this scenario only one interface between the interlocking core and the control elements needs to be tested instead of three for the generic structure of the modularised interlocking system. This reduces the effort for the testing of this scenario by two interfaces. Since the new combined interface presumably needs to be more complex than the three ‘old’ ones the reduction will not be two thirds of the former effort of these three interfaces (see Table 4).

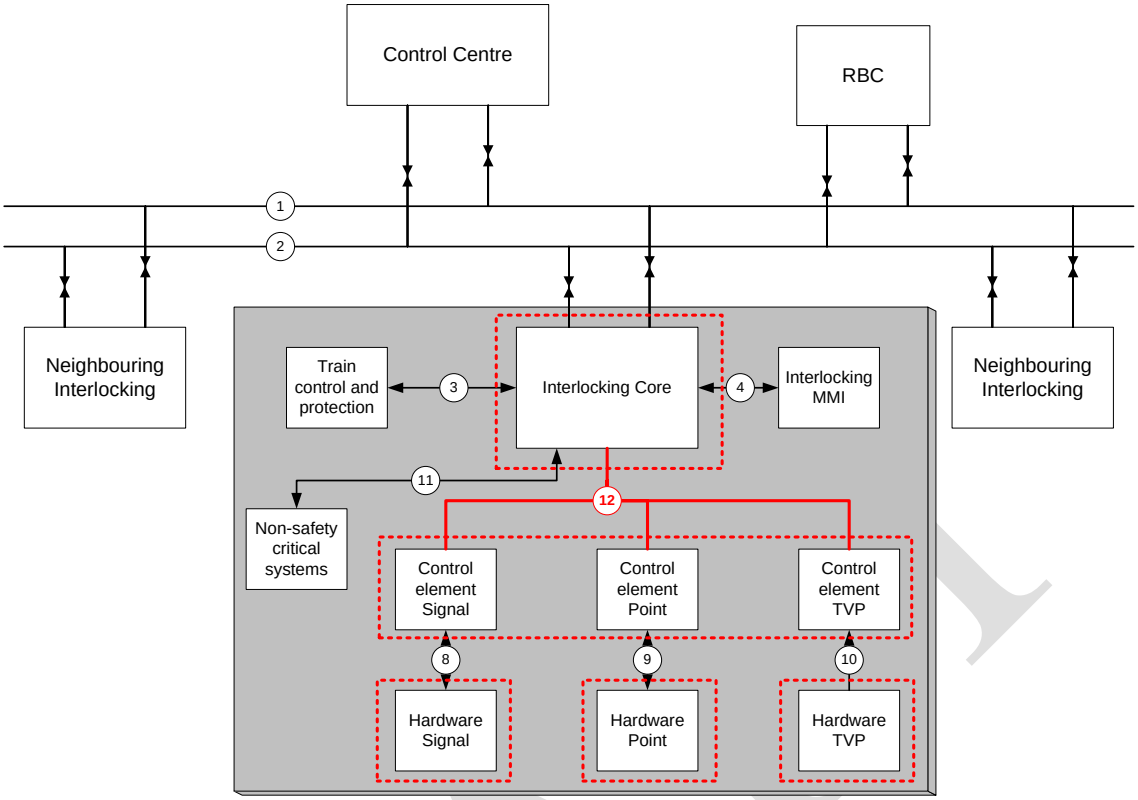


Figure 6: Structure of interlocking system for modularisation scenario CCE

To reduce the effort further, the standardisation of the protocol for this interface would be recommended. By standardising this interface and its protocol the functionality and the safe design of the interface needs only to be tested once. This statement is valid for both positive as well as negative testing.

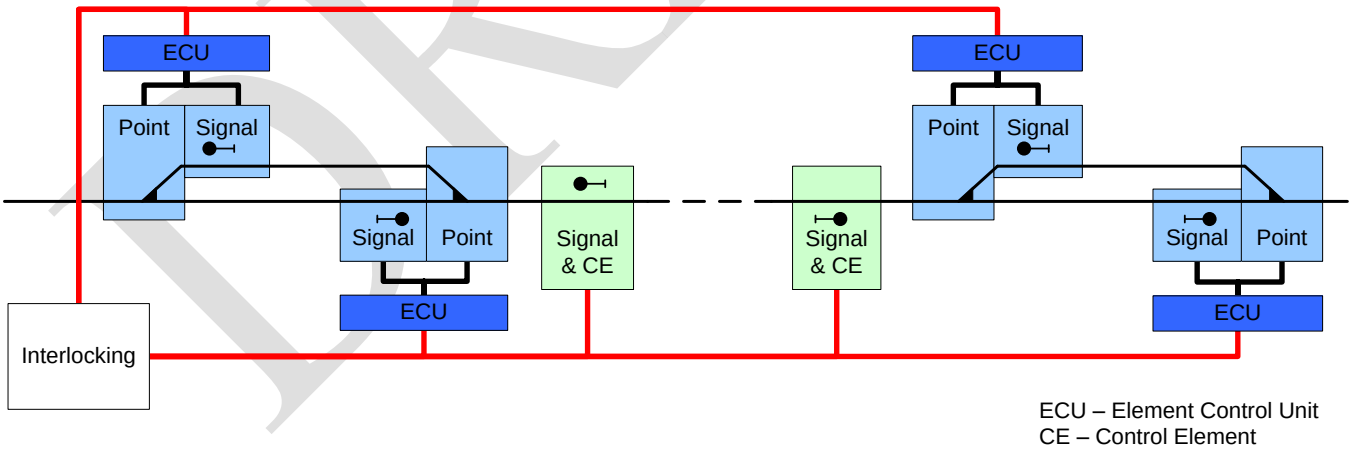


Figure 7: CCE (blue boxes) and IEHC (green boxes) integrated in an example track layout

3.2.2.2.2 Modularisation scenario B – Integrated Element Control & Hardware (IECH)

The second modularisation scenario is another adaptation of the generic architecture shown in Figure 5. The IECH scenario extends the CCE scenario by combining the Element Controller and the Hardware of the respective Field Element (see green box architecture in Figure 7).

The Control Element of the field element is directly connected to the hardware of the respective field element. Both modules form a unit, which can then be used for each field element on the line that is controlled by the interlocking system. The structure of this modularisation scenario is displayed in Figure 8. The connection to the Interlocking Core will be done by interface 13 and could be implemented for example by a BUS-line.

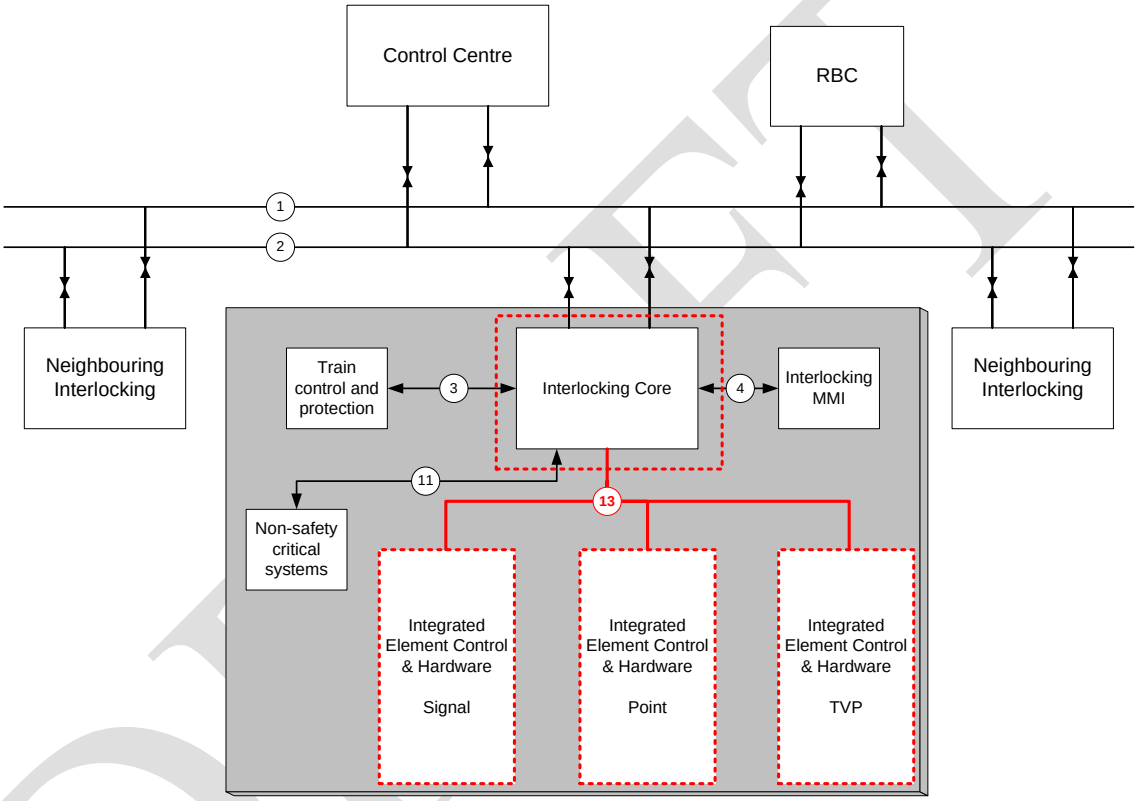


Figure 8: Structure of interlocking system for modularisation scenario IECH

The elimination of the physical interfaces between the Element Controller and the field element hardware has positive implications on the testing efforts. At first, as discussed in the section before, the new interface between the interlocking core and the Integrated Element Control & Hardware can be designed as one complex data bus interface. This interface needs to be specified and tested in the factory once and can then be implemented as often as needed for all used field elements.

Secondly the integration of the Control Element within the Field Element minimises the interface between the Control Element and the Field Element Hardware to an internal interface, ideally specified only as a software interface. Such a software interface can be easily tested in the laboratories of the supplier. After that step, the interface can be implemented in the unit and installed in the field. These testing can cover both functional and safety tests as well as positive and negative testing.

