



SAPIENZA
UNIVERSITÀ DI ROMA

MASTER'S THESIS IN TRANSPORT SYSTEMS ENGINEERING

Faculty of Civil and Industrial Engineering

July 2018

In collaboration with Italcertifer, FS Group

Procedure to place railway Electronic Interlocking products in service

A comparative study between the Italian and Indian Railways using Hazard and Risk Analysis

Supervisor	Prof. Stefano Ricci
Tutor	Ing. Luigi Caccamo, Italcertifer S.p.A.
Candidate	Mainak Chakraborty
Matricola	1722616

This study was undertaken in collaboration with Italcertifer S.p.A., FS Group, Italy.



Italcertifer is an affiliated company of *Gruppo Ferrovie dello Stato Italiane*, but totally independent of it; the company has inherited extensive knowledge in the rail and transport industry from this group. Four major Italian universities (Polytechnic University of Milan, University of Pisa, University of Florence and University of Naples), which are also stakeholders into the company, further expand the company's range of expertise by establishing a center for excellence in rail verification of conformity and safety.

Third-party rail compliance assessments are the company's core business, which Italcertifer can perform under the many authorizations obtained from various regulatory and control agencies. In 2008 the company obtained provisional accreditation of Independent Safety Assessor (ISA), which became permanent in 2012. In 2010 ITCF obtained accreditation with ACCREDIA (the Unified Italian Accreditation Body) as Certification and Inspection Body for the rail industry and design verification for validation purposes. [Ref.13]

"At the end of the day, the goals are simple: safety and security."

– Jodi Rell, former Governor of Connecticut

Acknowledgements

This thesis is imagined with the constant support and encouragement of my advisor Professor Stefano Ricci, and the able guidance of my mentor Ing. Luigi Caccamo. I am extremely grateful for their valuable input throughout the process and helping me navigate through the numerous confusions and difficulties, while letting me choose the philosophy and the direction of the work.

I would like to extend my warmest gratitude towards my colleagues in Italcertifer for sharing their immense technical expertise, experience and accepting me into the community. I would like to mention Ing. Marco Eibenschutz for sharing his vast knowledge of Railway systems and policies worldwide. Also I would like to thank Giuseppe Docile, Gianluca Marino, Chiara Aielli, Mariellen Cataldo, Marco Corvino, Paola Bocci, Riccardo Ascenzi, Davide Emanuele Lisi, Simone Pannozo, Salvatore Vetrucchio, Annalisa Suriano, Salvatore Pirrone, Elena Foschi, Ilaria Di Nucci, Giorgio Porcaro and Luca d'Amelio for their timely assistance.

I am overjoyed to have the opportunity to study in this prestigious institute, Sapienza University of Rome. I have had the good fortune of learning from and working in close collaboration with the brilliant professors during my course, namely Prof. Gabriele Malavasi, Prof. Gaetano Fusco, Prof. Guido Gentile, Prof. Maria Vittoria Corazza, Prof. Massimo Guarascio, Prof. Luca Persia and Prof. Sarno Debora. Thank you for all for your precious contributions.

I am forever indebted to my classmates and friends for their support and aid for the realisation of this thesis. I would like to mention Abhishek, Akaash, Anand, Kabyajyoti and Ravi for their assistance and encouragement.

I would like to thank Laziodisu for supporting my course, and all the invaluable friendships I created staying in the dormitory. It has been an amazing experience living with and learning from people all over the world. I would like to mention my friend and roommate Giuseppe for his tremendous support. He is a gentleman through and through. I would like to thank Imen for her consistent backing and motivation, which pushed me to go on amidst some trying moments.

I thank my parents and my sister for their constant encouragement and for believing in my dreams. It would not have been possible without their support.

Many people has left their mark directly or indirectly in this work, I wish I could name them all, but I fear I might run out of pages. Thank you everyone.

Abstract

The study attempts to define the organizational structure and the procedure for obtaining authorization to put railway components/products into service in the Italian Railways and in the Indian railways, and seeks to compare them based on their methodologies. The study highlights the areas of disparity between the two systems using a Hazard and Risk Analysis approach and identifies the areas of potential improvement. Finally, the attempts to bridge the gap between the two systems for better mutual understanding and aid in doing business together.

Contents

Acknowledgements.....	2
Abstract	3
Contents	4
List of Abbreviations	8
List of Figures.....	10
List of Tables.....	11
1 FOREWORD.....	12
1.1 Definitions.....	13
1.2 CENELEC life-cycle phase.....	17
2 Procedure in Italy	19
2.1 Powers and Responsibilities.....	19
2.1.1 National Agency for the Safety of Railways.....	19
2.1.2 Independent Safety Verifier	20
2.1.3 Applicant.....	20
2.1.4 Railway Undertaking	23
2.1.5 Infrastructure Manager.....	23
2.2 Technical Procedure	24
2.2.1 Commissioning of structural subsystems as a result of modification	24
2.2.2 Authorization to use generic and first specific applications, generic products or components.....	25
2.3 Authorization procedure for the structural subsystems	27
2.3.1 Start of the technical process.....	27
2.3.2 Evidence Fulfilment	29
2.3.3 Intermediate statement of verification	31
2.3.4 "EC" declaration and verification certificate: Minimum content.....	32
2.3.5 Request for putting in service	33
2.3.6 Releasing of APIS.....	34
2.4 Procedure for authorization to use generic applications and first specific, generic products or components	35

2.4.1	Start of the technical process.....	35
2.4.2	Definition of processes.....	37
2.4.3	Procedure for the granting of use.....	38
2.5	Managing requests for exemption.....	44
2.6	Overview	44
3	Procedure in India	46
3.1	Responsibilities.....	46
3.1.1	Research Design and standards Organisation	46
3.2	Expression of Interest	47
3.3	Request for Proposal.....	48
3.3.1	Terms of Reference	49
4	Differences in procedure for placing a product in service	54
4.1	The Italian process for obtaining APIS for SML400.....	55
4.1.1	The subjects.....	56
4.1.2	Process flow	57
4.2	The Indian process for obtaining APIS for SML400.....	57
4.2.1	Signalling System Overview	58
4.2.2	The subjects.....	58
4.2.3	Process flow	59
4.3	Disparities	60
4.3.1	Type tests	61
4.3.2	Field trials	62
4.4	Hazard Analysis.....	65
4.4.1	FUNCTIONAL ANALYSIS.....	69
4.4.2	SAFETY ANALYSIS.....	72
4.4.3	Overview.....	78
5	Conclusion	79
6	References	80
	Appendix A	81
	Appendix B.....	85
	Appendix C	91

Appendix D93

To my parents Mihir and Panchali, and my sister
Mahasweta.

List of Abbreviations

ALARP	As Low As Reasonably Practicable
APIS	Authority to place in service
ANSF	Agenzia Nazionale per la Sicurezza delle Ferrovie (National Agency for the Safety of Railways)
ASIPL	Alstom Systems India Private Limited
CCS	Control Command and Signalling
CENELEC	European Committee for Electrotechnical Standardization
CSM	Common Safety Method
CSO	Central Standards Office
DeBo	Designated Body
DFC	Dedicated Freight Corridor
DFCCIL	Dedicated Freight Corridor Corporation of India Limited
DIV	Dichiarazione Intermedia di Verifica (Intermediate statement of Verification)
DPC	Disposizioni Particolari di Circolazione (Special Circulation Regulations)
EC	European Commission
EI	Electronic Interlocking
EMC	Electromagnetic Compatibility
EN	Europäische Norm/Norme Européenne/European Standard
EOI	Expression of Interest
ERADIS	European Railway Agency database for Interoperability and Safety
EU	European Union
EUAR	European Union Agency for Railways
GP	Generic Product
GPSC	Generic Product Safety Case
HA	Hazard Analysis
HMI	Human Machine Interface
IM	Infrastructure Manager
IRCA	Indian Railway Conference Association
ISA	Independent Safety Assessor
ITCF	Italcertifer
IXL	Interlocking
LooPs	List of open points
MOR	Ministry of Railways
NoBo	Notified Body
NSA	National Safety Agency
OC	Object Controller
PHA	Preliminary Hazard Analysis

RAMS	Reliability, Availability, Maintainability and Safety
RDSO	Research Designs and Standards Organisation
RFP	Request for Proposal
RTRC	Railway Testing and Research Centre
RU	Railway Undertaking
SML	Smartlock
SMS	Safety Management System
TFFR	Tolerable Functional Failure Rate
TOR	Terms of Reference
TSI	Technical Specifics of Interoperability
TT	Type Test
V&V	Verification and Validation

List of Figures

Figure	Title	Page
1	<i>Interrelation of RAMS management process and system life-cycle [Ref.1]</i>	17
2	<i>The V-cycle representation [Ref.1]</i>	18
3	<i>Overview of the process within the scope of this study</i>	44
4	<i>Flow of the technical process for obtaining APIS</i>	45
5	<i>Constituents of the RFP</i>	48
6	<i>Constituents of the TOR</i>	50
7	<i>SML 400 [Ref.11]</i>	54
8	<i>SML400GP Design, Safety and V&V Life Cycle (Source: SML400 GPSC)</i>	55
9	<i>Functional modules of the work</i>	56
10	<i>Overview of process to obtain APIS for SML400GP</i>	59
11	<i>Sequence of activities for field trial and approval of SML400GP Electronic Interlocking system</i>	63
12	<i>The seven stages of the HA process [Ref.16]</i>	64
13	<i>A basic interlocking system</i>	65
14	<i>Hazard management at integration of product life-cycle and system life-cycle</i>	66
15	<i>Detailed representation of the interface between the point module (PM4W) with point machine (s700K) (Source: GPSC)</i>	67
16	<i>IHA methodology flow diagram</i>	68
17	<i>Point Machine NORMAL to REVERSE movement</i>	75
18	<i>Point Machine REVERSE to NORMAL to movement</i>	75

List of Tables

Table	Title	Page
1	<i>SIL quantitative and qualitative measures [Ref.2][Ref.1]</i>	15
2	<i>Climatic TT reference standards for Europe [Ref.8]</i>	61
3	<i>Differences in the test specifications according to the different standards</i>	62
4	<i>Repeated TT with RDSO specifications</i>	62
5	<i>Siemens S700K parameters</i>	69
6	<i>Three Phase AC Motor Interface Compliance</i>	74
7	<i>PM4W and Cable Compliance of environmental characteristics</i>	77

1 FOREWORD

In the post-modern era, the world is intricately connected by a complex network of communication which sustains our way of life. As globalisation interconnects our economies more profoundly, movement of people and goods has become vital for supporting the human society as we know it. As it became evident that unhindered access to markets facilitates and stimulates the global economy, countries have long sought to standardise transportation subsystems both within and around them.

Several international bodies have sprung up to regularise one single standard to be followed by all member nations. The European common market bloc spearheaded by the European Commission directed its members to recognise the standards set by it. Specifically, for the railway sector the foundation is set up by the TSIs (Technical Specifics of Interoperability), ratified by all member countries of the European Union, which guarantees the interoperability of railway subsystems all over Europe. The European Committee for Electrotechnical Standardization, better known as CENELEC, are the pilots of European Standards (ENs), which became a model to follow for all over the world. The onus of checking the compliance with the ENs in the national level falls on the respective national authorities, known as the NSAs (National Safety Agency) who optimises those core standards to fit in their respective requirements.

In Italian NSA is the National Agency for Railway Security, ANSF (*Agenzia Nazionale per la Sicurezza delle Ferrovie*) and the RDSO (Research Designs and Standards Organisation) is the regulatory body in India. In this study a comparison is drawn between the procedure to place products in service in the railways in Italy and in India.

A general sequence has been followed in this work to achieve the objective.

The study is commenced with a brief description of the Agency in Italy, its structure and competencies. The general procedure for obtaining the authorisation of a railway product or application is examined and documented. All the steps and the actors with their powers and responsibilities are mentioned. A similar approach is used for examining the Indian authority and the differences between them is outlined. For a deeper understanding, the same product which is being put to use in India and in Italy is analysed and the differences in the procedure to place them in service are identified. An area of disparity is selected and focused on and further analysis were carried out to identify and avoid the hazards involved. According to the analysis and the subsequent results, a conclusion is drawn around the area where improvements in the procedure were deemed necessary.

1.1 Definitions

- **Generic Product**
Product (hardware and/or software) which can be used for a variety of installations, either without making any changes or purely through the configuration of the hardware or the software (for example by the provision of application-specific data and/or algorithms).
- **Hazard**
Condition that could lead to an accident.
- **Hazard Analysis**
Process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to a tolerable level.
- **Hazard Log**
Document that records or refers to hazards identified, decisions made, solutions adopted and their implementation status.
- **Independent safety assessment**
Process to determine whether the product meets the specified safety requirements and to form a judgement as to whether the product is fit for its intended purpose in relation to safety.
- **Life-cycle**
Series of identifiable stages through which an item goes, from its conception to disposal.
- **Maintainability**
Ability to be retained in, or restored to, a state to perform as required, under given conditions of use and maintenance.
- **Pre-existing Software**
All software developed prior to the application currently in question is classed as pre-existing software including commercial off-the-shelf software, open-source software and software previously developed but not in accordance with this European Standard.
- **Product**

Collection of elements, interconnected to form a system, a subsystem or an equipment, in a manner which meets the specified requirements.