The reduction potential of this modularisation scenario with respect to testing effort will be presumably in minimum as high as stated for the CCE scenario. It might be possible to increase the saving potential due to the integrated approach of the Control Element with the Field Element Hardware. The integrated

approach reduces the number of physical interfaces by 5 in comparison to the Generic Structure of a modularised interlocking system (see Table 4).

3.2.2.2.3 Comparison of qualitative testing effort for the modularisation scenarios

The above described generic structure of a modularised interlocking system (see Figure 5 in section 3.2.2.1) and the modularisation scenarios CCE (see Figure 6 in section 3.2.2.2.1) and IECH (see Figure 8 in section 3.2.2.2.2) are designed to reduce the testing effort during development and commissioning of the system. The level of potential reduction varies between the three scenarios due to the number of included interfaces. An overview of the existing interfaces is given in Table 4.

Interface number	Generic	CCE	IECH
1	X	X	X
2	X	X	X
3	X	X	X
4	X	X	X
5	X		
6	X		
7	X		
8	X	X	
9	X	X	
10	X	X	
11	X	X	X
12		X	
13			X
Number of inter-faces to be tested	**11**	**9**	**6**

Table 4: Number of interfaces within the modularisation scenarios

The summary in Table 4 shows that the design of the modules of the interlocking system has an impact on the number of interfaces and therefore on the testing effort needed. The possibilities to combine modules into module units should be connected to the operational needs and conditions as described for the two example modularisation scenarios.

But it has to be considered that the reduction of interfaces by combining modules can not be interpreted as a 1 to 1 correlation with the effort reduction potential. Mostly the combination of modules goes in line with an increase of the complexity of the new created interface, which will need more testing effort than the old more simple interfaces. Meaning, replacement of three simple interfaces by one complex one will not lead to a reduction of effort by two thirds. The real decrease of the effort would be much lower.

3.2.2.4 Approach for testing a modularised interlocking system in a laboratory environment

To save time and money it is useful to test each component before a real track will be equipped. It is beneficial to test them by using hardware in the loop test in a rail component test laboratory. The components can be stimulated with pieces of information. This is the first technical test step for a track side conformity test.

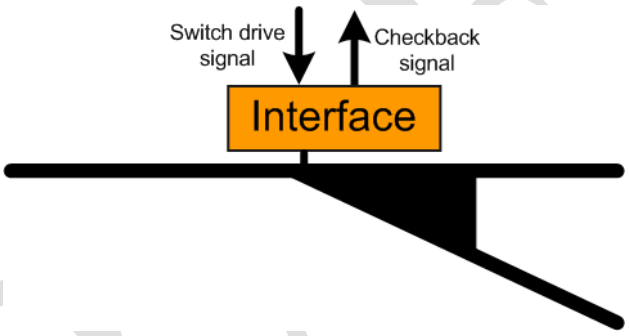


Figure 9: Simple example of a modularised switch

To stimulate the logic of each component, the interfaces to the dependent components, which are connected, must be clarified and specified. The interface specification includes the input and output information to the connected components. The expected behaviour for the communication is described within the requirement specification of the whole interlocking system. The test cases can be developed through the method used for the generation of test cases and the interlocking specification with the Requirements (see section 3.2.1).

Before a test run can be implemented it must be clarified, which kind of information of the component that has to be tested shall be stored and is needed to get checked for the trackside conformity test. The easiest form to depict is a switch that consists of a switch drive which receives information from the control computer and some pins which will give a feedback signal to the control computer that the switch has been detected in moved to the reverse or normal position. With this example, it can be shown that the test object which is in this case a really simple figured shape of a switch, needs to be stimulated by a testing environment with a defined input (from test case description) and the object shall answer with an expected output (from test case description). This information shall be stored within a log file as the proof that the component works correctly when driven by the interlocking.

This procedure for the preparation of the test cases and test sequences and the testing of the components of the interlocking system needs to be used for any component to be tested on component level.

The next step is to test the components at the integration level. This means that different components, which are modularised and have been checked during the first test run will be verified how they work with each other at the technical layer without operational tests. It is necessary to check if the inputs and outputs between the components under usage of the interfaces are in line with the specification and requirements. It is feasible to investigate this process including simulated and real components. So a real RBC which is connected with a real interlocking can be interfaced with a simulated Onboard Unit like the TSD. Or trackside components like a level crossings or signals can be simulated and only the control computer with its control panel and the RBC is real, all other components are simulated. Different combinations of real and simulated modules are feasible during the different test runs. The following figure shows a simple non detailed overview about one interlocking system and the possibilities to replace real and simulated modules during the test run within the integration level.

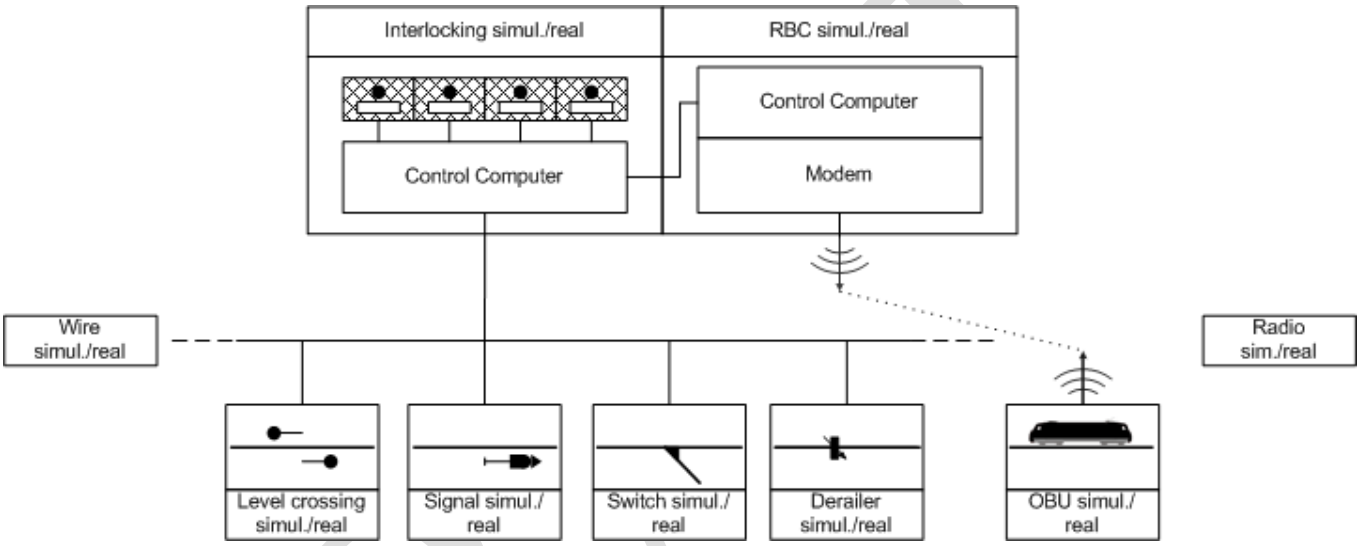


Figure 10: Integration test of technical modules

The next-to-last step is to check if, under testing conditions, different real and simulated components work with each other and are in line with the expected behaviour. This will be done by the usage of the requirements which are the basis to perform the test cases and test sequences.

The last level is to test that the components work together as a closed system and cover the technical and operational requirements. For this test it is useful to check the requirements at a complete track layout. This can be on a real track layout or in a laboratory with a simulated infrastructure. The tests should contain the requirements for the track including the kind of operation which will be realized. The focus is at the humans which are a part of the whole system like the signal man or the train driver.

3.2.3 Usage of industrial engineering methods

An area to explore to decrease the effort of testing the interlocking is the usage of industrial engineering methods. The following sections will give a short introduction of the ideas of the industrial engineering, the possible usage in the context of testing of interlocking systems and the adaption to INESS.

3.2.3.1 Principles of Industrial Engineering

Industrial engineering is a branch of engineering dealing with the optimization of complex processes or systems. It is concerned with the development, improvement, implementation and evaluation of integrated systems with the principles and methods of engineering design to specify, predict, and evaluate the results to be obtained from such systems or processes.

Its underlying concepts overlap considerably with certain business-oriented disciplines such as operations management, but the engineering side tends to emphasize extensive mathematical proficiency and usage of quantitative methods.

Efforts to apply science to the design of processes and of production systems were made by many people in the 19th and 20th centuries. They took some time to evolve and to be synthesized into disciplines that today would be labelled with names such as industrial engineering, production engineering, or systems engineering.

Further developments in industrial engineering and the more frequent usage of computer based tools have lead to the establishment of the “advanced Industrial Engineering” (aIE).

The aIE deals with the planning of networks, factories, processes, machines, equipment and the operational organization. It combines the basics of working and process planning - the original Industrial Engineering - with the methods, models for increasing the versatility and enhances them with the premise of continuous process chain, participatory planning and integrated planning process. Digital tools and methods as well as the potential of technology management complete the advanced industrial engineering scope.

The aIE makes a significant contribution of the computer-based simulation and visualization tools that are commonly grouped under the term "digital tools". The application of digital tools more or less permanently allows evaluation of processes before they are actually run by modelling, calculation and simulation to optimize and customize the structure of production. A common software platform for integration is crucial because the entire process from different employees from different areas such as process planning, material planning and logistics, layout, design, architecture, etc. is processed.

3.2.3.2 Adaption of the industrial engineering to the INESS testing processes

The "advanced Industrial Engineering" (AIE) is a general approach for optimization of complex technical procedures and processes. With regard to the testing of interlocking systems it can be applied to all process steps. Approaches for this are in the two previous sections already explained how the shift of test procedures in the laboratories of most manufacturers, and the modularization of the interlocking system into unified component, which can be used for all use cases again.

The optimization approaches taken so far cannot be described as falling under the aIE umbrella because they are considered only as individual measures. To fall under aIE they must be combined into an overall set of processes.