- **RAMS management process**

Activities and procedures that are followed to enable the RAMS requirements for a product or an operation to be identified and met. It provides a systematic and systemic approach to continually manage RAMS through the whole life-cycle.

- **Reliability**

(Of an item) ability to perform as required, without failure, for a given time interval, under given conditions.

- **Residual risk**

Risk remaining after risk control measures have been taken.

- **Risk**

Combination of expected frequency of loss and the expected degree of severity of that loss.

- **Risk analysis**

Systematic use of all available information to identify hazards and to estimate the risk.

- **Risk assessment**

Overall process comprising a risk analysis and a risk evaluation.

- **Safety case**

Documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements.

- **Safety integrity**

Ability of a safety-related function to satisfactorily perform under all the stated conditions within a stated operational environment and a stated period of time.

- **Safety Integrity level**

One of a number of defined discrete levels for specifying the safety integrity requirements for safety related functions to be allocated to the safety-related systems.

TFFR [h ⁻¹]	SIL attribution	SIL qualitative measures
$10^{-9} \leq \text{TFFR} < 10^{-8}$	4	Defined in sector-specific standards
$10^{-8} \leq \text{TFFR} < 10^{-7}$	3	
$10^{-7} \leq \text{TFFR} < 10^{-6}$	2	
$10^{-6} \leq \text{TFFR} < 10^{-5}$	1	

Table 1: SIL quantitative and qualitative measures [Ref.2][Ref.1]

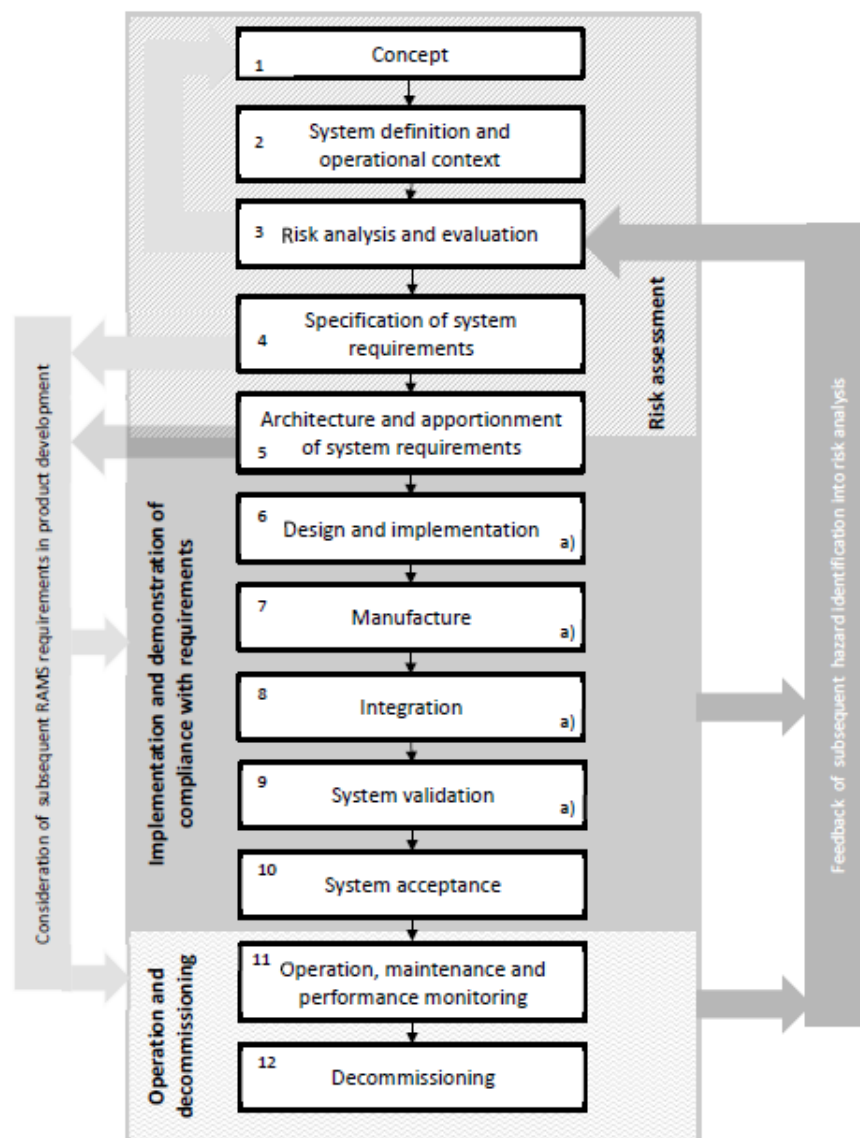
- **Safety plan**
Documented set of time scheduled activities, resources and events serving to implement the organisational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project.
- **Sub-system**
Part of a system, which is itself a system.
- **System**
Set of interrelated elements considered in a defined context as a whole and separated from their environment.
- **Systematic failure**
Failure that consistently occurs under particular conditions of handling, storage or use.
- **Validation**
Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.
- **Verification**
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
- **DeBo**
A body designated by a member state with the task of checking the conformity of a subsystem with national rules.
- **NoBo**
The body designated by a member state, to assess the conformity or suitability for use of interoperability constituents or for the establishment of the EC verification procedure of the subsystem.

- **Generic Application**
System with specific functions that are related to “a category of applications” associated with a general environmental and operational context, developed on the basis of standardisation criteria and parameterisation of its elements, so as to make it usable in various real applications.
- **Specific Application**
A configured generic application used only for a particular installation.
- **Authorisation for use**
Final act of a process through which the correspondence of a generic application, a generic product or a component to the security requirements defined by the technical standards applicable to it.
- **Authorisation for placing in service**
Conclusive act of a process through which compliance of structural subsystems with safety requirements defined by the applicable technical standards are certified.
- **Commissioning**
Final act of a process through which the railway companies and infrastructure managers put a structural subsystem in operating state for which the certificates and permits were issued, under applicable regulations.
- **Independent Safety assessor**
The body authorised by the agency responsible for assessing compliance of a vehicle, structural subsystem, generic application, generic product or component with the requirements of security defined by the national technical standards applicable to them and the suitability for use of the same, and/or instructing the procedure for authorising the placing into service and/or use, at the request of an applicant.

1.2 CENELEC life-cycle phase

The process of safety management and assessment of safety conformity of a product is a complex process which requires careful planning, tracking of development and validation at each stage aided by expertise to manage the applicable procedures. CENELEC has meticulously set up a standard procedure which makes the management of safety requirements well-structured and comprehensible, which is defined in the standard EN 50126:2017 [Ref.1].

This standard falls in the category of Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), and is divided into two parts.



a) May contain many subsystem and components

Figure 1: Interrelation of RAMS management process and system life-cycle [Ref.1]

The first part enlists the generic RAMS process while the part 2 deals with the systems approach to safety, applicable to railway applications fields, namely Command, Control and Signalling, Rolling Stock and Fixed Installations. This standard is independent of the technology used and outlines the procedure for obtaining the authorisation for the final prototype.

According to CENELEC, EN 50126 Standard promotes co-operation between the stakeholders of Railways in the achievement of an optimal combination of RAMS and cost for railway applications. Adoption of this European Standard will support the principles of the European Single Market and facilitate European railway inter-operability

For an effective RAMS management, the product life-cycle approach is defined by CENELEC. It provides a structure for planning, managing, controlling and monitoring all aspects of the system under consideration, as it passes through the different phases of its life-cycle, from its conception to disposal. This model is fundamental to the successful implementation of EN 50126:2007.

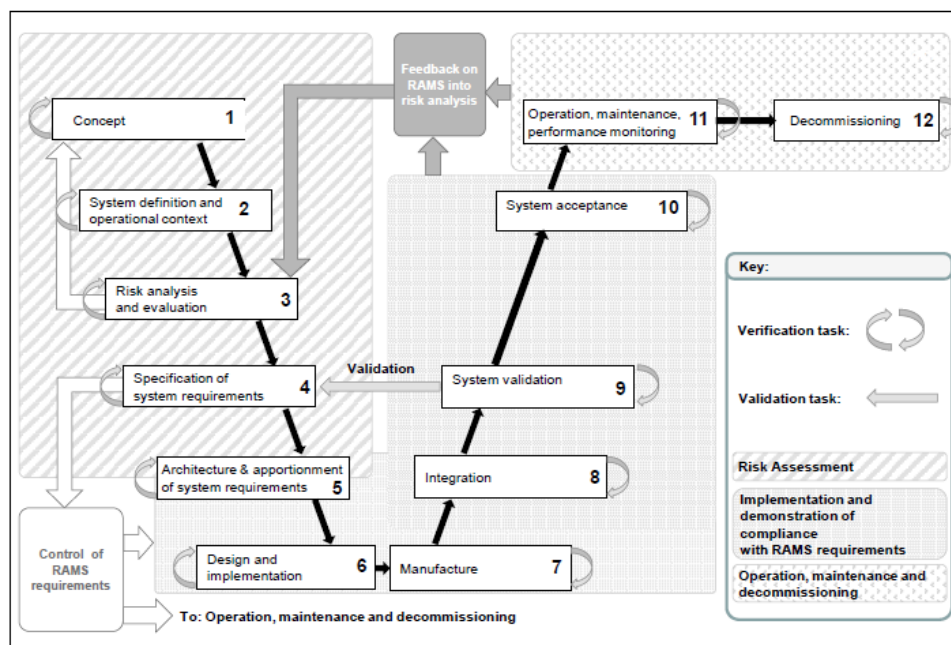


Figure 2: The V-cycle representation [Ref.1]

The product life cycle is represented in the shape of the alphabet “V”. The left (top-down) branch is called “development”, which ends with the manufacturing phase. The right (bottom-up) branch represents the assemblance, installation, handing over and the operation and maintenance of the whole system. The life cycle phases are represented inside the numbered box in Figure 2, and the RAMS task along the life cycle phases are tabulated in Appendix A.

2 Procedure in Italy

After the fulfilment of the RAMS management, the NSA regulations comes into place for individual member countries. The Italian NSA (ANSF) have approved a procedure to be followed for the final authorisation in the “Guidelines for release of authorisation for placing in service of vehicles and structural subsystems and authorisation to use generic applications, generic products and components (*Linee guida per il rilascio dell'autorizzazione di messa in servizio di veicoli e sottosistemi strutturali e dell'autorizzazione all'utilizzo di applicazioni generiche, prodotti generici e componenti*, 2017)”[Ref.3].

The *Agenzia Nazionale per la Sicurezza delle Ferrovie* (ANSF) is the Italian National Safety Authority (NSA) for railways. Based in Florence, with offices also in Rome and in other Italian main cities, ANSF is active since June 2008, according to article 4 of the Legislative Decree 10th of August 2007 no. 162 (the Italian law implementing the Safety Directive 2004/49/EC) [Ref.9].

The Ministry of Infrastructure and Transport supervises the NSA activities. The agency is technically independent from all the railway operators: it guarantees a non-discriminatory treatment to all the subjects related to the railway transportation [Ref.9].

The agency has clearly set out procedures to follow for obtaining the authorization to put railway products and applications in service. These procedures are an extension of the broader European procedures as regulated by CENELEC.

In the subsequent sections, the procedure to obtain an Italian APIS for a structural subsystem is briefly explained.

2.1 Powers and Responsibilities

2.1.1 National Agency for the Safety of Railways

The agency (ANSF) is responsible for:

- defining the technical standards applicable to vehicles, subsystems, general purpose, generic products components for the verification of the correspondence of the same to the requirements for the granting of commissioning and use;
- in the case of renewal or upgrading of subsystems, to decide whether the size of the works means that a new authorization for placing in service within the meaning of Legislative Decree no. 191/2010, as amended;
- release the authorization for placing in service of subsystems and vehicles and the use of own generic applications and generic products or components;

- guidelines for the commissioning authorization service of vehicles and structural subsystems and authorization to use generic applications, generic products and components;
- authorization to make the online test drive vehicles and in the field of sub-tests structural, generic applications, generic products or components;
- inform the EUAR (European Union Agency for Railways) if granted, modified, suspension or revocation of authorization.

2.1.2 Independent Safety Verifier

The ISA is an accredited body, appointed by the agency. Italcertifer is one of the approved ISAs for recognised by ANSF.

The Independent Auditor of Security is responsible for:

- Through field tests, to evaluate the consistency between the configuration described in the technical documentation and the state of the subsystem to be measured;
- Where the risk assessment body, evaluate the adequacy of the application procedure risk management in to Regulation (EU) 402/2013, as amended, and the related results, even in case of performing in-line tests;
- as appointed body, assess the completeness and relevance of the list of specifications and standards national reference techniques produced by the Applicant and transmitted when initiating the technical procedure;
- inform the Agency approvals of quality management systems issued and withdrawn, and, periodically or upon request, make available to the Agency the list of the system of approvals quality management refused, suspended or otherwise restricted;
- submit to the Agency request for temporary authorization to the execution of test runs in line of vehicles.

2.1.3 Applicant

The applicant is the body which request the authorization from the agency, and is responsible for:

- forwarding the application to the Agency for the authorization for commissioning in service or the authorization to use generic applications, generic products or components;
- guidelines for the authorization of commissioning in service of vehicles and structural subsystems and authorization to use generic applications, generic products and components;

- appoint a body or bodies to carry out the role of CSM assessors as regards the activities covered by Regulation (EU) 402/2013 [Ref.4];
- instruct an DeBo for the application of the "EC" verification procedure of subsystems as regards the verification of conformity to national rules;
- appoint a NoBo for the application of the "EC" verification procedure as regards the verification of compliance with the TSI;
- appoint a VIS (Verificatore Indipendente di Sicurezza, ISA) to perform its duties referred to in §2.1.2;
- to entrust a railway company, whose SMS foresees the carrying out of online testing activities, to acquire the traces and to conduct the service for the possible execution of tests on line;
- in the role of applicant for the "EC" verification (see §2.1.3.1), draw up the "EC" declaration for the verification of the subsystems referred;
- adopt, where required by the relevant modules for the conformity assessment verification procedure, the suitability for use and "EC" verification, a quality management system approved by the NoBo and / or by the DeBo which also covers the production, inspection and testing of the subsystem concerned;
- in the role of proposer, carry out the risk management process, also for the execution of on-line tests;
- provide the Agency with technical documentation to demonstrate the compliance of vehicles, subsystems, generic applications, generic products or components to the safety requirements defined by technical standards as applicable to it;
- carry out the analysis of non-intrusiveness of the structural changes to the ground subsystems in operation necessary for carrying out the tests and submit it to the opinion of the IM;
- establish and maintain, ensuring the integrity and consistency, throughout the whole life-cycle, a copy of technical file accompanying the "EC" statements and contains the details of the project;
- insert in ERADIS the statements of reference of the "EC" verification.

The applicant, in the role of proposer, must make use of an organization and competent personnel deputed to:

- carrying out the activities provided for in Regulation (EU) 402/2013 [Ref.4], as amended (including the preliminary assessment potential impact of the change on safety and the relevance or otherwise of the same);
- taking into account the requirements of the contract;
- commission and check the documents of analysis of risk and overall system specification;
- commissioning the specification document of the system requirements;
- analysing the evaluation report;

- issuing the security agreement.

Within the Safety Management System or equivalent the applicant, in the role of proposer, must ensure that the following procedures are defined:

- procedure for the identification of all the components / subsystems for which it has been authorized for use. They must be catalogued by version and fields of application and for each of them the product / system version must be clearly identified that have undergone a security setup and authorization process;
- procedure for identifying changes relating to safety;
- procedure for the management of any non-conformity that existed at the moment of the year. In it the use of the adopted monitoring tool must be defined, clarifying responsibilities, methods and timing of the individual non-conformities, until their complete resolution;
- procedure related to the whole process that goes from the conception and definition of the functional and technical requirements of security until the development of the systems / subsystems and the test phase, verification and validation. In it the definition and management of risk acceptance criteria allowed must also be included;
- procedure for creating and managing the register of hazards;
- procedure for the preparation of operating and maintenance instructions;
- procedure for document management.

2.1.3.1 Applicant for the "EC" verification and applicant for an authorization for placing a subsystem in service

In the Legislative Decree no. 191/2010 [Ref.5], the term "applicant" appears in several articles and annexes but not always refers to same figure nor must always be the same organism.

The applicant for the "EC" verification is the body responsible for the compliance of the subsystem to TSI / national standards and other rules applicable.

The applicant for the "EC" verification is responsible for:

- the design, manufacture and final testing of the subsystem. He is responsible for design and construction of subsystem even if some of the same elements have been designed and manufactured by others;
- the preparation of the "EC" verification, which must be performed by a NoBo / DeBo;
- the drafting and signing of the "EC" declaration of subsystem.

The applicant for the "EC" verification may delegate or subcontract certain tasks relating to a subsystem (such as design, manufacture and final tests), but retains overall control and responsibility of the subsystem as a whole and remains responsible for the declaration of "EC" verification,

Finally, the applicant for "EC" that draws up the declaration of verification "EC" must be the same that got the "EC" certificate of type examination.

If certain parts or stages of the subsystem are the subject of an intermediate statement of verification (see §2.3.3), the bodies completing the verification certificate can be different from the person / body that drafted the intermediate verification statement.

2.1.4 Railway Undertaking

The Railway Undertaking, in accordance with the procedures of its SMS for conducting the test runs on line vehicles, is responsible for:

- carrying out the activities of conduct and escort of the vehicle in the case of execution of tests on the lines for which a safety certificate has been issued by the agency;
- enacting the provisions and operating requirements for conducting the test runs in the line;
- and, in the case of involvement, issue, to the extent applicable, the provisions and operating requirements for carrying out the tests in the field of a structural subsystem or parts of it;
- enacting, even in case of on line testing, the Special Circulation Regulation (DPC, Disposizioni Particolari di Circolazione).

2.1.5 Infrastructure Manager

It is a body or undertaking entrusted in particular with the implementation of the maintenance of railway infrastructure and the management of control and safety system infrastructure and railway traffic. The task of the IM is constrained and defined in EU and national regulations. [Ref.1]

In Italy, the infrastructure Manager for the railway network is RFI (Rete Ferroviaria Italiana).

The IM, in accordance with the procedures of its SMS relating to the execution of tests on the line, has the task of:

- enacting the provisions and operating requirements, including the interface procedures between their own personnel and that of the RU, for performing field tests of structural subsystems, which takes into account:

- the safety acceptance dossier for the definition of the conditions of circulation predisposed by the applicant;
 - the current financial year legislation (Annex B to the ANSF Decree 04/2012 – Regulation railway traffic);
 - the technical conditions of the structural subsystem (or part of it) to be tested;
 - specification of the activities;
- where the case occurs, preparing the special operating provisions (detailed instructions) for the authorization for placing in service the CCS structural subsystems on land, energy, infrastructure and for the authorization of the use of generic applications, generic products or components;
 - provide, when requested by the parties concerned to on-line tests, information on characteristic infrastructure data that allow the defined set of tests to be performed and effective performance of the same;
 - verify the analysis of non-intrusiveness of changes to the necessary structural subsystems in operation for carrying out the tests, carried out by the applicant, and issue an opinion on the applicant.

The IM must, however, endeavour by any means, in consultation with the applicant, that all possible necessary tests are carried out within three months of receiving the application by the applicant.

2.2 Technical Procedure

2.2.1 Commissioning of structural subsystems as a result of modification

Whenever an intervention is expected on a structural subsystem in operation, it is up to the applicant to determine the type and extent of modification to be made.

2.2.1.1 Owner of Authorisation

Except as provided in the following paragraph, the only person entitled to make an application of any kind modification of a structural subsystem is the owner of the existing authorization for putting in service structural subsystem itself. This does not preclude the possibility that such person, during the authorization process collaborate with other parties (IM, RU, suppliers, etc.); however, only the holder of the authorization may approach the agency in the role of the applicant.

This does not preclude the possibility that another person, different from the owner of the existing permission for commissioning, may acquire, in the manner permitted by law, the legal right to change the structural subsystem.

2.2.1.2 Authorization type: New or Modification on an existing system

In the context of these guidelines, “new” authorisation shall be construed as one that must be issued to new subsystems or to changes involving the same.

In the case of generic applications and generic products, the variation of the configuration is described in the relevant safety case and / or the application context associated with the current authorization.

In the context of these guidelines, it is to be understood as permission "to date" that must be issued in the face of changes in the case of generic products and generic applications, but not covered by the previous paragraph.

2.2.2 Authorization to use generic and first specific applications, generic products or components

The authorization referred to in this paragraph shall be issued by the Agency on the following criteria:

- a) The authorization procedure applies to the development and realization of generic applications, or individual generic products or safety components for railway signalling, trackside and on-board;
- b) The authorization issued for generic application on the basis of the first specific application realized, is valid, without further intervention by the Agency, also for all subsequent specific applications, provided that they are in accordance with the application context in which said generic application and the first specific application has been authorized, i.e. as long as the **functionality, the points of interaction, the operational circumstances and environmental conditions** remain unchanged and that their safe integration is guaranteed. Similarly, the authorization issued for the use of the generic product or component, is valid without further interventions Agency for use in other applications of the same generic product or component, provided that it conforms to the application context in which said generic product or component has been authorized, i.e. as long as the functionality, the points of interaction, the operational circumstances and conditions environmental are the same and that their safe integration is guaranteed. The evaluation of these conditions must be carried out by the

applicant / person responsible for placing into service in accordance to Regulation (EU) No. 402/2013 [Ref.4];

- c) If the authorized generic applications (concurrently with their respective first specific application) are combined together in order to meet a specific need, this new configuration will constitute a new generic application and first specific application for which the safe integration of the various generic applications must be demonstrated that make it up, as well as the safe integration with the context in which it will be used.
- d) Whenever the applicant intends to commission a specific application resulting from the authorized configuration of the generic application, including the first specific application, such activities must be managed with particular attention to the need to reauthorize the structural subsystem referred to this specific application which will constitute an integral part;
- e) It is the obligation of the Infrastructure Manager prior to the putting into service of a specific application, a generic product or component connected to the network to ascertain the compliance of the various constituent elements of the system with those of the authorized project and filed with the Agency, which is the basic norm for subsequent modifications;
- f) In the case of subsequent supplies of generic applications, generic products or components confronting to those subject to prior authorization, it is also the duty of the Infrastructure Manager to acquire the declaration of conformity by the manufacturer both for the hardware and the software version implemented;
- g) Generic products or safety components for railway signalling for which specific request for authorization to use has not been made, but integrated into a generic application for which has been granted authorization for use, means it is authorized also for use as a single product or component. This is provided that such generic products or components are clearly identified inside the generic application that integrates them, and they are accompanied by specific safety case. In addition, functionality, the points of interaction, the operational circumstances and environmental conditions context in which the new application will eventually be used must be the same of the authorised first generic application to which they belonged; their safe integration must finally be guaranteed. The evaluation of these conditions must be carried out by the entity in charge of putting into service / use in accordance with Regulation (EU) No. 402/2013 [Ref.4];
- h) Generic products or safety components for railway signalling and generic applications (and their first specific application) for which a specific request for authorization to use has not been made, but integrated into a structural subsystem CCS (on-board or on the ground) for which commissioning authorization has been granted, the latter is also authorized for use as a single generic products or

components and generic/specific applications. This provided that such generic products or generic components and applications/specifications are clearly identified within the subsystem that integrates them, and they are accompanied by specific *safety case*. In addition, the functional, operational and environmental conditions of the new context in which they will be might be used must be of the same structural subsystem of which they were authorized part; their safe integration must finally be guaranteed. The assessment of those conditions must be carried out by the applicant / entity in charge of putting into service / use in accordance with Regulation (EU) No. 402/2013 [Ref.4];

- i) Specific authorization for individual components intended for use in a different context from railway signalling (e.g. exchanges, brake discs, brake linings, etc.) are not provided. Their use is authorized under the structural subsystem or part of it in which these components are integrated and for which the Agency has issued authorization for placing in service. However, except as art. 19 of Legislative Decree. 191/2010, the aforementioned components can be used for other part modifications of the subsystem concerned, provided they are always accompanied by a safety dossier prepared by the manufacturer and provided that the functional, operational and environmental conditions remain unchanged. The evaluation of these conditions must be made by the applicant, in accordance with Regulation (EU) No. 402/2013 [Ref.4].

2.3 Authorization procedure for the structural subsystems

In the case of ground subsystems authorized to be placed in service, it will be defined on a geographical basis by taking progressive kilometric reference which delimit the part of the rail system in which the above-mentioned subsystems are inserted. The limits may be different for each subsystem examined. It is desirable that both of bounded parts are as homogeneous as possible with regard to the technical characteristics of the subsystem of which such approval is requested.

2.3.1 Start of the technical process

The request to start the commissioning authorization procedure for commissioning in service of those structural subsystems referred to in this section must be received by the Agency by the applicant.

This request must be accompanied by the following preliminary documentation:

- a) Technical documentation illustrating the subsystem subject to the authorization request. This documentation, which must contain all the elements necessary to

identify, unequivocally, the boundaries of the subsystem (including, by way of example, the precise indication of the components of the subsystem from authorize installed at the limits of the subsystem itself), must be composed of:

- a. descriptive report of the subsystem adapted to illustrate the configuration to be authorized and its general technical characteristics;
- b. drawings, required to enable the identification of typological characteristics, spatial, functional and technological subsystem to be authorized. In particular, for the Control and Command and Signalling trackside subsystems: drawings (plans or schematic block diagrams) with evidence of the limits of the subsystem, and / or summary tables;
- c. for the Control and Command and Signalling trackside subsystem: description of any generic applications that make up the sub-system and, where required, will be subject to specific authorization as defined in §2.4 (also in this regard, please refer to §2.2.2 letter h).