The implementation of the Industrial Engineering methods will result in an improvement of the previously discussed methodological improvements to create a greater impact. This area is concerned with the ideal combination of an advanced modularisation to optimise the test procedures in the laboratory.

The aim must be to reduce the effort for the testing of interlocking modules continuously. This can be done for example by identifying frequently recurring combinations of components of control centre and subject them to a development pre-test as combinations to create large modules to avoid further repetitive testing for the particular application.

The first step is to identify frequently used combinations of components and assemble them into larger modules accordingly. These combinations of components will probably be set up differently for each railway company, there are strong national interests in and requirements herein reflect on the basis of the tight coupling to the railway operations.

To show the methodology explained in the paragraphs above, the following three combinations are chosen:

a) Facing point movement
b) Trailing point movement
c) Crossover

These three cases will hereafter serve as examples to explain the procedure for creating the module combinations.

To illustrate the approach, exemplary module combinations were equipped with a simplified signaling system on the German model. This is for illustrative purposes only and does not claim universal validity or completeness.

a) Facing point movement

The facing point movement is the first combination of modules for implementing the aIE (see Figure 11). This scenario is generally part of each network of a railway administration all over Europe. For this scenario the following interlocking components are included:

1. Main Signals (A,N,M) only able to show proceed and stop aspects
2. Track vacancy proving, here using axle counters
3. Point

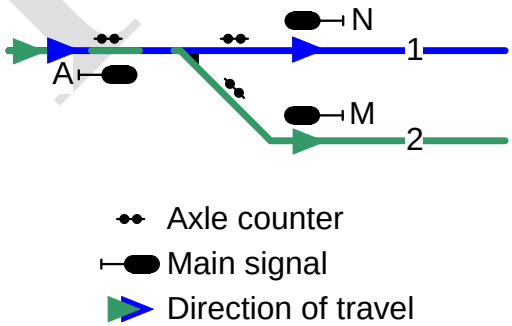


Figure 11: Elements of the „facing point movement" scenario

The following scenarios – positive as well as negative – need to be tested for this combination of modules:

I. Positive testing:

- Signal A only shall show a proceed aspect, when the signals N and M showing a stopping aspect, the point is locked in the end position and the point is not blocked (valid for the blue and the green travelling connection).
- The signals N and M have to show a stopping aspect as long as signal A shows the green aspect.
- The point must not be turned as long as signal A shows the proceed aspect.
- The point must not be unlocked as long as signal A shows the proceed aspect.

II. Negative testing:

- Signal A must immediately switch to a stopping aspect, when one of the following events occur:
  i. Signal N and/or M does not show the stop aspect any longer
  ii. Signal N and/or M reports a degraded mode to the interlocking
  iii. The point is no longer locked
  iv. The point reports a degraded mode to the interlocking
  v. The TVP section of the point is no longer reported as free.
  vi. The TVP section or one of the axle counters reports a degraded mode to the interlocking

b) Trailing point movement

The second combination of modules is a trailing point movement (see Figure 12). This scenario is generally part of each network of a railway administration all over Europe. For this scenario the following interlocking components are included:

1. Main Signals (B, O, P) only able to show proceed and stop aspects
2. Track vacancy proving, here using axle counters
3. Point

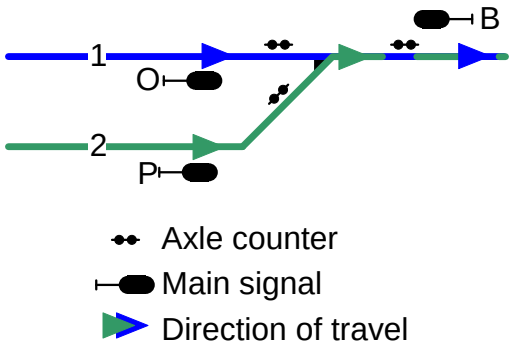


Figure 12: Elements of the "trailing point movement" scenario

The following scenarios need to be tested for this combination of modules:

I. Positive Testing:

- The Signal O only shall show the proceed aspect, as long as the signals P and B are showing a stop aspect, the point is locked in normal position and the point is not blocked (valid for the blue travelling connection).
- The Signal P only shall show the proceed aspect, as long as the signals O and B are showing a stop aspect, the point is locked in diverging position and the point is not blocked (valid for the green travelling connection).
- The signals P and B shall show a stop aspect as long as signal O is showing the proceed aspect.
- The signals O and B shall show a stop aspect as long as signal P is showing the proceed aspect.
- The point must not turn as long as signal O is showing the proceed aspect
- The point must not be unlocked as long as signal O is showing the proceed aspect
- The point must not turn as long as signal P is showing the proceed aspect.
- The point must not be unlocked as long as signal P is showing a proceed aspect
- The point has to be locked as long as signal O is showing the proceed aspect
- The point has to be locked as long as signal P is showing the proceed aspect.

II. Negative testing:

- Signal O must immediately switch to a stop aspect, when one of the following events occur:
    i. Signal B and/or P does not show the stop aspect any longer
    ii. Signal B and/or P reports a degraded mode to the interlocking
    iii. The point is no longer locked
    iv. The point reports a degraded mode to the interlocking
    v. The TVP section of the point is no longer reported as free.
    vi. The TVP section or one of the axle counters reports a degraded mode to the interlocking
- Signal P must immediately switch to a stop aspect, when one of the following events occur:
    vii. Signal B and/or O does not show the stop aspect any longer
    viii. Signal B and/or O reports a degraded mode to the interlocking
    ix. The point is no longer locked
    x. The point reports a degraded mode to the interlocking
    xi. The TVP section of the point is no longer reported as free.
    xii. The TVP section or one of the axle counters reports a degraded mode to the interlocking

c) Crossover

The third combination of modules is a crossover between two parallel tracks (see Figure 13). This scenario is generally part of each network of a railway administration all over Europe. For this scenario the following interlocking components are included:

1. Main Signals (S, T, U, V) only able to show proceed and stop aspects
2. Track vacancy proving, here using axle counters
3. Points a and b

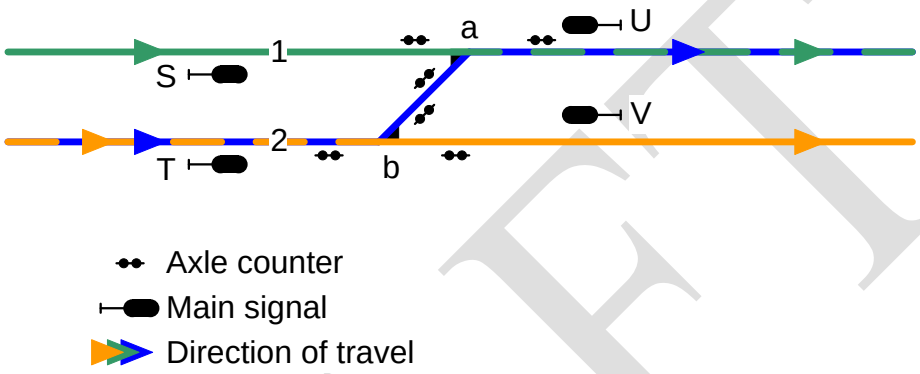


Figure 13: Elements of the "crossover" scenario

The following scenarios need to be tested for this combination of modules:

I. Positive testing:

- Signal T only shall show the proceed aspect, as long as the signal V shows a stop aspect, points a and b are locked in normal position and the point 'b' is not blocked (valid for the travel connection marked in orange).
- Signal S shall only show a proceed aspect, as long as the signal U shows a stop aspect, points a and b are locked in normal position and the point 'a' is not blocked (valid for the travel connection marked in green).
- Signal T shall only show a proceed aspect, as long as the signals V, S and U are showing stop aspects, the points a and b are locked in diverted position and the points are not blocked (valid for the travel connection marked in blue).
- Signal V has to show a stop aspect as long as signal T is showing a proceed aspect.
- Signal U has to show a stop aspect as long as signal S is showing a proceed aspect.
- The signals V, S and U have to show stop aspects as long as signal T is showing a proceed aspect.
- The points 'a' and 'b' must not move as long as signal T is showing a proceed aspect (valid for the travelling connections marked in orange and blue)
- The points 'a' and 'b' must not move as long as signal S is showing a proceed aspect (valid for the travelling connection marked in green)

II. Negative testing:

- For the green marked travelling connection signal S must immediately switch to a stop aspect, when one of the following events occur:
    i. Signal V no longer shows a stop aspect
    ii. Signal V reports a degraded mode to the interlocking
    iii. The point ‘a’ and/or ‘b’ (flank protection no longer guaranteed) is no longer locked
    iv. The point ‘b’ and/or ‘a’ (flank protection no longer guaranteed) reports a degraded mode to the interlocking
    v. The TVP section of the point ‘b’ is no longer reported as free.
    vi. The TVP section of diverted leg of point ‘a’ is no longer reported as free
    vii. The TVP section or one of the axle counters within the point ‘b’ reports a degraded mode to the interlocking
    viii. The TVP section or one of the axle counters of the diverted leg within the point a reports a degraded mode to the interlocking (flank protection is not guaranteed)
- For the orange marked travelling connection signal T must immediately switch to a stop aspect, when one of the following events occur:
    ix. Signal U no longer shows a stop aspect
    x. Signal U reports a degraded mode to the interlocking
    xi. The point ‘a’ and/or ‘b’ (flank protection no longer guaranteed) is no longer locked
    xii. The point ‘a’ and/or ‘b’ reports a degraded mode to the interlocking
    xiii. The TVP section of the point ‘a’ is no longer reported as free.
    xiv. The TVP section of diverted leg of point ‘b’ is no longer reported as free
    xv. The TVP section or one of the axle counters within the point ‘a’ reports a degraded mode to the interlocking
    xvi. The TVP section or one of the axle counters of the diverted leg within the point a reports a degraded mode to the interlocking (flank protection is not guaranteed)
- For the blue marked travelling connection signal T must immediately switch to a stop aspect, when one of the following events occur:
    xvii. Signal S and/or U and/or V no longer shows a stop aspect
    xviii. Signal S and/or U and or V reports a degraded mode to the interlocking
    xix. The point ‘a’ and/or ‘b’ is no longer locked
    xx. The point ‘a’ and/or ‘b’ reports a degraded mode to the interlocking

xxi. The TVP section of point ‘a’ and/or ‘b’ is no longer reported as free.

xxii. The TVP section or one of the axle counters of point ‘a’ and/or ‘b’ reports a degraded mode to the interlocking

After having tested the combinations of modules successfully with the positive and the negative tests, they can be used for the design and development of the interlocking application on project level. By using such an approach it is possible to minimize the testing effort significantly, since the generic functionality of the described scenarios is only tested once but can be integrated in the design as often as planned.