The level of detail and the scale of representation of the documents described above must be consistent with the level of development of the design of the subsystem subject to the authorization request;

- b) List of the specifications and technical standards which the applicant intends to use for the demonstration of compliance of the subsystem with the requirements for the issue of authorisation. This list must be accompanied by one of the evaluation reports on the completeness and relevance of the documentation itself, drawn up by the evaluation bodies (DeBo / NoBo) appointed by the applicant. Application exceptions of the relevant TSI must be managed;
- c) Evidence of compliance with the requirements of all the principles of the Regulations for Rail Traffic with respect to which the subsystem of the application for authorization is meant to declare conformity to, and which have relevance for the purposes of the regulation;
- d) General program for the performance of activities provided in the authorization process in which they are content timing and the manner in which the applicant intends to deal with the phases of the authorization process; the program must contain the following minimum information:
 - a. description of the stages of development of the authorization process of the subsystem which take into account, where expected, verification of compliance with TSI and the national rules, of technical compatibility and safe integration of the subsystem with the network;
 - b. list of persons involved in each of the phases and the responsibilities of each;

- c. documentation of the plan;
- e) Of the preliminary version of hazards and associated risks.

It is understood that if part of the aforementioned documentation has already been presented attached to the file provided for by art. 19 of Legislative Decree no. 191/2010 [Ref.5] in the event of renewal or restructuring, what is required by the aforementioned points a) -e) is to be considered as an integration of what has already been delivered to ANSF.

The provisional program for the conduct of the authorization process will be updated during the course the authorization process in relation to the changed circumstances.

Within one month of receiving the request, the Agency shall convene by the requesting a meeting with the applicant, the Independent Auditor of Security and, where required, the NoBo appointed by the same applicant. On this occasion, the applicant will carry out a presentation attached to the documentation required.

Within the month following the date of such meeting, as they fulfil the conditions, the Agency shall issue the authorization for the development of the subsystem subject to the authorization request, or notify any additions and amendments to the proposal documentation.

In the latter case, within one month of receipt of additional documentation, if required, or within a month from the date of the hearing, the Agency, as they fulfil the conditions, release the authorization for the development of the subsystem subject to the authorization request.

After the definition of the preliminary documentation activities of the applicant, with reference to the program agreed, it may proceed with the sending of technical documentation as provided from the plane of documentation.

The above-mentioned clearance, to be construed as opinion feasibility of the project as described in this preliminary phase, it constitutes a necessary condition to proceed with the subsequent stages of the authorization process.

2.3.2 Evidence Fulfilment

For carrying out any testing activities that have relevance for the authorization of commissioning structural subsystems apply, in principle, the same rules defined in "Testing of validation." For other types of evidence apply, where relevant, the same principles as defined in the section "Other types of evidence."

2.3.2.1 *Switch-off facility*

In the event that the commissioning of the subsystem including activities (including trials) involving the passage without solution of continuity from the configuration during operation (hereinafter original configuration) to subentrante 13 (so-called phase *switch-off*), the applicant must define a migration process between the two configurations.

2.3.2.1.1 *Purpose*

The procedure of *the switch-off* must:

- identify the person in charge of the GI who has delegated to the commissioning of the subsystem;
- provide a comprehensive description of the work to be done, roles and responsibilities of all parties involved;
- provide for test mode that is appropriate to the verification of compliance with the essential requirements of the portion of the subsystem concerned by the *switch-off*;
- to show that the activities to be implemented in the *switch-off* does not affect the fulfilment of the essential requirements part of the subsystem portions not affected by the *switch-off* itself.

The procedure must be evaluated by a VIS in terms of completeness and adequacy of the points mentioned above.

The procedure must integrate the technical documentation in support of the "CE" declaration of verification referred to in

2.3.2.1.2 *Procedure*

The switch-off procedure includes the following activities:

- the applicant forwards the authorization for placing in service as detailed in the following point §2.3.5, accompanied by the "CE" declaration of verification and its annexes; among the attachments it will be included the aforementioned procedure and its evaluation report for the management of the activities aimed at the *switch-off*;
- the Agency, following investigations successfully, within one month of receiving the request releases authorizing the placing in service of the subsystem, which will also be understood as permission to proceed with the activities of *switch-off*. The validity of this authorization is subordinate to the success the activity of *switch-off*;

- to ultimate evidence, to which must compulsorily be present at the VIS, the GI responsible identified in procedure *switch-off*, acquired the formal opinion of the VIS on the success of their operations in proceeds the commissioning of the subsystem;
- where the activity *switch-off* highlighting critical issues related to the putting into service of the subsystem, the applicant shall, whenever possible, to identify and receiving the report about from the VIS, the implementation of appropriate mitigative measures;
- if the activity *switch-off* highlighting critical issues related to the putting into service of the subsystem for which the applicant is not able to identify appropriate mitigative measures, the applicant provides for the recovery the original configuration;
- in the case, proceed to the putting into service of the subsystem, the GI manager identified in the procedure of *switch-off* or the applicant provides to anticipate as soon as possible (but within the next two days the placing in service) to the Agency:
 - o the formal opinion of the VIS, about the success of the above activities;
 - o the act by which the GI declare the commissioning of the subsystem;
 - o about the above, if the task *switch-off* highlighting critical issues related to the commissioning which resulted in the subsystem operating / application conditions limitations, documentation of post-activation will be specifically mentioned;
- the applicant shall then send to the Agency updated documentation as a result of the above evidence. In this regard, it is understood that the only permitted changes (compared to the configuration of subsystem for which it was possibly already issued the relevant 'EC' declaration of verification) in this phase are exclusively those related to switching from the old to the new configuration of the subsystem and the relative calibration and tuning of equipment (including, where applicable, any of specific application configuration changes evaluated not relevant within the meaning of Regulation (EU) n. 402/2013) [Ref.4], which remains under the full responsibility of the applicant assessment of the need to involve a NoBo and / or DeBo for updating certificates if the relevant circumstances.

2.3.3 Intermediate statement of verification

As indicated in §2.2.1 of Annex VI of Legislative Decree no. 191/2010 [Ref.5] and subsequent amendments, at the request of the applicant, the verifications referred to in

the aforementioned Annex VI may be carried out for parts of a subsystem or be limited to certain phases of the verification procedure. In these cases, the results of the verification can be documented in an "intermediate verification statement" (DIV) issued by the appointed notified body.

In this regard, with reference to Legislative Decree no. 191/2010 [Ref.5] and subsequent amendments, the following is stated:

- the DIV should refer to the TSI with respect to which has been carried out the assessment of conformity;
- applicants may apply for an ISV for each part they decide to split the subsystem;
- each part must be checked in each stage as described;
- the DIV is only a tool for the organization of work between notified / designated bodies: Allows to prepare statements on certain parts verified with respect to some or all the steps provided for (Design, production, final test). Such statements may then be transferred to other assessors that they will not repeat the checks on those parts / phases;
- while the phases are predetermined, the parts of a subsystem may be freely identified by the applicant (depending on your needs). However, a DIV is not in all cases sufficient to require the commissioning or the entire subsystem or part thereof: for this purpose it will be necessary to produce certificate and "EC" declaration of verification complete;
- in case of a TSI makes explicit provision (as in the case of the TSI CCS), the parts in which a subsystem can be divided shall be explicitly stated in the same STI (in the case of the TSI CCS: train protection, radio communication, train detection). Should one of these parts has occurred with respect to the three phases in the normative, for this part a complete verification certificate may be issued, which it can be used to request the AMIS;
- in case they are issued the DIV, the notified body responsible for verification of the subsystem takes behalf of those and, before issuing its own verification certificate:
 - o to verify that the DIV properly covering the relevant requirements of TSI;
 - o checks all aspects that are not covered by the DIV;
 - o Verification testing of the subsystem as a whole.

2.3.4 "EC" declaration and verification certificate: Minimum content

Annexes V and VI of Directive 2008/57/EC [Ref.14], as amended, report the minimum contents, respectively, of the "EC" declaration of verification and of the technical documentation accompanying the declaration "EC" verification.

With regard to what is set out in paragraph 1, letter j) of the directive, which says that the "EC" declaration of verification must contain "*all relevant provisions, provisional or final, which the subsystems, in particular, must meet, where necessary, any operating restrictions or conditions*", it should be noted that "CE" certificates and declarations must contain only any prescriptions, limitations or operating conditions resulting from the analysis of the DeBo / NoBo, providing, however, formal evidence also of a possible absence of the same.

2.3.5 Request for putting in service

A successful conclusion of the activities of verification of conformity provided by the process, the applicant shall submit the authorization for placing the subsystem into service (if not already submitted as per §2.3.2.1), drafted and executed. The request must be in stamp duty and to provide a stamp for response.

The request must be accompanied by the following documentation:

- "CE" declaration of verification accompanied by the technical documentation defined in Annex VI of Legislative Decree no. 191/2010 [Ref.5][Ref.3] and following modifications and in particular by the following appendices:
 - verification certificate;
 - copies of the "EC" declarations of conformity / suitability for use of interoperability constituents incorporated into the subsystem;
 - if available, the / DIV accompanying (or not) the certificate of verification, including the result of verification by the notified / designated VIS about the validity of the same;
 - technical documentation attached to the said certificate, including, where applicable, the necessary data updating of the register of the national rail network, including the report of Risk Assessment (Risk Assessment Report) and its annexes, on the issues of secure integration of the subsystem with the system into which it will be used;
 - the aforementioned technical documentation must contain the documentation relating to maintenance of the subsystem;
 - the aforementioned technical documentation is to define the requirements to which the subsystem is declared;
 - the aforementioned technical documentation must provide explicit evidence of compliance of the above requirements to the safety standards as applicable to the particular subsystem;
 - verification certificates issued in accordance with other legislation deriving from the Treaty, referring to the relevant EU legislation including all relevant national rules;

The request must indicate the name of the person responsible and the place of record-keeping.

2.3.6 Releasing of APIS

The process to be followed for the authorization for placing in a structural subsystem is specified in Chapter IV of Legislative Decree no. 191/2010 [Ref.5], detailed in Annexes V and VI of the same Decree. In this regard, it is noted that the procedures of "EC" verification that the subsystems are identical for both aspects covered by TSI and for those covered by national standards: the completion of such verification procedures will enable the applicant, if the circumstances so conditions, to declare, under its sole responsibility that the subsystem concerned satisfies the requirements of relevant EU legislation including all relevant national standards.

Therefore, NoBo DeBo and carry out its own activities and collect relevant evidence gathered in the certificate of Verification of Annex VI of Legislative Decree no. 191/2010 [Ref.5]. This certificate:

- must indicate the TSI in respect of which the evaluation of conformity was carried out;
- when a subsystem has not been assessed for its conformity with all relevant TSI (e.g. in case derogation, partial application of TSIs for upgrade or renewal, transitional period in a TSI or case specific), it must provide the precise reference to TSIs or their parts whose conformity has not been examined by the notified during the verification procedure;
- if they apply to national rules, it must contain a precise reference to the national standards whose conformity has been examined by DeBo,

In the limiting case where the "EC" verification procedure is to be completed with respect to the exclusive application of rules national, the verification process still leads the issuance of a verification certificate from the DeBo.

The verification certificates, usually distinguished by portions attributable NoBo / DeBo, can form single document if the role of NoBo and DeBo is covered by the same body.

For structural subsystems of land that fall outside the scope of the TSI, the modules to be used for National Audit process are the same as those provided by the TSI to which the subsystem can be traced. Specifically, the central should be treated in accordance with the TSI of Control-Command and Signalling. The modules provided by these documents (certificates / certificates, declarations) also covers the "EC" verification of general applications, generic products and components forming parts of the CCS subsystem

concerned. For the verification of these elements nevertheless apply CENELEC process, as provided for in section §2.4.

A successful conclusion of the permitting process, including the verification of the payment of relevant costs, the Agency shall issue the document of the Authorization for placing the subsystem into service, as first authorization or following its amendment.

Such authorization may be issued in temporary form in the event that the Agency considers that the subsystem can be put into service under conditions or requirements.

Where an application for authorization has covered the entire subsystem (case considered in this paragraph), it is not expected to issue a separate license to use for generic applications (first and specifications) and for generic products or components forming part of the authorized subsystem, except in the case in which are presented explicit requests (even by different requesters) with separate instances in accordance with the normed to §2.4.

2.4 Procedure for authorization to use generic applications and first specific, generic products or components

The verification is carried out according to the CENELEC process, as specified in the following points.

2.4.1 Start of the technical process

The request to start the licensing procedure with the use of generic applications (first specifications), generic products or components for railway signalling, ground and on board must be received by the Agency by of the applicant, through an application signed by the applicant.

This request must be accompanied by the following preliminary documentation:

- descriptive GA / GP relationship or component containing at least the following elements:
 - application context: the description must be with sufficient level of detail of functionality, the points of interaction, the operational circumstances and environmental conditions of use;
 - functional description;
 - preliminary assessment of the applicability of the TSI and national rules. Exceptions application of the relevant TSI will be managed on the basis

of the provisions of art. 8 of the Legislative Decree no. 191/2010 [Ref.5], as amended;

- configuration to be authorized, including its technical characteristics;
- preliminary version of the Plan Documents containing a reference list of the specifications and technical standards that the applicant intends to use for the demonstration of compliance GA / GP or component with the requirements for the release of authorization. Such list shall be accompanied by one or more evaluation reports regarding the completeness and relevance of the documentation, written assessment bodies (VIS / DeBo / NoBo) instructed by the applicant;
- evidence of compliance with the principles of the Regulations for Rail Traffic of all requirements with respect to which the generic application (first specification) / generic product or object component of the request for Authorization is meant to declare conformity, and that are relevant for the purposes of the same Regulation;
- preliminary version of hazards and associated risks;
- list of subjects that the applicant intends to engage in the authorization process, including the / name/s VIS and any notified / designated body that the applicant wishes to instruct;

It is understood that if part of the above documentation has already been submitted attached to the file referred to art. 19 of Legislative Decree. 191/2010 [Ref.5] in the case of renewal or restructuring as requested to the above points a) -f) is considered as a supplement to the documents already handed over to the ANSF.

Within one month of receipt of the request by the applicant, the Agency shall convene a meeting with the applicant, the Independent Auditor of Security and, where required, with the notified body appointed by the applicant. In that seat, the applicant makes a presentation of the documents attached to the request.

Within the month following the date of such meeting, as they fulfil the conditions, the Agency shall issue the no objection certificate to the generic application development / generic product or object of the required component authorization, or notify any additions and amendments to the proposal documentation.

In the latter case, within one month of receipt of additional documentation, if required, or within one month from the date of the hearing, the Agency issues the certificate.

The above-mentioned clearance, to be construed as feasibility opinion of the project as described in this preliminary phase, constitutes a necessary condition to proceed with the subsequent steps described below.

2.4.2 Definition of processes

The authorization for the use of a generic application, a generic product or component is based on documentary evidence that the applicant will produce towards the Agency in the course of the procedure described below, and which will be collected in the safety acceptance dossier. This dossier, drafted by the applicant, will also contain one or more evaluation reports produced by / in charge VIS.

The safety acceptance is the final act of the activities carried out by the applicant for a specific phase. It determines the validity of the certification of and suitability of the documents issued in the subject process, and includes the positive verification the documents.

Based on the results produced by the VIS, the applicant shall ensure:

- the completeness and adequacy of the requirements of the safety functions and those related to the integrity of the of applications and security products in question (SRS);
- the validity and adequacy of provisions and operating requirements and maintenance applied;
- the validity and adequacy of the safety management process, which also includes the identification of hazardous situations and of the solutions adopted (hazard record);

And, in particular, the safety acceptance file must contain at least the evidence relating to:

- generic definition of the application / generic product;
- sufficiently detailed definition of the application context, namely the definition of functionalities, points of interaction, the operational circumstances and environmental conditions of use;
- provisions of applicable laws;
- definition of the applicable requirements and evaluation of the functional aspects;
- evaluation of the safety aspects, including the compliance of the above requirements the principles of safety, for as applicable to the GP / GA under review;
- problems that emerged during the evaluation of the functional and safety aspects;
- intrusiveness of analysis for the existing rail system;
- the hazard record;
- configuration;
- verification of the technical compatibility and safety conditions with the structural subsystems involved;
- the security plan.

In this dossier the evidence will also be given of:

- assumptions (with the definition of the mission profile);
- application conditions;
- provisions and operating requirements and maintenance;
- system requirements;
- deviations and exemptions from the standards;

related to the authorization request.

The VIS should assess the entire authorization process, and in particular the adequacy, correctness and completeness:

- of the definition of generic / generic product application and its application context;
- of identification of the hazard and related risk analysis;
- of the phases of the risk assessment and acceptance (acceptance criteria properly applied);
- of the demonstration phase of compliance with safety requirements (safety measures identified effectively implemented - Acceptance by the operators of the application conditions to them exported);

of the hazard record.

The process described below includes the demonstration of safety requirements of the generic application, generic product or component subject to authorization, and verification of technical compatibility and safe integration of these subsystems within which they will be integrated.

2.4.3 Procedure for the granting of use

The release of the authorisation by the Agency to use generic application (and first specification), a generic product or component is based on the security of acceptance dossier drawn up by the applicant and its annexes.

2.4.3.1 Preparation of risk assessment documents and demonstration of compliance with security requirements

The activities described in this chapter are carried out by the applicant and provide a final evaluation on the part of VIS.

In this phase, the applicant, through its technical body, carries out the V&V activities provided by its own system Security Management or equivalent.

The applicant must provide for the creation of all documentation agreed with the VIS and reported in the Plan of Security for the stages 2-10 of the standard EN 50126 [Ref.1][Ref.2]. If the generic application includes interoperability constituents, documentation will be supplemented by the conformity / suitability certificates for use of the components.

The applicant must document the risk assessment process used to evaluate the levels of security and compliance with previously defined security requirements, so that all documents necessary to demonstrate the correct application of the risk management process are available to the body for assessment of risk. It must also include the technical assessment of the suitability of a product / application station its intended use based on compliance with the prescribed conditions.

If it becomes necessary to carry out field tests with impact on a system in operation, these tests, defined by the applicant, they are subject to explicit authorization issued by the Agency.

2.4.3.1.1 Tests

The process of development and commissioning of a generic application or a generic product or component requires, normally, the execution of laboratory tests and field trials.

In order to define the roles and responsibilities of those involved in the trials, it is helpful to divide the same into categories identified on the basis of finalization criteria, localization and executive mode.

Finalizing :

- tests for the definition of the functional requirements of the system specifications;
- evidence regarding the development;
- tests for the verification of the safety requirements as part of the V&V process defined manufacturer by the standard EN 50126 [Ref.1][Ref.2];
- tests of system validation aimed at the independent evaluation of the results of the V&V activities part VIS / NoBo, pursuant to standard EN 50126 [Ref.1][Ref.2];
- tests aimed acceptance of the system (in the case in which the applicant is a IM or a RU):
 - o without switch-off facility;
 - o with *switch-off* system;
- tests for the verification of contractual requirements in the context of the relationship between the client and supplier.

Execution method:

- instrumental tests;
- functional tests.

As described in the following paragraphs, about the possibility of some tests under the direct responsibility of the IM applies to the CCS subsystem only when issuing permits related to a GA / first specification, where such a process requires the use of instrumental vehicles already registered in the European register, the usage limitations resulting from the restrictions and conditions authorized for the vehicles themselves.

Among the types listed above, the tests that are of interest to the Agency for the purposes of start-up action are those of validation and acceptance of the system, with respect to which the Agency must always be informed by the applicant.

This information is expressed by the applicant by sending its programming to the Agency sufficiently in advance.

Validation Tests

The system validation tests, whether they are made in the laboratory or in the field, always require the involvement of a VIS that, in addition to the usual role of risk assessment body and will also serve the additional roles under specified:

- Field tests: *Test Manager*.
- Laboratory tests:
 - o or if the laboratory is accredited: no additional role;
 - o or if the laboratory is not accredited;

Other types of test

All test types other than those of system validation fall under the direct responsibility of the IM that will supervise the execution of the same and coordinate all the parties involved (manufacturer, technical support teams, IM, laboratories, etc.).

These tests can be performed in the field without involvement of the Agency to the following conditions:

- exclusion of the part of the network concerned by the tests from the circulation and manoeuvres of trains;
- in the case of interfacing with existing systems, any kind of influence over the management of the part of network remained in operation should be excluded.

In the case where the applicant who has the need to perform field tests is a person other than the IM and the IM does not accept the responsibility for overseeing the conduct of the tests, these will take place under the responsibility of a VIS, which will act as the *Responsible Party of the tests* , with the approval of the Agency released VIS itself. In this case, the IM will ensure that the tests are carried out in a fair and non-discriminatory

terms and will to enact the provisions and the operating requirements for conducting tests that must be evaluated by the VIS. If the tests provide an authorization by the Agency, such authorization may be granted for a single test or for a group of tests.

2.4.3.1.2 Validation Tests

Where the execution of the validation tests for the purpose of issuing the authorization to use a new generic application (first specification) or a generic product or a component, must be authorized by ANSF, this authorization provides for the release of an authorization for use by the applicant for tests of the technical element to be subjected to checks and tests and an authorization for the execution of the tests, for this technical element, to the Independent Security Verifier.

2.4.3.1.2.1 Temporary authorization for use to perform validation tests

The temporary authorization to use for the execution of system validation tests is issued by the Agency applicant, following the submission by the same applicant, a specific request for authorization temporary use to perform validation tests.

The temporary authorization to use for the execution of system validation tests is issued by the Agency within one month from receipt of the request.

For the issue of such authorization, the applicant must have produced all the documentation indicated in the Safety Plan for Phase 9 of the EN 50126 [Ref.1][Ref.2] (including generic application *safety case* and first specific and, where applicable, a risk assessment report for the integration of CCS trackside and on-board subsystems) for the purpose of demonstration of the technical compatibility with the infrastructure. This proof must include the analysis of non-intrusiveness of the installations necessary for the execution of the tests and the plane of the tests to be performed.

This documentation must be accompanied by specific VIS evaluation report, which forms part of the overall evaluation report of the process of demonstrating compliance with the safety requirements.

2.4.3.1.2.2 Authorization execution of validation tests

Authorization to carry out validation tests is issued, for the technical elements in possession of the authorization for placing in service for the validation tests, by the Agency to the VIS appointed by the applicant, following the presentation by the aforementioned VIS, of specific request for the execution of validation tests.

In order to obtain authorization for the field tests, the VIS, after a specific analysis of the potential risks connected to the tests performed by the applicant, must collect and deliver the following documentation to the Agency, together with the evaluation reports produced by the same:

- general procedure for carrying out field tests;
- specific procedures for type testing;
- Operating instructions (issued by the IM or RU);
- special instructions for this (prepared by GI);
- RU indication which will be possibly involved in the execution of the tests;
- rules for the execution of maintenance interventions during the trial period (prepared by GI or IF);
- on the recommendation of the applicant, identifying the parties responsible for carrying out the tests and preparation of related reports;
- identification of the test head (in the VIS), which is responsible for orchestrating the execution of tests in the field;
- Safety acceptance dossier related to a risk analysis prepared by the proponent.

The Agency shall issue the VIS authorize the execution of the tests within one month of receipt of documentation above. Based on this authorization, the VIS oversees the installation of the necessary equipment for the implementation of test program and coordinates the evidence and the parties involved. In particular it is the responsibility of the VIS, during carrying out the tests, monitor that the same are effected in accordance to what is defined in the test plan and that, on the recommendation of the head of the laboratory or laboratories involved, the values of any parameters impacting the safety is kept within the specified limits.

2.4.3.1.3 Authorization to perform field trials

With the exception of the validation tests, in all cases in which the execution of tests requires the Agency's authorization, such authorization is as follows:

- the applicant shall send the Agency a request for authorization in the field with interference testing exercise (Movement of trains and manoeuvres);
- the request must contain:
 - o or the results of risk analysis carried out as well as the proposal of appropriate mitigations, and relative report evaluation of the VIS;
 - o or the floor of the tests;
 - o or formal evidence of acceptance by IM responsible for the execution of the role of evidence or indication that the VIS will supervise the execution of the tests (in case of failure agreement with GI);

- the Agency, where the circumstances so require, authorize the applicant.

Only where applicable, the results of these tests will be subject to evaluation by the VIS. This assessment will be part of ratio of overall assessment referred to in §11.3.2 of [Ref.3].

The Agency shall issue the authorization referred to in this paragraph within one month of receipt of the above documents.

2.4.3.2 Evaluation of the demonstration of compliance with safety requirements process

The VIS draws its conclusions as part of a final safety evaluation report (final safety evaluation report). This report must be consistent to the end of its acceptance by the applicant.

2.4.3.3 Acceptance of Safety

Act of the applicant who, through the updating of the security dossier acceptance, ensure that all activities for the safety acceptance of the organizational units involved in safety management process have been successfully completed.

2.4.3.4 Request for authorization for use

Once it has reached the end of the requirements of the authorization process, including the creation of all the documentation agreed with the VIS and reported in the Security Plan for the stages 2-10 of the standard EN 50126 [Ref.1][Ref.2], integrated by "EC" certification for conformity / suitability for use of generic application in interoperability constituents may be included, and using in the safety acceptance dossier, the applicant must send the Agency request for authorization to use generic application (first specification), of generic products or components. This request must be on stamped paper and require a stamp for the reply.

2.4.3.5 Authorization for Use

Concluding Act of the development process, carried out by the Agency, through which is attested, on the basis of the dossier of safety acceptance, that the generic application (in the configuration indicated by the respective first specific application) or the generic product or component is suitable and usable in the shown application contexts, on railway installations specified by the applicant.

Such authorization may be issued in temporary form in the event that the Agency considers that the GA, the GP or component can be used under conditions or requirements that must be resolved within a specified time span.

2.5 Managing requests for exemption

Where the need for exceptions from the application of TSI, the procedure laid down in Article 8 of Legislative Decree no. 191/2010 [Ref.5] is applied.

Where the need for exemptions from compulsory national technical regulations arises, the applicant must demonstrate compliance with the safety requirements through alternative measures, supporting the demonstration through an appropriate risk analysis, which will be submitted to the evaluation of the VIS and acceptance of the Agency.