Furthermore, those pre-tested module combinations can be integrated in any other project, in which these functionalities are needed. This can decrease the effort for future interlocking applications.

To realise the designated interlocking project, the correct association of the different module combination within the interlocking design needs to be tested. But this task has to be done anyway when testing the route settings of the interlocking project. These tests can be performed in the factory’s laboratories without integrating on-site tests.

In the field only the correct connection of the wiring has to be tested to be sure that the interlocking will work correctly. Further functional field tests are not needed.

3.2.4 Safe by Design

As stated in several industry standards, the safety assurance is obtained both by implementing safety driven quality procedures and giving evidence of such assurance.

If the system's own procedures would lead to safe results without testing, this is called "safe by design". Tests performed in order to obtain evidence would not be necessary or, in case tests are required by the authorities, the effort would be minimised.

The main objective of this section is to investigate whether these procedures are of common use in the industry and see if they can be improved.

For railway signaling systems the addressed industry standards are the CENELEC standards, which consists mainly of

- EN 50126 that addresses the complete signaling system as a set of individual equipments,
- EN 50129 that states how to obtain the conformity or approval of a particular signaling system or equipment and
- EN 50128 that focuses on methods for providing software that complies with the safety integrity requirements.

As stated in these standards, a certified quality assurance system is required in order to provide systems that are safety related.

A Software Quality Assurance Plan is required in order to provide a safety level demanded by the requirements of the electronic safety related systems such as interlocking systems.

3.2.4.1 Safe Design

Before the probability and consequences of a failure are estimated and compared with a target, there should be asked whether the failure possibility can be eliminated.

Designers have a second chance, opportunities to go over their designs again, but operators and maintenance workers do not get second chances. Safety related systems should therefore be designed, whenever possible, so that they are user-friendly, and can tolerate departures from ideal performance by operators or maintenance workers without serious effects on safety, output, or efficiency.

Similarly, although much attention has been paid to the improvement of equipment reliability, 100% reliability is unattainable, and compromises have to be made between reliability and cost. Systems should therefore be designed, whenever possible, in a way that equipment failure does not seriously affect safety, output, and efficiency. Fail safe systems (interlocking systems among them) are designed in this way so a failure of the system leads to a safe state.

There are some ways by which friendliness in system design can be achieved. The characteristics are not sharply defined and merge into each other.

Friendly systems can be achieved through intensification or minimization. This implies designing them in a way that they contain fewer subsystems or procedures, ideally the minimum elements required to work properly, in order to have a lower probability of failure. The concept is that what the system does not have, cannot fail. If fewer components are present, there will be less need for resources. Much of the pressure for intensification has come from those who are primarily concerned with cost reduction. In fact, friendliness in plant design is not only an isolated concept but a desirable one into a package of measures, including cost reduction, lower resource usage, and simplification that the industry needs to continue to adopt in the following years.

If intensification is not possible, then an alternative is substitution: using safer equipment in place of a hazardous one. Both intensification and substitution decrease the need for additional protective equipment and thus decrease plant cost and complexity, but intensification, in addition, brings about a reduction in the system size and further reduction in cost. Intensification, when it is practicable, is better than substitution, if both are possible.

Another alternative to intensification is attenuation or moderation by using a hazardous component under the least hazardous conditions. Attenuation (moderation) is sometimes the reverse of intensification (minimization), for if the components are more likely to fail there should be more replicates in the system in order to assure correct functioning. In designing friendly plants, there has to be a compromise by considering different possibilities.

It is also a possibility the limitation of effects (a form of moderation) by changing designs or conditions rather than by adding protective equipment or failure procedures that may fail or be neglected.

Intensification, substitution, attenuation, and limitation of effects produce inherently safer design because they avoid hazards instead of controlling them by adding protective equipment or procedures. The term inherently safer implies that the process is safer because of its very nature and not because something has been added to make it safer. Note that it is said inherently safer systems, not inherently safe ones, for all hazards cannot be removed. Note that sometimes the term inherently safer design is used in a wider sense to include all the methods of making systems friendlier. It can go even further and expand the concept of inherently safer designs to include methods so that the effects of a failure are minimized.

On the other hand is the simplicity. Simple systems are friendlier than complex ones because they provide fewer opportunities for error and less equipment that can fail. They are usually also cheaper. The main reason for complexity in systems design is the need to add equipment to control hazards. Inherently safer systems are therefore also simpler systems. Other reasons for complexity are as follows:

- Design procedures that result in a failure to identify hazards or operating problems until late in design. By this time, it is impossible to avoid the hazards, and all it can be done is add complex equipment to control them.
- A desire for flexibility. Complex systems with numerous elements or subsystems have numerous weak points, and errors are more likely.
- Persistence in following rules or practices, which are no longer necessary.
- Intolerance of risk. There should be a limit for the acceptable risk.

Equipment can, of course, combine more than one of the features of friendly systems, and they are interlinked. Thus, intensification and substitution often result in a simpler system because there is less need for added safety equipment or procedures.

Friendly plants are also designed so that those incidents that do occur do not produce knock-on or domino effects, and so that incorrect assembly is difficult or impossible.

With friendly equipment, it is possible to see at a glance if it has been assembled or installed incorrectly or whether it is in the open or shut position, so it is very important to make the status of each component or subsystem clear. There should also be some tolerance of misuse, as it will tolerate poor installation or operation without failure.

When possible, there should be an ease of control, by the use of physical principles rather than adding control equipment. Friendly systems have a slow and flat response to change rather than a fast or steep one; very accurate measurements or tests are not necessary, and the control limits are not close to the safe operating ones. The control and safety systems are resilient; i.e., they do not interfere with operations or maintenance to the extent that there is a temptation to bypass them.

In a safer system there has always to be a computer control of the system. Friendly software is scrutable; i.e., it is easy to see whether or not it will do what it is supposed to do. Most software is not. In addition, software should be designed by people who understand the process. The software should allow for foreseeable hardware failures and should not overload operators with too much information, such as numerous alarms sounding at the same time. It also should have been tested thoroughly, though testing of every possible combination of conditions is impracticable. Old software should be reused with caution.

Instructions and other procedures should not try to cover every conceivable condition that might arise; otherwise, they will be so long and complex that no one will read them.

Nowadays there is another concept to have in mind that is the life-cycle friendliness. It should consider the problems of creation, development, commissioning and dismantling as well as operation and maintenance.

If hazards cannot be avoided and protective measures have to be added, then whenever possible, they should be passive rather than active or procedural. Passive protections do not fail, while active protections based on human actions or on devices can fail at a certain point and be unprotected. Another disadvantage of active systems is that they may fail safe; that is, they may operate without need and shut down the system unnecessarily. Though this is preferable to failing to operate when required, it does tempt operators to disarm the systems. More effort should be made to choose basic designs, and design details, that are user-friendly.

Inherently safer and friendlier design should be seen as a part of an overall approach to safer systems. The steps to be followed to achieve these characteristics are often summarized as identify, prevent, control, and mitigate hazards. Inherently safer and friendlier design might be described as part of prevention, but it is better to use the additional guide words avoid or reduce because designers seem to respond to the word prevent by adding protective equipment.

Of course, every hazard cannot be avoided, and then it is important to prevent, control, and mitigate them. The methods that can be used are, in the usual order of preference, passive, active, and procedural.

Inherently safer and friendly features should be introduced during design. It is often difficult and expensive to incorporate them into an existing plant. However, some characteristics or elements can always be reduced and sometimes there is a way to make an old system inherently safer, but it is not the regular case.

These designs are not merely desirable but isolated features, but rather parts of a total package of improvements that the industry needs: a move toward systems that are simpler, cheaper, and safer and that use less resources and need less maintenance. As already stated, friendly systems are often cheaper than hostile ones.

A hierarchy of Controls has to be made. Inherently safer and user-friendly systems are designed and operated according to the systematic approach to loss prevention. Safety can be studied from two points of view: inherent safety, and add-on safety.

The preferred order of consideration for risk-reduction measures is – from most to least effective – inherent, passive engineered, active engineered and procedural safety. This is akin to the layer of protection analysis (LOPA) concept in which inherently safer process design sits at the central core of the layers. According to Andrew Hopkins, there is a hierarchical ordering of controls to deal with hazards and the ensuing risk called hierarchy of controls. This hierarchy covers the spectrum from elimination (at the top of the hierarchy) through engineering and administrative (procedural) controls, to PPE (personal protective equipment) at the bottom of the hierarchy. F. A. Manuele calls this sequence the safety decision hierarchy.

Although safety is generally thought in a comparative sense, the distinction between safe design and safer design should be made. With safe design, there are active safeguards to prevent the occurrence

of hazardous events and to protect people and the system itself from the effects. With safer design, there are fewer hazards, fewer causes, and fewer people to be exposed to the effects. The safety adviser has acquired a reputation as someone who adds to the cost and complexity of the plant, the added equipment is necessary, there is no doubt, but it is also expensive and complex, and the test procedures to assure safety are also an added cost to the development of the system.

There always has to be a balance between the costs to assure the inherent safety and the costs of the performance of tests to assure the safety with evidences.

3.2.4.2 Examples for Safety Assurance

3.2.4.2.1 Spain

Currently in Spain most of the safety assurance is done according to the CENELEC approach and based on quality assurance and procedures rather than safety evidences obtained through testing. Testing is usually used in order to validate that the specified functionality is implemented in the interlocking and this is not a time consuming task, since in one or two weeks up to one month, depending on the complexity of the interlocking, this task is finished. On the other hand, tests in the field are basically concordance between interlocking indications and real elements position or aspects.

There are two ways of validation:

- documental validation and
- functional validation.

Documental validation is carried out compiling all the documentation generated during the development. Thanks to the traceability of the documentation a documental demonstration of the achievements of all the requisites of the product is obtained. All this documentation is part of the safety case documentation and RAMS dossier of the product.

In order to obtain the functional and integration validation, conformity tests to assure that the product complies with the specified functional requisites are needed.

These product validation tests are carried out for the equipments of the provider that are not homologated for their application in the line or for the new functionalities that were not included when homologated.

3.2.4.2.2 United Kingdom

In UK, Network Rail is developing a new system called Modular Signaling that introduces simplification to signaling principles; reducing the complexity of configuration data and making greater re-use of previously designed and tested logic.

This last part is in line with the Spanish case where already safe proven functionalities do not have to be safe-tested again. The first part that deals with restricting the options available to designers will mean reductions in design time as designs will be produced to a much more consistent standard and less effort is needed to ensure compliance with standards and to meet the aspirations of other parties. This second part can lead also to safer designs, since simpler designs can lead to safer ones.

3.3 Effort Saving Potentials

One of the most important topics of the research work of INESS with respect to testing and commissioning is the potential of the proposed methods for effort savings. The potential needs to be evaluated by estimating the expected effort of using these methods during the development and application of an interlocking system.

A pre-requisite to carrying out a competent evaluation, especially to gather comparable results, is the implementation of a generic reference track layout. The generic track layout will be used for the identification of effort saving potential at suppliers and the railway administrations, since both are involved in this process. The development and design of the generic track layout is described in section 3.3.1.

Furthermore a method for the evaluation of the effort saving potential is developed and described in detail in section 3.3.2.

The last section of this chapter will summarize the identified effort saving potential of the different proposed testing methodologies with reference to the generic track layout.

3.3.1 Track Layout

An interlocking can control very different kinds of infrastructure, stations and lines. Therefore the specific functionality of the applied interlocking differs irrespective of the performance of the core product. To get comparable information for the identification of effort saving potential it was decided to develop a reference track layout. This layout can then be used as the basis of the investigation for the saving potential of the application of each of the developed testing and commissioning methodologies.

The layout can also help the manufacturers and the railways to estimate their effort savings. With this layout it is possible to produce comparable results from all the industry partners, since all estimations are based on the same station layout with the same number of switches, signals and tracks that need to be equipped and therefore tested. Additionally the basic test functionality of the interlocking is given and the manufacturer can tailor the estimates by adding the specific national functionalities of the home or main country. Equally railway administrations can take advantage of the reference system for estimating purposes.

To give every manufacturer the possibility to estimate their savings, the layout represents a generic mid-size station, based on general operational functionalities, which every railway requires. The identification of the general operational functionalities (see chapter 3.3.1.1) as well as the development of the track layout (see chapter 3.3.1.2) is described as follows:

3.3.1.1 Identification of the general operational functionalities

The necessity to meet as many national requirements for a mid-size railway station leads to strategy of identifying basic operational functionality rather than modelling every conceivable combination. An operational functionality represents basic railway operation that is carried out by every infrastructure manager, regardless of the nationality and without taking the signalling or protection system into account. Such an approach allows development of a track layout which can be used by every industry partner within the INESS project.

The identification of basic operational functionality is split into two independent steps:

- Identification of basic system elements, such as single or double track line, dead-end or through station, etc. (see section 3.3.1.1.1)
- Development of general operational events, which can be performed using the basic system elements, such as “entering the station”, “stopping at a platform”, etc. (see section 3.3.1.1.2)

3.3.1.1.1 Basic system elements

In the first of the two steps, the basic system elements were identified. By selecting these elements the framework for the track layout that should be designed was build up.

The identification and assessment of the basic elements is based on an academic perspective in order to meet the needs of most of the railway administrations in the INESS project. The intention of the basic system elements is to design a station both close to reality and being testable using the methodology approaches described above.

Table 5 shows the subset of basic system elements including the description for the selection criteria, which are acknowledged to be taken into account for designing the track layout. To give the whole set of identified system elements, also those elements, which were considered and rejected are displayed in Annex A.1.

System decision	Selection criteria
Number of station tracks (single / double)	The track layout should contain two tracks because it is one of the most usual situations in the network of railway administrations.
Dividing the station into freight traffic area and passenger traffic area	In practice it would not be very common to have passenger platforms at the part of the station where freight trains are shunted, loaded or unloaded. The necessity of keeping the tracks free for the scheduled passenger train stops would not provide the flexibility that is necessary for a freight track. Therefore, the track layout for the station will be divided into a passenger and a shunting area.
Alignment of freight traffic area and passenger traffic area	In the track layout freight traffic area and passenger traffic area should be parallel. A sequential layout of areas would lead to the necessity of having additional signals. That would be very complex and will be handled differently, depending on a specific railway. To create a track layout that is independent from any railway specifics passenger and shunting areas will be designed as a parallel track layout.
Operating program (non-mixed / mixed traffic)	The track layout should handle mixed traffic because this is the usual case on most of the lines of all railways. Depending on different priorities of trains, it will lead to scheduled or unscheduled passing.
Operating program (speed difference)	On every railway line (without high speed lines and rapid transit) trains with different speed and priority can be found. This is the basis for scheduled and unscheduled passing in practical operation.
Type of station	Combination of junction station layout and intermediate station layout with flat junctions provides a combination of all different kinds of station layout.
Main layout of station (terminus station or through station)	The track layout should represent a through station because this variant of layout is easier to create, especially with respect to complexity and testing effort. In the layout example, the main characteristic of a terminus station, the end of a train ride at a bumper, is captured by dead-end tracks within the through station.
Type of platforms	The type of the platforms is not relevant for the track layout with respect to testing of interlocking functionality.
Construction of crossovers (A- or V-construction)	Based on maintenance point of view, crossovers are either built in A- or V-construction.
Track layout in freight traffic area	A freight traffic area should only contain fans of sidings, if there is not any gravity shunting.
Through track in the middle of the station	A through track should be located in the middle of the station. On a double track line, only in this case it is possible to use the track from both directions without crossing the track of the opposed direction.
Changing the direction of travel	The track layout should offer the possibility for changing the direction of travel by shunting the locomotive to the other side of the train.

Table 5: List of generic basic system elements

3.1.1.1.2 General operational events

After identifying the basic system elements for the creation of the track layout, the development of a set of general operational events was carried out. The general operational events are listed in Figure 14. Those operational events marked in grey were not taken into account for the design of the track layout. The complete table of the identifies general operational events can be seen in Annex A.2

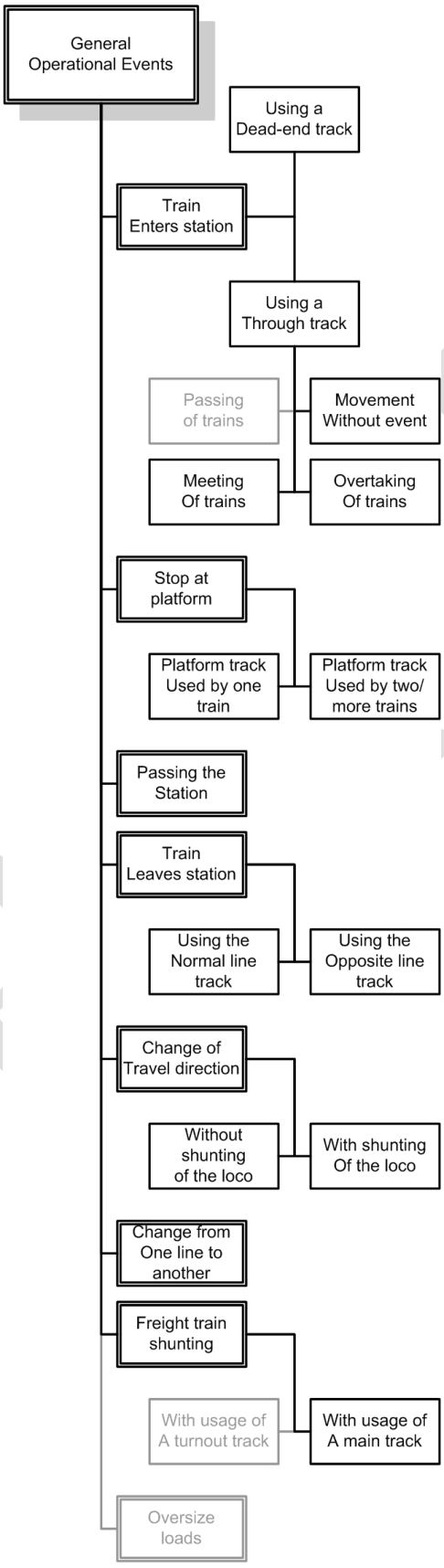


Figure 14: Listing of general operational events

3.3.1.2 Development of the track layout

After identifying the basic operational functionality, the track layout was developed by implementing the basic system elements into a topology of a generic railway station, carried out in two steps:

- Designing a track layout by combining the basic system elements and the general operational events (see Figure 15 and Annex A.3)
- Creating a set of basic travel connections for the track layout (see Table 6)