2.6 Overview

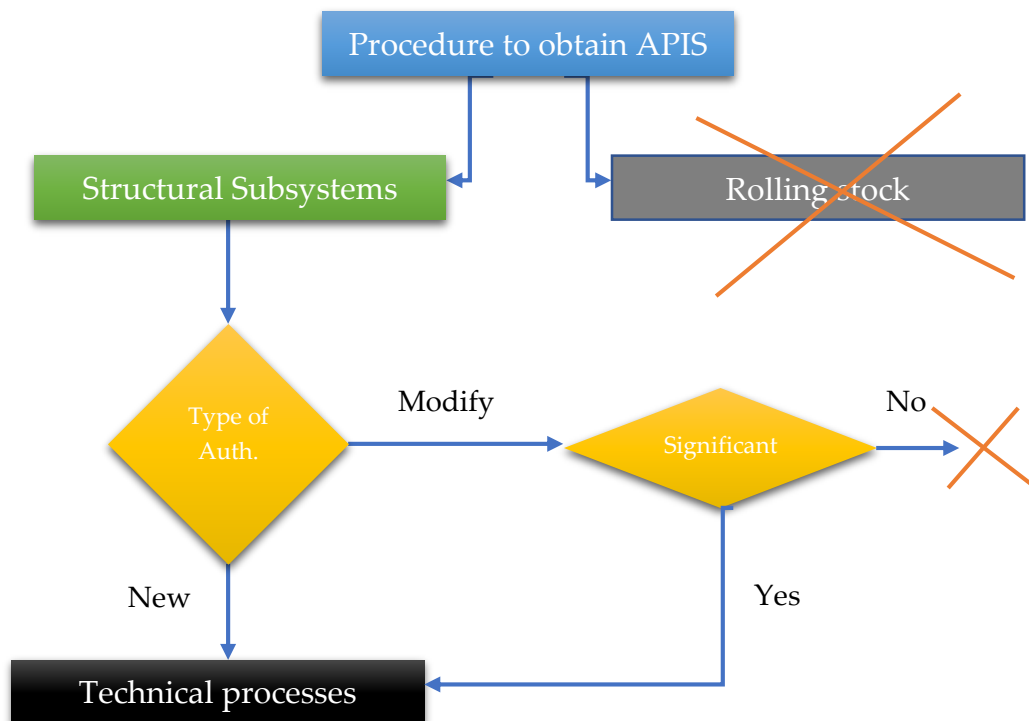


Figure 3: Overview of the process within the scope of this study

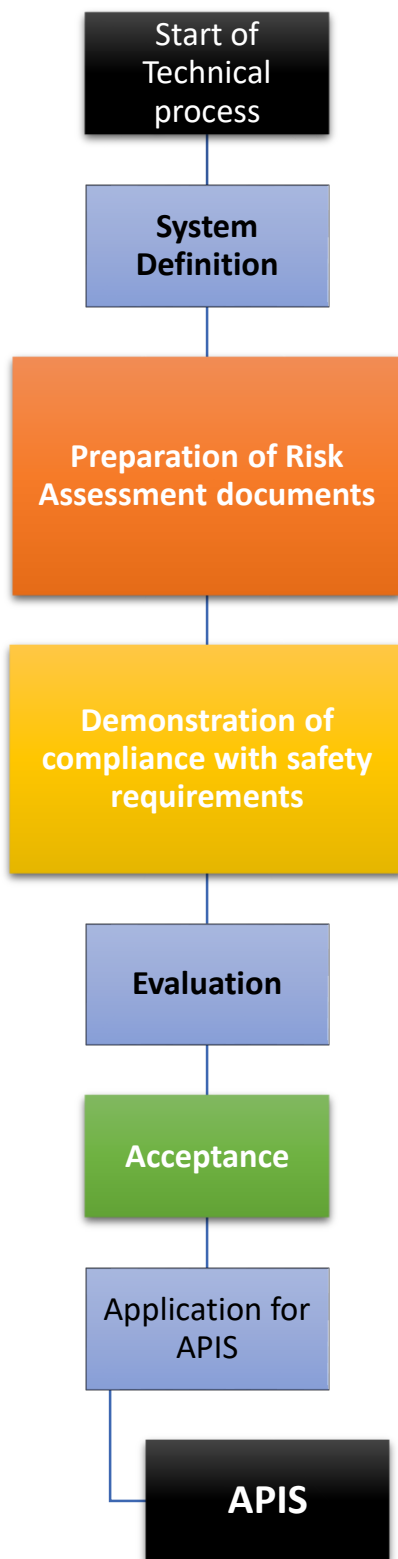


Figure 4: Flow of the technical process for obtaining APIS

3 Procedure in India

Railways were introduced in India in 1853 and as their development progressed through to the twentieth century, several company managed and systems grew up. To enforce standardization and co-ordination amongst various railway systems, the Indian Railway Conference Association (IRCA) was set up in 1903, followed by the Central Standards Office (CSO) in 1930, for preparation of designs, standards and specifications. However, till independence, most of the designs and manufacture of railway equipment were entrusted to foreign consultants. With Independence and the resultant phenomenal increase in country's industrial and economic activity, which increased the demand of rail transportation - a new organisation called Railway Testing and Research Centre (RTRC) was setup in 1952 at Lucknow, for testing and conducting applied research for development of railway rolling stock, permanent way etc. [Ref.10]

Central Standards Office (CSO) and the Railway Testing and Research Centre (RTRC) were integrated into a single unit named Research Designs and Standards Organisation (RDSO) in 1957, under Ministry of Railways. [Ref.10]

3.1 Responsibilities

3.1.1 Research Design and standards Organisation

RDSO is the technology centre of Indian Railways and has to perform the role of R&D. It has the following functions as per [Ref.10]:

- Development of new and improved designs.
- To concentrate on this core function, RDSO confines themselves to approval of new types of rolling stock, new technologies and new systems for use in Indian Railways.
- Further RDSO plays the key role in development, adoption and absorption of selected new products including prototype approval, as directed and monitored by Railway Board.
- Technical investigation, statutory clearances, testing and providing consultancy services.
- Development of standards for materials and products specially needed by Indian Railways.
- Inspection of critical and safety items of rolling stock, locomotives, signalling & telecommunication equipment and track components.

- In order that RDSO's role is focused on product / process research and in areas of new technologies and new materials, their involvement in vendor development/inspection is restricted to important items of wagons only.

3.1.1.1 The Signal Directorate

The Signal directorate has the following functions as per [Ref.10]:

- Design, development & Standardisation of Signalling & Safety equipments;
- Adaptation & absorption of emerging software embedded technologies;
- Investigation, analysis & remedial measures of specific field problems referred by Zonal Railways / Railways Board;
- Improving reliability of signalling equipments;
- Providing technical assistance/guidance to Zonal Railways;
- Vendor development;
- Testing of signalling items for vendor development & investigation;
- Issue, review & revision of specifications, Test formats & STRs;
- Issue of Pre-Commissioning Check Lists for vital signalling equipments.

The procedure can be initiated by the client, i.e. the zonal railways for the procurement of new technology or modification of existing technology, which is governed by the relevant cross acceptance policies of RDSO, or by RDSO itself. In the later case, RDSO issues an Expression of Interest (EOI), which vendors can reply to.

3.2 Expression of Interest

The RDSO floats EOIs for the following as per [Ref.10]:

- Development of specification of new products either to replace product with new technology, better manufacturing process or additional item in equipment or rolling stock;
- Developing more vendors for an item;
- Selection of panel for consultancy;
- Equipments/items which have RDSO specifications but vendor approval is not done by RDSO are procured by railways on their own. Inclusion of such items as identified by Railway Board in RDSO approved list shall be done by inviting EOI for vendor registration in which existing firms can also participate;
- Any other need with specific approval from competent authority.

3.3 Request for Proposal

In the Indian Railways, the process for any kind of work is initiated by the relevant zonal railway board with the issuing of a Request for Proposal (RFP). The RFP is a contract which outlines the objective of the work, the methodology to be followed, the required competencies and resource pool. It is a single document comprising of both the technical, financial and legal aspects of the project.

The RFP binds the contractor to present within a stipulated timeframe what they have understood about the objectives of the project, a detailed methodology to be used, the personnel involved and a safety assessment plan.

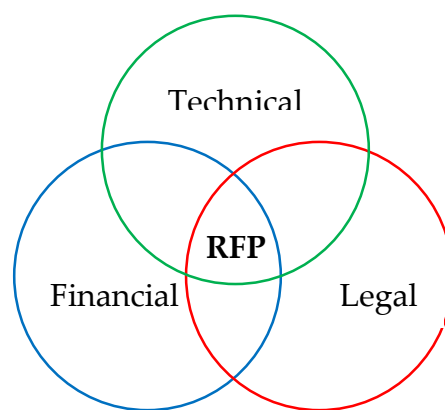


Figure 5: Constituents of the RFP

The description of approach, methodology, and work plan for performing the assignment is comprised of the following sections, which is a part of the Technical Proposal, which the company must present to the client.

- **Technical Approach, Methodology and Organisation of the Consultant's team**
The consultant must explain their understanding of the objectives of the assignment as outlined in the Terms of Reference (TOR), the technical approach, and the methodology they would adopt for implementing the tasks to deliver the expected output(s); the degree of detail of such output(s); and describe the structure and composition of their team.
- **Work plan and Staffing**
The consultant must outline the plan for the implementation of the main activities/tasks of the assignment, their content and duration, phasing and interrelations, milestones (including interim approvals by the Client), and tentative delivery dates of the reports. The proposed work plan should be consistent with the technical approach and methodology, showing understanding of the TOR and ability to translate them into a feasible working plan and work

schedule showing the assigned tasks for each expert. A list of the final documents (including reports) to be delivered as final output(s) should be included here. The work plan should be consistent with the Work Schedule Form.

- **Safety Assessment Plan**

A detailed Safety Assessment Plan on services indicated in the scope of work.

- **Comments** for further clarification, requirements or modifications

3.3.1 Terms of Reference

The Terms of Reference (TOR) outlines the scope and limitations of the assignment. All relevant technical information regarding the assignment are outlined in this section of the RFP.

The TOR gives a brief introduction and background of the project. It puts forward the overall entailment, the geographic area of the project, details of the contract packages, technical information regarding the junctions, stations, crossings and such. The TOR also outlines the overview and scope of the assignment under the particular project. It also lists the relevant standards and specifications to be followed.

The TOR goes into detail regarding the procedure for the procurement of items/equipment, objectives of the ISA services, the scope of such services, procedure for the safety assessment, document reviews, audits, and structure of the reports to be submitted, list of deliverables, testing, installation and commissioning guidelines.

The TOR includes:

- Background information about the project
- The systems works contract for the project, which the ISA must assess
- The systems overview, specifically for which the ISA service is desired
- Scope of works
- List of applicable standards
- Procedure for procurement of items/equipment
- Scope of ISA services
- Safety assessment procedure
- Document review guidelines
- Safety audit procedures
- The program of the work
- Regulations regarding interim ISA reports
- Observation Management and Tracking log
- Structure of reports
- List of deliverables, which includes:
 - Safety assessment plan

- Assessment of contractors plans
- Design assessment
- Manufacturing and installation audit and assessment
- Testing and commissioning audit and assessment
- Engineering safety validation case
- Operation and maintenance process assessment
- Trial running and test assessment
- Procedures regarding safety assessment of Generic Products used in Signalling system
- Quarterly progress reports' guidelines
- Final safety assessment
 - For the generic product
- Guidelines regarding the team composition and Qualification/Experience requirements.

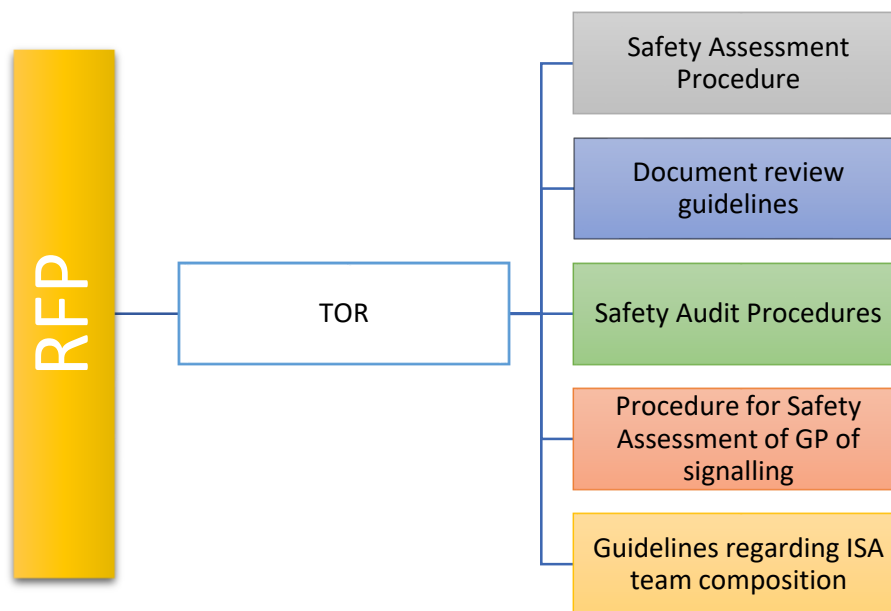


Figure 6: Constituents of the TOR

3.3.1.1 Safety Assessment of signalling system

The ISA shall carry out Independent Safety Assessments and Independent Safety Audits covering all Safety critical (SIL 3 and 4) and Safety related (SIL 1 & 2) systems as required and functions for the Signalling System.