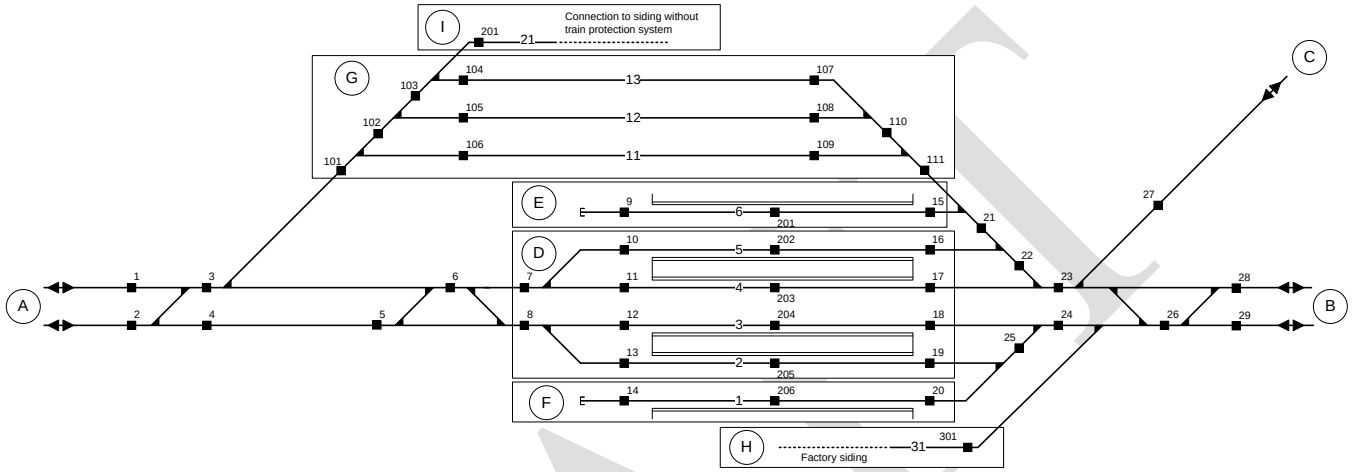


Figure 15: Generic track layout for an INESS interlocking

The track layout is structured into 9 segments, marked with an alpha-numerical signed circle:

A. Double track line with a single and a double crossover, a connection to the passenger station part D, to the shunting area G and I and the factory siding H
B. Double track line with a double crossover, a connection to the branch line C, the passenger station parts D/E/F and a connection to the shunting area G
C. Single track branch line, connected with the double track line
D. Passenger station, consisting of two through tracks and two through tracks for stopping, passing, etc.
E. Dead-end single track as additional track of the passenger station connected with the double track line B
F. Dead-end single track as additional track of the passenger station connected with the double track line B
G. Shunting area consisting of three tracks and connections to the double track lines A and B and to the siding area I
H. Factory siding with connection to the double track line B
I. Siding area with connection to the double track line A

This 9 segment structure provides a subset of direct travel connections as shown in Table 6. For the identification of the routes only those were taken into account where a train can run directly, without any shunting movements or changing of travel direction.

From ... \ To ...	A	B	C	D	E	F	G	H	I
A	-	-	-	X	-	-	X	-	-
B	-	-	-	X	X	X	X	X	-
C	-	-	-	X	X	-	X	-	-
D	X	X	X	-	X	X	X	X	-
E	-	X	X	X	-	X	X	-	-
F	-	X	-	X	X	-	X	-	-
G	X	X	X	X	X	X	-	X	X
H	-	X	-	X	-	-	X	-	-
I	-	-	-	-	-	-	X	-	-

Table 6: Set of basic travel connections for the generic track layout

These constraints give a total amount of 38 travel connections, which need to be implemented into test sequences.

For the evaluation of the three previously described testing methodologies, this number of travel connections gives an amount of 114 tests, which need to be performed. Additionally, the effort to test the track layout with its 38 travel connections using the SoA testing methodology of each industrial partner of the Work-stream needs to be evaluated as the basic effort information.

3.3.2 Methodology for the identification of saving potentials

There are several approaches to increase the efficiency of testing and to accelerate the commissioning of signalling systems, in addition there is the option to combine these methodologies.

Shifting the majority of necessary testing activities from on-site testing towards factory or laboratory testing has the potential for significant effort savings and an improvement of quality. The magnitude of the potential depends on the state of the art in the specific country, on the complexity of the system and on the number of modifications (renewals, exchanges…) of the infrastructure within the assessed time frame.

In case of testing the interaction between onboard units and infrastructure, the gain of efficiency is evident, as testing of these components requires real engines running on a real track. The effort to bring a locomotive onto the infrastructure which has to be tested and the effort for blocking this infrastructure for testing purpose instead of producing traffic service are in completely different orders of magnitude compared to running tests in a laboratory or factory environment.

But also testing interfaces between infrastructure elements in the laboratory can bring many advantages as opposed to testing them in the field during commissioning. The detection of malfunctions or errors in the field and the necessity to fix issues at this stage is more expensive than in the factory or laboratory. Furthermore, laboratory tests can be done under controlled repeatable conditions without significant additional effort. In the best case scenario, the complete functional testing of a new installation could be done in the laboratory. The system will be brought into the field afterwards, can be assembled and the only final testing could be to check the correct assembly and the failure free functioning of the cabling in the field. This will require changes also in regulations and within some NSAs etc., but could lead to significant improvement of effort efficiency.

The industrial engineering approach described in section 3.2.3 aims to not only to improve the testing itself, but also the engineering process for designing new track layouts. One of the most time-consuming and expensive factors is the application of individual, non-standard solutions in the design of a new system application. Reducing these bespoke solutions and the use of standardised layouts instead can lead to significant increase of efficiency e.g. in the test case generation. The more complex an individual solution is the more manual work is required. Minimising individual options can lead to an increase of standardised design elements which can be used like a construction kit which can be tested in a standard way. Following this approach consequently is a first precondition for – in the best case – the implementation of plug & play in the railway infrastructure domain.

The concept of the investigation to increase efficiency for testing and commissioning within WS F is shown in Figure 16:

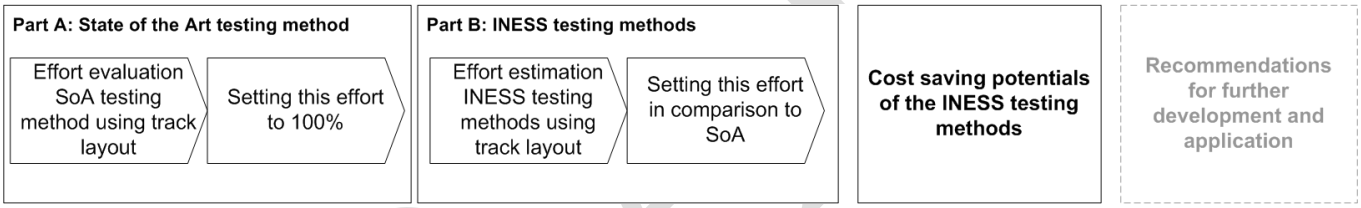


Figure 16: Rough steps for the evaluation of effort saving potentials

The track layout as described in section 3.3.1 is to be used for evaluating the potential of effort reduction by comparing the actual effort for testing (state of the art) and the expected effort for the same testing using more sophisticated methods in the factory or laboratory.

The track layout description does not include any signalling presetting in order to allow for national specifics of the user. This leads to challenges in the analysis, but this compromise is necessary and gives insight into more details. Further input for the comparison is the use of the 38 travel connections (see Table 6) and the decision to use the individual national-specific signalling system for the application.

The application of the track layout is done normally by both infrastructure managers an industry partners. The first step is the design of the signalling system according to the track layout for the companies' main market and its national specifics.

This is the basis for, firstly creation of the corresponding test cases and test sequences. The efforts for testing the specific application according to the specific state of the art methods need to be determined and described. These figures serve as a reference for the trial of new / other methods.

It is important to describe the aspects of the individual starting basis which are relevant for testing and commissioning because this needs to be compared with the application of new methodologies later. A company which already uses more effective methods for testing (e.g. sophisticated test automation) will not have the same potential for effort reduction as a company which does not (e.g. high manual efforts for test generation and execution).

In order to determine the individual potential for increasing efficiency, the next steps of the evaluation phase are the repetition of the design of the exemplary signalling system for the track layout described

in section 3.3.1 and the determination or estimation of effort using the methods according to section 3.2. Here several approaches and combinations of methodologies can be tried to maximize the effect of effort reduction.

The results are then compared to the reference which was determined as the first step. The potential for effort savings (or increase) using new methodologies can be expressed as percentage with the state of the art effort as the reference point.

It is expected that the highest impact on effort and duration will be achieved by:

a) reasonable combination of different approaches,

b) the consistency of following the principles of standardisation, modularisation and automation and

c) the actual technical and process-related application of the specific company applying these methods.

For the INESS WS F partners the latter has been investigated in WP F1 and is described in the State of the Art report [1].

The results have to be described in enough detail to allow for an analysis and comparison. Essential for the interpretation of the results is a detailed description of the application, the assumptions that were made and the assignment of figures to the different methodologies that are used for the comparison. It is possible that some of the methods lead to effort reduction, whereas others lead to higher efforts. In order to give recommendations of possible combination of ways of testing, it is necessary to describe these effects during the application of the track layout by the partner.

3.3.3 Effort saving potentials of the described testing methods

Three INESS partners have described their estimations and evaluation after applying the described testing methods. The results comprise one infrastructure manager and two industry partners. Their experiences and conclusions can be summarized as follows:

a) From an infrastructure managers' point of view, a modularisation of track layout elements which reduces the flexibility of the design is not applicable, especially not in large stations. It also does not seem reasonable since the costs of the signalling system form approximately 10 % of the total investment costs of the rail infrastructure.

   In the case of this railway administration, the reduction of field tests is already implemented to the level that only the concordance with the field elements has to be tested. The laboratory tests are determined by the infrastructure manager and will be maintained, irrespective of European standardization. Therefore, this approach does not contribute to cost savings for this company.

   The main part of the testing is effort for the industry partner, who automates and optimises the processes. Reduction of this effort could generate savings for the infrastructure manager as well. Currently the costs (and therefore also saving potentials) are not known by the customer. This could be overcome by a standardized interlocking.