The ISA Safety activities shall closely follow every stage of the Project development process i.e. detailed Hardware and Software design, V&V, Installation and Testing stages, Trial runs etc.

The Independent Safety assessment shall be carried out in accordance with the principles and processes described in the CENELEC railway application standards EN 50126 [Ref.1][Ref.2] (or IEC 62278), EN50128 [Ref.17] (or IEC 62279) and EN50129 [Ref.18] (or IEC 62425) as well as the relevant CENELEC guides for the implementation of these standards.

The Independent Safety Assessment shall broadly cover the following, but not limited to:

- Review and assess the adequacy and robustness of the Signalling safety management organization of the Contractor and safety management processes undertaken by the Contractor during requirements specification, design, manufacturing/installation, testing and commissioning and system handover phases;
- Review and assess the adequacy of the safety requirements for the design, manufacturing, installation, testing and commissioning of the Signalling system and determine that these requirements have been met;
- Verify that the planned Signalling activities are being or have been carried out and in the manner and to the standards prescribed in the Contractor's Safety Plan, System Assurance Plan and RAM Plan;
- Verify that adequate competent staff are deployed by the Contractor for the Signalling works;
- Assess the adequacy and robustness of hazard identification, ranking, resolution, recording, monitoring and close out processes and to verify that risk has been reduced to As Low As Reasonably Practicable (ALARP) and in accordance with the Safety Requirements for each system;
- Evaluate the effectiveness of the Signalling safety management activities undertaken by the Contractor during design, verification & validation, installation, testing, commissioning and test running phases of the Project for each safety critical and safety related system;
- Evaluate the adequacy and effectiveness of the processes and methodologies for managing and ensuring compliance with relevant safety codes, standards, regulations and specifications;
- Evaluate the adequacy of test plans, test scenarios, test passing criteria, processes, follow up of test reports and competency management of test engineers, the migration plan, the contingency plan and similar documentation;

- Review the Contractor's processes for determining the readiness of the Signalling System for test running and revenue service;
- Evaluate the process of handling design changes (both software and hardware) and configuration management;
- Evaluate the processes for managing key safety interfaces, including Electro-Magnetic Compatibility (EMC), EMI management;
- Assess on the compliance of Signalling and Communication systems with EN50126 [Ref.1][Ref.2] (or IEC 62278; EN 50128 [Ref.17] (or IEC 62279) and EN50129 [Ref.18] (or IEC 62425) ;
- Conclude on the achievement of SIL classifications for all Safety related and Safety critical sub-system; and the capability of the Signalling System to operate and maintain to an adequate level of safety.

The ISA may adapt the level of detail of the Safety Assessment according to the following factors:

- Sub-system Safety Integrity Level (SIL); and
- Existing Safety demonstrations for the related system/sub-systems.

Methodology

The Safety Assessment shall be broadly based upon two types of activities:

- a) Review of the Contractors' documentation pertaining to quality/safety aspects throughout the various stages of development of the Signalling System and;
- b) Inspections and Safety Audits within the Contractors entities and on site.

Safety assessment will combine the use of design analysis, results from safety audits and practical assessment. Each assessment will include a review of the processes and organization employed at respective stage. It is expected that the results of safety audits conducted independent of the safety assessments shall be used as the basis of assessment for each respective phase.

The assessment will pay particular attention to the project Hazard Log as this contains the traceability from the safety requirements to documentation supporting Engineering activities for the project.

3.3.1.2 Document Review guidelines

- ISA shall independently review all relevant documents for compliance with the selected standards, consistency with the respective specifications as well as for adequacy of the determined Safety Integrity Level according to EN50126 [Ref.1][Ref.2](or IEC 62278), EN 50128 [Ref.17] (or IEC 62279), and EN 50129 [Ref.18] (or IEC 62425) standards;

- The ISA may carry out technical assessment of the documents, including all relevant design documents and plans, design calculations, installation documents, test plans and test procedures, software/hardware documentation, meeting minutes, the Contractor's Internal Audit reports and Internal Safety Assessment reports, RAMS analysis documentation, Reliability growth report, testing and commissioning records, change records for both hardware and software, Safety cases & Trial run;
- The ISA shall pay special attention to the applicability and appropriateness of the available pre-certificates and reports, fulfilment of safety-related application conditions, impact and requirements on the operational concept, including the safety-related systems interfacing with the Signalling System;
- The ISA shall collect, inspect and analyse all necessary data required to assess whether the Contractor has throughout the project duration, applied appropriate processes and Safety solutions in accordance with the requirements of the applicable Safety standards in the Contract between the Employer and the Contractor, as well as the applicable local and national laws/acts;
- Where some of the documents are not being made available, the relevance of the same and the need for the same shall be justified by ISA for the Engineer/Employer to intervene and provide the same from the contractor;
- The ISA shall also assess the documentation of systems interfacing with the Signalling System as well as documentation related to Operation and Maintenance;
- The ISA documentation review shall include audit and assessment of the Contractors' reports on EMC/EMI analysis and test data.

The detailed procedure for individual works are mentioned in the RFP inside the TOR. However, the TOR explicitly mentions the process according to the body it is issued for. Thus it is difficult to understand the general procedure for obtaining the authorisation of railway products to place in service in the Indian railways. In the context of this study, a brief overview of the Indian process is mentioned in Section 4.2.

4 Differences in procedure for placing a product in service

For the purpose of comparing the different processes used by the two railways, a product is chosen which has already been placed in service in Italy recently, and is being placed in service in India. By comparing the same product, which is verified by the same ISA in the two countries, the majority of the discrepancies are thereby eliminated and the complete focus falls in the procedure.



Figure 7: SML 400 [Ref.11]

The product so chosen is an electronic interlocking system SMARTLOCK 400, manufactured by ALSTOM. This is a hugely popular product having been put in active service in numerous countries all over the world.

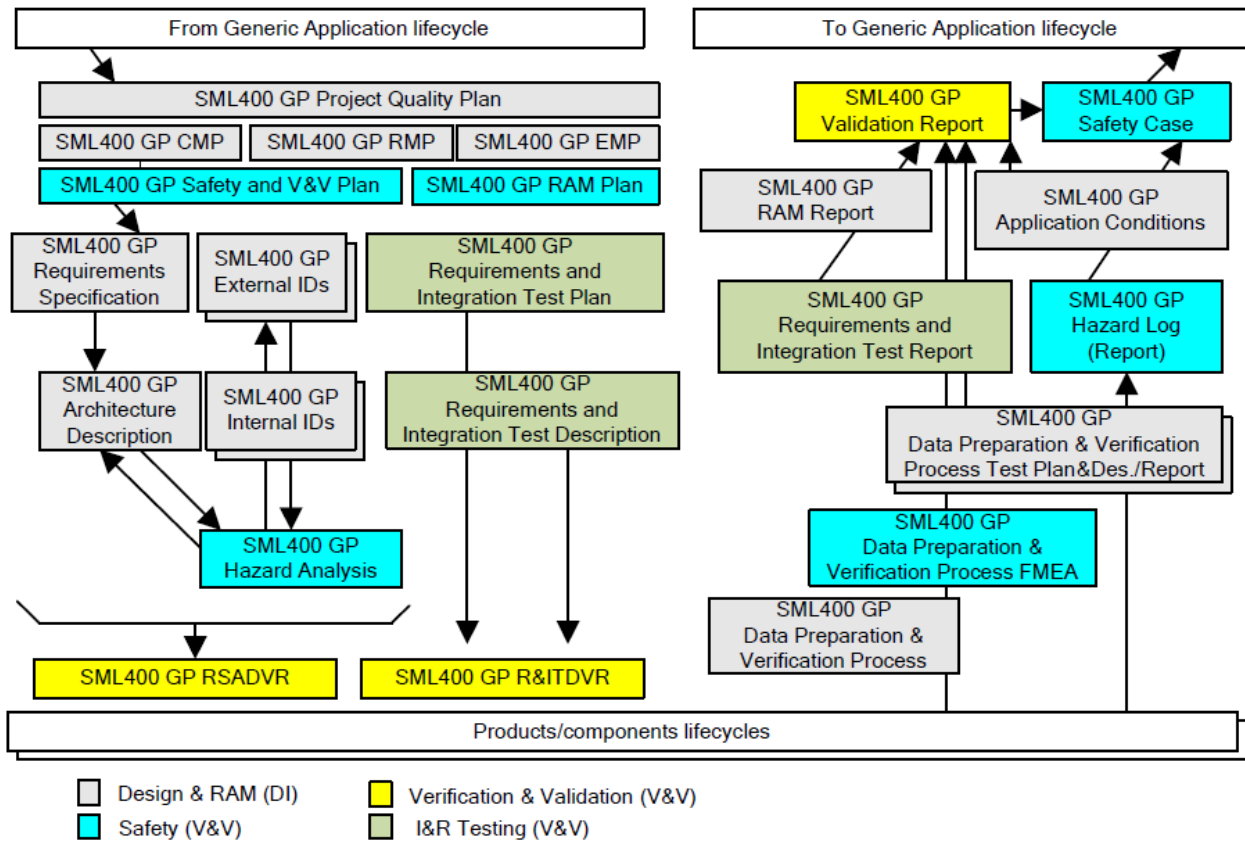


Figure 8: SML400GP Design, Safety and V&V Life Cycle (Source: SML400 GPSC)

4.1 The Italian process for obtaining APIS for SML400

The process for obtaining an APIS in Italy for an electronic interlocking system is defined in the Guidelines [Ref.3] document issued by the agency, ANSF.

For this section, an ongoing Italian project has been chosen. The project “Technological enhancement of the Rome node”, due to the extent and importance of the area under investigation, the heterogeneity of the activities and of the involved systems make the project characterised by a high degree of complexity, and thus is divided into several functional modules:

- Functional Module A: Rome Tiburtina - Orte
- Functional Module B: Ciampino - Colleferro
- Functional Module C: Rome Casilina - Campoleone - Priverno and Campoleone - Nettuno
- Functional Module D: Monte Mario - Rome Tiburtina

For this study, the module A of the project is considered. The phase 1 of this project is limited to the lines Rome Tiburtina – Settebagni and Settebagni – Fara Sabina. The route

Rome Tiburtina - Settebagni (part of the Rome – Florence line) is part of the Scandinavian Mediterranean corridor (passengers and freight) and provides for the implementation of the ERTMS system by 2020. The section Settebagni - Fara Sabina also falls on this corridor.

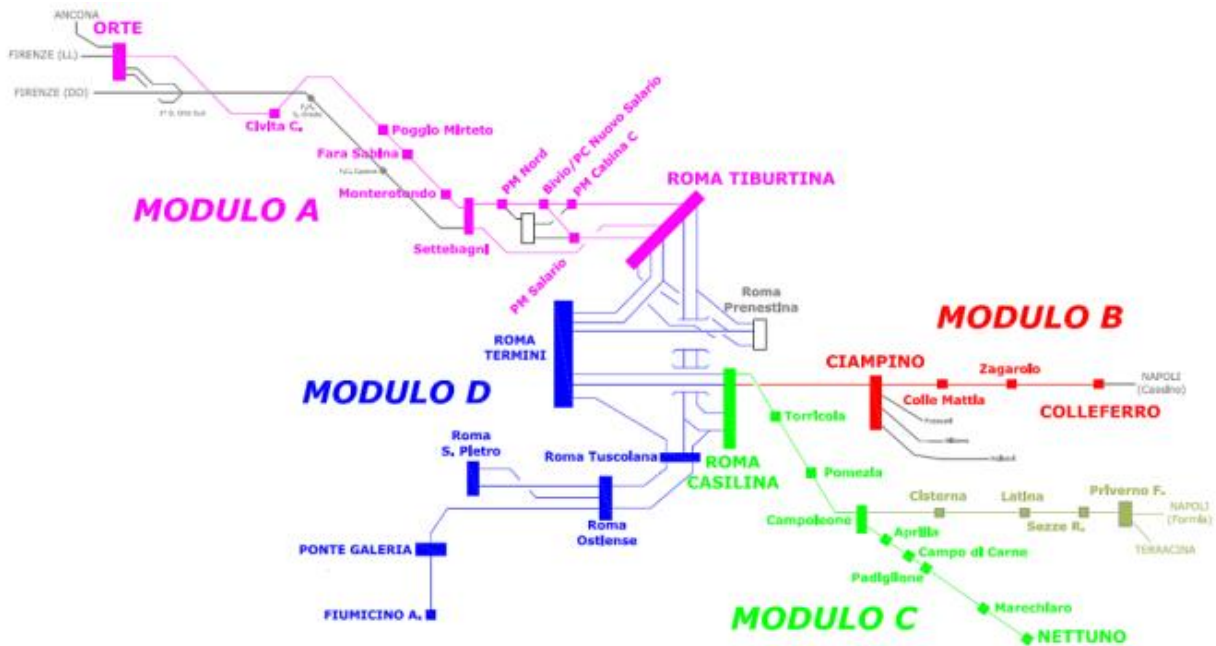


Figure 9: Functional modules of the work

As regards civil works, the main interventions envisaged are:

- creation of new technological buildings of various dimensional types, distributed at the sites
- intervention along each of the three legs;
- refurbishment of existing technological buildings, or internal spaces, in order to allow the provision of dimensionally and technologically adequate spaces to the installation of the equipment;
- construction of 3 new pedestrian railway underpasses and related works, i.e. temporary works, shelters, etc.;
- civil works aimed at modifying railway platforms on some of the intervention sites in correlation to military works.