   The conclusion is that from an infrastructure managers' perspective, the increase of efficiency in testing does not lead to significant cost savings. It is assumed that higher potential can be created by the standardization of the interlocking interfaces. This is a precondition for the inter-changeability of parts or whole interlocking systems independently from a specific supplier.

b) The industry partners' conclusions differ from these results due to the different perspective. It has been noted that the individual potential for saving costs depends on the initial situation of the specific company.

Industry partner 1 already applies a number of the methods and principles like functional testing mainly in the laboratory as well as the optimization of test sets by clustering features and sub-features. Therefore, one main aspect to create cost savings consists of the standardization of test specifications and test cases corresponding to the INESS common kernel of requirements.

The one-off effect of this in comparison to the state of the art would be the avoidance of the test case design for each new project. This can be quantified in a saving from 20% to 25% of the initial costs for this activity.

A further effect is the reduction of iterative test set refinements, which occurs multiple times. Its saving potential can be 5%.

The principle of modularization is already being applied by this partner as well. Therefore the enhancement of simulators and tools might be an optimization, but with only minor cost reduction of about 5%. As for the modularization of the design and the associated testing which is also already applied, a deeper cascading into lower levels of the V-cycle could be possible. Here also a cost saving of about 5% is assumed as a reasonable ratio. The restriction for higher savings is the overcompensation due to higher effort to realize them.

The usage of generic functions to be tested only once, as described in the industrial engineering methods, is part of the development of generic applications and specific applications and therefore already applied in principle. The consideration of the testability of design choices would result in better identification of classes of equivalence, bringing also a one-off effect of 5% to 10% cost reduction and a repeatable saving potential of about 5%.

Industry partner 2 had to modify the application of the track layout as 19 of the proposed main routes are not valid in that specific country. To compensate this, he added 19 different, but valid routes. The effort for taking all possible (i.e. 104 main routes) routes into account for the testing was measured as 563 person hours. This was necessary because of national rules in the specific country. This effort was defined as the 100% reference for any cost savings.

Reducing the effort of re-testing already tested infrastructure elements in the main and shunting routes has been applied as one simple method by marking and skipping all tested elements during the procedure. The saving potential here was estimated to be about 20% compared to the reference.

It has to be remarked that a deeper analysis of which repetition of re-testing can actually be neglected could not be done. In a real project, this needs to be guaranteed. Therefore, the figure saves as an expert's estimation which can be proven by more detailed analysis. The estimation is also that the saving potential is higher for larger stations (maybe up to 50%) and might be significantly less in smaller stations (approx. 5%).

This effect can be enforced by the approach of applying industrial engineering methods. This can further optimize the set of selected routes to be tested. For the reference track layout, the further saving potential is estimated 10% additionally to the 20% described above.

The possibility to reduce field tests by testing mainly in the laboratory is disbelieved since the real functioning of interfaces is influenced by parameters which cannot be simulated (e.g. length of cabling, proximity of HV electricity nets etc.). Therefore, no cost saving potential is seen in this approach.

To conclude, it can be said that a standardisation of tests to be performed only once generally leads to a reduction of effort in the test specification for industrial partners. The potential of this depends on the actual status of the specific company. The application of the industrial engineering methods in both cases were estimated to further increase the efficiency by 5% to 10%.

An important precondition for the reduction of testing effort as hypothesized would be to convince a number of national authorities since this affects rules and regulations. In the case of the infrastructure manager, it has already been said that this is not acceptable for his country.

Section 4 – CONCLUSIONS

This handbook has explored a number of novel approaches to the subject of testing and commissioning. There has been a clear indication that the way forward is to reduce/remove the need for on-site testing and move the functional and safety testing into the factory environment where conditions are controlled. It has taken input from the current industry state-of-the-art as the starting point for the exploration and has then looked into the approach taken by interoperable subsystems, scripting, modularisation and increased usage of factory based testing.

It is apparent from the outcomes that an optimised approach can be obtained through the combination of a number of the techniques because each offers benefits in specific areas of the process and are not mutually exclusive.

A method of assessing the effectiveness of the testing methods has been developed which can be used by both railway administrations and suppliers alike. The method avoids the trap of approaching the assessment through the application of administration specific signalling technology and focuses instead on an operational approach which leads to an optimised evaluation of the methods.

It is recommended that the methodologies described are further developed to an exploitable level where industry can take practical advantage. To achieve this goal it is recommended that suppliers review their designs from a testing perspective and optimise them for testability, in addition that suppliers take the methods proposed and develop internal processes to the enact them in a practical industrial environment.

Railway administrations are recommended to reduce the reliance on bespoke application designs and converge on standard forms that can be rolled out across the network. This will allow the modularisation approach to be adopted for the vast majority of applications which will facilitate reuse of test results and a reduction on the effort required to develop an interlocking application.

Section 5 – BIBLIOGRAPHY

[1] State of the art report

Section 6 – ANNEXES

Annex A: Track Layout

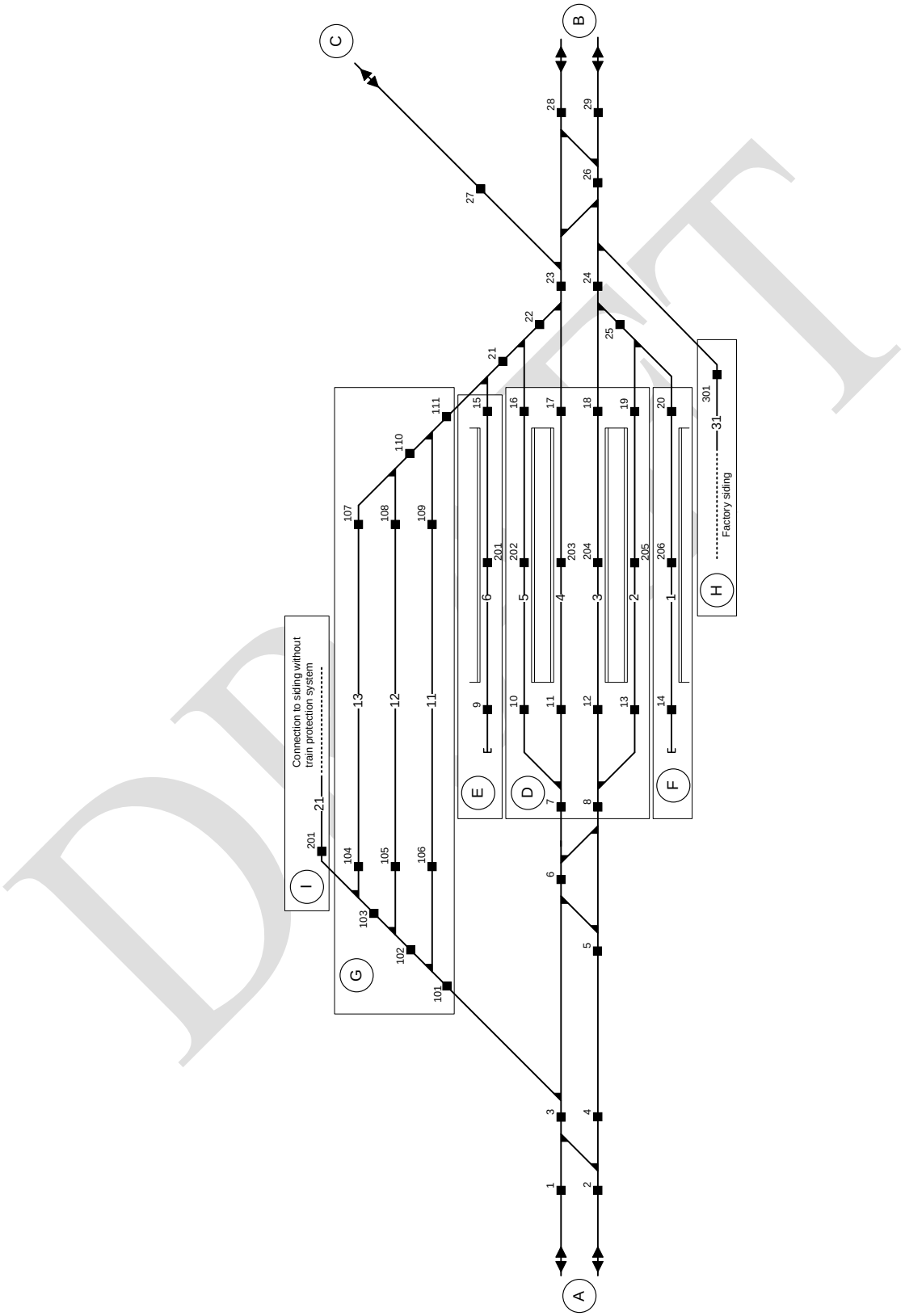
Annex A.1: Basic System Elements

TrackLayout--System Decisions

Annex A.2: Operational Events

TrackLayout--OperationalEvents

Annex A.3: Track Layout



Annex B: Evaluation of methods for cost saving by INESS Partners

Remark:

The text in this annex contains the original answers of the three INESS partners, which have given their evaluation results. Since this Testing & Commissioning Handbook as the official deliverable of the Workstream F will be classified as public and to guarantee the discretion of the names of the partners and their respective figures, the text is shown anonymous.

Annex B.1: Industry partner 1

1. Reduction of field tests by increasing laboratory tests

   1.1. Wiring, concordance, calibration etc. cannot be reduced (they are intrinsically field activities).

   1.2. The approach we usually follow

      1.2.1. already foresees that functional testing is mainly carried out in laboratory, and

      1.2.2. already includes the mechanisms of features and sub-features as an optimization of test sets;

therefore

   1.3. the main aspect to leverage to obtain savings is the standardization of test specifications: like IOP, the availability of a standardized set of test specifications (set of test cases + criteria to configure them) would

      1.3.1. avoid the phase of test case design (as long as the corresponding requirements remain the same – which is the case of INESS common core), and

      1.3.2. reduce the need for iterative test set refinements.

      The cost saving potential of this aspect has a “one-shot” component (point 1.3.1 above), applicable only once (as long as requirements do not change), and a “repeatable” one (point 1.3.2 above):

      1.3.3. the “one-shot” component can be quantified in a saving from 20% to 25%, but is applicable only the first time the related set requirements is implemented (and then needs to be tested);

      1.3.4. the “repeatable” component can be quantified in a saving of about 5%.

2. Modularized interlocking

   2.1. Modularity in terms of testing environments (partially simulated and partially target) is an approach we usually follow; marginal enhancement to simulators and tools could bring about a saving of no more than 5%.

2.2. Modularity in terms of design (and associated testing) already exists, anyway it could be cascaded more deeply into the lower levels of the V-cycle (e.g. code module and unit level), its effect being the anticipated detection of errors and non compliances; the saving can be quantified in about 5% (reaching higher figures is prevented by the larger amount of work to do).

3. Usage of industrial engineering methods

3.1. "Generic functionalities tested only once but integrated in the design as often as planned" is a consequence of having a Generic Application and a Specific Application; the approach we follow for Generic Application testing is already the one described, since it is intrinsic in our software architecture (abstract code driven by application data).

3.2. Considering testability of design choices would match with the consideration above, insofar as the identification of classes of equivalence would be made easier; again, two components can be identified (refer to 1.3.1 and 1.3.2):

3.2.1. the "one-shot" component can be quantified in a saving from 5% to 10% (depending on the amount of simplifications);

3.2.2. the "repeatable" component can be quantified in a saving of about 5%.Industry partner 2:

Annex B.2: Industry partner 2

Part A – Effort evaluation of SoA testing method

Remarks to the track layout:

1. It needs be noted that according to the national signalling rules of our railway only half of the proposed main routes (called train routes in our terminology) are valid routes. Another 19 routes are not possible to be set up. The table shown below indicates the routes not allowed.

To ...

From ...	A	B	C	D	E	F	G	H	I
A	-	-	-	X	-	-	X	-	-
B	-	-	-	X	X	X	X	X	-
C	-	-	-	X	X	-	X	-	-
D	X	X	X	-	X	X	X	X	-
E	-	X	X	X	-	X	X	-	-
F	-	X	-	X	X	-	X	-	-
G	X	X	X	X	X	X	-	X	X
H	-	X	-	X	-	-	X	-	-
I	-	-	-	-	-	-	X	-	-

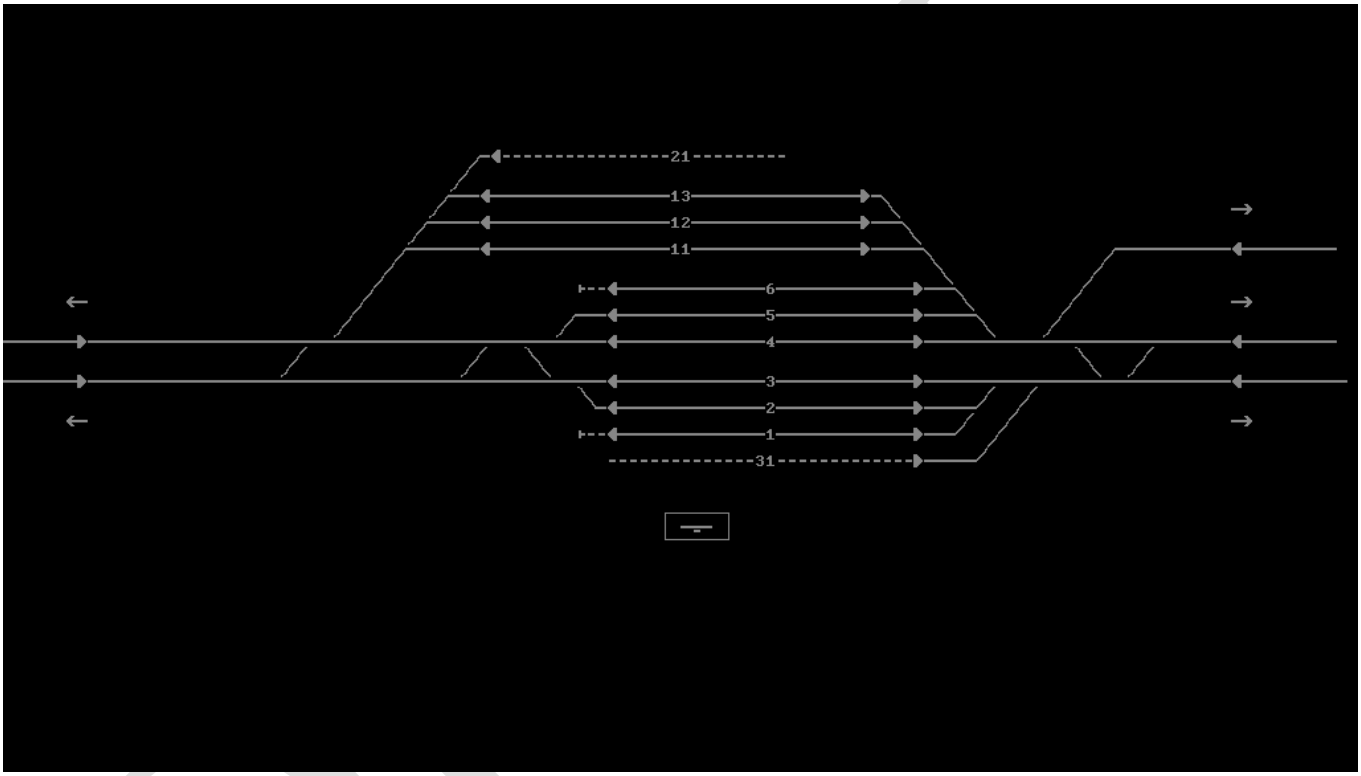
2. The average station in the national rail network includes typically the configurations and elements used in the reference track layout. But many station layouts often include configurations and elements

which impose considerably higher burden on the testing process and the tester. These are not included in the reference track layout hence not showing the impact on the testing efforts.

3. The national rules define the tests which must be carried out during the commissioning phase of the IXL. It is not possible, without changing the rules by a standard administrative procedure, to omit any specified tests. They require e.g. to test all the allowed main and shunt routes listed in the interlocking table.

As the Key process indicator the number of person-hours required to test the station according to the mandatory set of tests was chosen.

The result of the designing of the signalling to the track layout according to the national rules is shown below:



Therefore, because of the invalid routes, the evaluation was carried out in the following way:

a. first of all the evaluation of the efforts taking into account only the 19 valid main routes was done.

b. in the second evaluation another 19 random main routes were added to the list of checked routes during the testing of the IXL - equal to an increase of 4,7 %,

c. in the third phase the whole set of possible main routes in the station were identified, giving the figure of 104 main routes – equal to an increase of 16 %.

Part B – Effort estimation INESS testing methods

The phase for the SoA methods were taken as the 100 % reference for the comparison to the results of the INESS testing methodology proposed in the chapter 3.2. The precondition applied was to use the standard procedure which uses all the 104 possible main routes for the testing. This precondition, required by the national rules, is regularly applied both for the laboratory tests done in our labs before the application, and especially its specific software, is put into the phase of the FAT testing and to the com-

missioning tests in the real station application. There were carried out a few evaluations which results are shown below:

d. reduction of the number of the main and shunt routes and the tests of the signalling elements included in the route by the analysis of the already tested elements. The tests done would be identified and eliminated by a simple procedure – taking the routes listed in the interlocking table in the order given in it and checking out the elements and their positions or parameters already tested so that they are not tested again. It needs to be expressed that accurate and in-depth analysis of the way how and when it is possible to eliminate the next test of a particular route element. It must also be noted that the analysis was not done for the reference track layout exactly because of the missing time and effort figures for the WS F. So only expert's estimation was done giving the efforts, decreased to: 80 % of the reference value

It must be noted that the expert's estimation shows that the decrease would be better for large stations (possibly down to 50 %) and worse for the small stations (up to 95%).

e. as far as reducing the tests of real elements in the field during commissioning is concerned our company raises doubts of the possibility to do the tests only in the factory because the interfaces are largely influenced by the actual configuration, length of cabling etc., hence the figure would show again: 100 % of the reference value

f. incorporating the Industrial engineering methods will improve the first method by optimizing the set of selected routes and the elimination of already tested route elements by reordering the routes to be tested in the optimum order, the decrease could be even better than in the point d.: 70 % of the reference value.

It is evident that the estimations are quite rough. The fact is that using the proposed methods of decreasing the efforts would need convincing many national authorities that the elimination of some regular tests from the rules based even on some specific methods which optimize the test based on the specific configuration of each station and its interlocking cannot compromise the safety. But it strictly depend on the quality of the analyses made by each supplier and the assurance that the minimum but sufficient set of tests was proposed by the supplier and applied during laboratory, FAT and commissioning phases. And this is an extraordinarily big problem which would take many many years.

Annex B.1: Infrastructure Manager

- Is not possible a modular set of elements, because the track configuration is almost always different. We always have to adapt something. A big station will not change the tack layout; the signal system will be adapted to the track layout. The reason is that the signal system is approximately 10% of the total cost of a rail infrastructure.
- We test, with an expertise technique, a sampling of the functionality in the laboratory, and in the track only the concordance with the elements (track circuits, point machines, blocks, etc). This functionality is fixed by us as the infrastructure manager. If the functionality were fixed by INESS, we would continue doing the same sampling.
- The supplier tests in the laboratory all the possibilities of the movement table and the incompatibilities, and reports in a Safety Case the results. Other department of our company analyse this Safety Case.

In conclusion, I think, the cost saving potentials, in our country, are not in the tests, but in the inter-changeability of interlocking, being not necessary, when an interlocking has to be changed, to change for one of the same supplier technology. The standardization of the interfaces is necessary to assure the inter-changeability.

The suppliers have automated the processes of data generation and data validation, but only the suppliers know the costs. With an INESS interlocking it will be easier to estimate the cost of the engineering processes.
It's important to mention, that the OBU/EVC to use for the interoperability tests will be a reference OBU/EVC. The experience in our country is that the interoperability, nowadays, is too far.