The IF, RFI, proposed placing the Alstom product SML400 in this line.

4.1.1 The subjects

For this project the Agency is ANSF, the applicant of the APIS is RFI, and the NoBo is Italcertifer.

4.1.2 Process flow

The process begins with the applicant sending a **Preliminary Dossier** to ANSF for its opinion if authorization is necessary for placing the IXL product on the line.

After getting opinion, the applicant files a **Technical Dossier** of National Verification and the NoBo analyses it.

The NoBo issues a **Normative Report** based on the Technical Dossier.

Along with the Preliminary Dossier, the applicant files the Normative Report to ANSF.

ANSF issues a **No Objection Certificate** to the applicant, which is basically a go-ahead to carry on the process for obtaining APIS.

The NoBo commences the process of certification based on **Decree 191/2010 [Ref.5]**. It issues an assessment **report** and a **certificate** to the applicant.

The report is prepared based on **EU regulation 57/2008 [Ref.14]**, Risk Analysis report, and Application conditions report.

The applicant compiles the certificate, the report from the NoBo, the risk Analysis report, Application condition report and files for a declaration, requesting an APIS.

The agency verifies the declaration and AMIS is awarded.

4.2 The Indian process for obtaining APIS for SML400

Ministry of Railways (MOR), Government of India has planned to construct Dedicated High Axle Load Freight Corridor covering about 3363 Kms on two corridors, Eastern Corridor from Ludhiana (Sahnewal) to Dankuni and Western Corridor from Jawaharlal Nehru Port, Mumbai to Tughlakabad/ Dadri near Delhi along with inter-linking of the two corridors at Dadri.

The DFC Project entails construction of mostly double line railway tracks except single line between Khurja – Sahnewal (near Ludhiana). Up-gradation of transportation technology, increase in productivity and reduction in unit transportation costs have been taken as guiding principles for formulating the DFC project. Various operating systems, motive power, Electric Traction, signalling and work processes are required to conform to this broad perspective.

This section discusses the eastern DFC, where the product SML400 is being proposed for installation.

4.2.1 Signalling System Overview

The entire stretch from New Bhaupur to New Khurja will be provided with Automatic Signalling system. Automatic Signalling shall be provided in the block sections and main lines of the stations. Trains will run observing automatic/ semi-automatic signals en route, which in normal conditions will be set for a through and uninterrupted run. The Automatic Signalling will be provided using 4 aspect line side Multi-aspect Colour Light Signals at a nominal spacing of 2 Kms. All the Signals will be provided with LED signal lighting units.

4.2.1.1 Scope of ISA services

The scope of the work of an ISA is defined in the TOR. It broadly includes the following:

- Independent assessment of Safety of Signalling System, being provided under Systems works contract.
- Independent Safety assessment of Generic product- Cross Acceptance/Approval for Railway Signalling as per “Procedure Order for Cross Acceptance/Approval of Software Embedded Electronics Systems and New/imported Technology Products for Railway Signalling”, provided in the contract.
- The scope of ISA services shall be limited to Signalling system and Signalling product provided under the Systems Works Contract Package.
- The assessment shall include Safety assessment of Point machine, Ground connections including Clamp Lock for used with thick web canted turnouts.
- The scope of services shall be limited only to the Signalling Safety aspects.
- The ISA services shall be limited to the Safety aspects of design, manufacturing installation, T&C and inputs to O&M. The ISA shall assess both hardware and Application Software (Data) components of the Signalling system.
- The ISA Safety activities shall include the mitigation of risks associated with hazards resulting from sharing of interface systems with Rolling Stock, Track, Traction, Power Supply, and Civil Works etc.
- The ISA shall assess the Signalling System and conclude that the adequate level of safety is achieved by the Signalling system, including interfaces with other systems to ensure safe operation of the trains. The ISA shall do the Safety assessment of the Generic Product – Electronic Interlocking and recommend to the Employer for its Project specific Cross Acceptance/Approval.

4.2.2 The subjects

For this project the supplier is ASPIL, the ISA is Italcertifer and the authority for granting the APIS is RDSO.

4.2.3 Process flow

The flowchart of the procedure to obtain the APIS has been illustrated below.

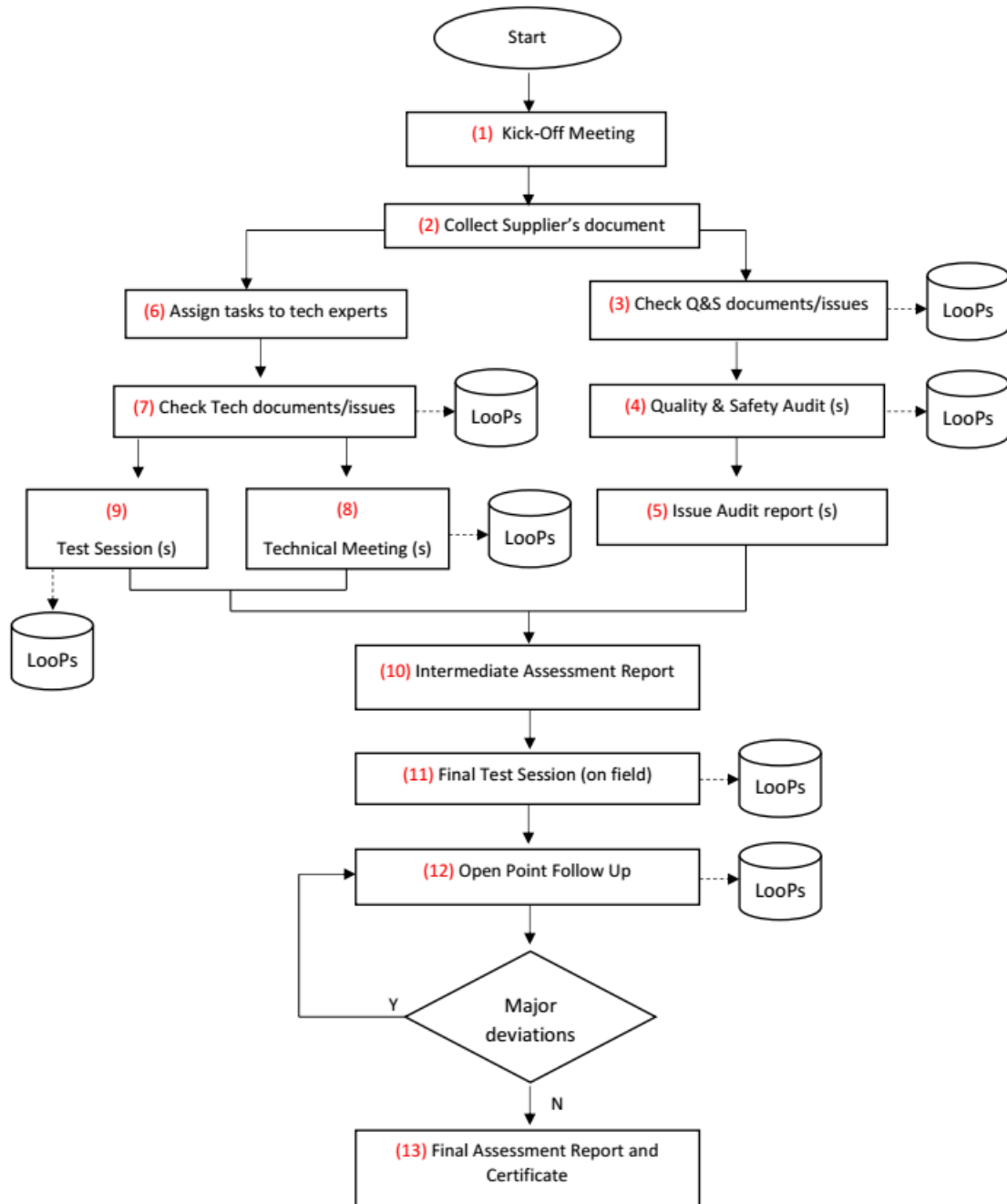


Figure 10: Overview of process to obtain APIS for SML400GP

The supplier provided these primary documents to the ISA; the Safety Case, RAMS plan and the Safety plan.

ITCF analyses these document and issues technical notes.

As the LooPs are closed, the First Assessment Report is issued by ITCF, as per the requirements of the RFP.

The supplier also forwards its Safety Assessment plan to ITCF as per the requirements of the RFP.

Consecutively, the processes for cross acceptance are carried out. The test plans provided by the supplier are evaluated and the ISA recommends the supplier to carry out the field trials.

The preliminary field trial plan is evaluated. After closing of all the LooPs, the final test plan is prepared. The ISA provides intermediate reports to the agency regularly. The final assessment report is prepared by the ISA along with the conformity of cross acceptance.

The supplier, will all the relevant reports and certificates apply for the APIS.

APIS is awarded after verification by the agency.

4.3 Disparities

The procedure for acquiring the authorisation, as apparent from the previous sections, are diverse. The Italian system has evolved over a long time according to a larger European framework. With a vast expertise, the system in Italy and Europe in general seems to be more optimised at this point.

The first apparent difference is in the process definition. The Italian railways have a better-structured set of general guidelines, while the process for the Indian Railways are outlined in contracts, relevant to the type of work. Although the RFP is similar to the European guidelines, they seems to be technologically dependent. It might create difficulty if newer technologies are needed to be authorised. Even though the ENs are more flexible, the sheer number of European and national norms can create confusions. This is better handled by the Indian system with just one document outlining everything.

The process flow in the Italian system appears to be simpler in comparison with the Indian one. After every step along the process, there is a clear understanding of the achievements until that point. In the Indian process, although similar goals are achieved along the process, the relevance of those achievement with the previous or subsequent steps are sometimes not so clear.

The broad comparison shows big differences, but upon closer investigation the philosophy appears to be similar, with a different approach. The TOR basically describes the same processes as in Italy. Disparities emerge on the testing of the products, both type tests and field trials. The RDSO requirement for type testing includes different specifications, which defines hardware testing guidelines, functionality tests and the way

of performing test all together. This might result in confusion as to which of these specifications would enjoy preference, as they sometimes state incompatible specifications to one another. This creates a critical situation in terms of safety, as products designed in Europe, keeping the local environmental and climatic conditions in mind, might not be suitable for optimal utilisation in India without a well-defined rigorous test suite.

Since this area has been identified as a major difference, this study will focus on the testing regimes from this point onwards.

4.3.1 Type tests

Type tests are a specific set of tests or scenario designed to verify product compliancy to environmental requirements (climatic conditions, mechanical dependability, electrical, EMC and safety aspects.

The requirements that are tested as per RDSO specifications [Ref.6] are mentioned in Appendix B.

Type of test	Reference standard
Change of temperature	EN 60068-2-14
Dry heat test	EN 60068-2-2
Damp heat test (1 st cycle)	EN 60068-2-30
Cold test (-40°C)	EN 60068-2-1
Cold test (-25°C)	EN 60068-2-1
Damp heat test (2 nd cycle)	EN 60068-2-30
Low temperature storage test	EN 60068-2-1

Table 2: Climatic TT reference standards for Europe [Ref.8]

The TT list as per the European specifications are listed in Appendix C.

4.3.1.1 Mandatory type tests for cross approval

The following tests shall constitute type tests, as per [Ref.7]:

- i. Visual inspection tests
- ii. Insulation resistance tests
- iii. Card level functional and fail safety tests
- iv. System level functional and fail safety tests
- v. Computerized testing
- vi. EMI/EMC tests
- vii. Environmental / Climatic Tests

- viii. System Diagnostic Tests
- ix. System Software Test
- x. Any other test deemed necessary by RDSO

The type tests were performed as per the European specifications by the supplier as those specification offers a larger range. However, some of the requirements were specifically included keeping in mind the local ambience in India.

		Reference Standards		Severity Level	Report Result	RDSO requirement	
		Reference	Test		Passed ?	§	Severity level
Climatic	Temperature variations	EN50125-3	EN 60068-2-14	+5°C/+45°C 3 hours at each T°, 2 cycles	Yes	9.3.1	-10°C/+70°C 7 hours at each T°, 3 cycles
	Dry heat	EN50125-3	EN 60068-2-2	+45°C for 16hours	Yes	9.3.2	+70°C for 16 hours
	Cold	EN50125-3	EN 60068-2-1	+0°C	Yes	9.3.3	-10°C
	Cyclic damp heat	EN50125-3	EN 60068-2-30	+45°C @ RH=85%	Yes	9.3.4	+40°C @ RH=95%
	Steady state damp heat	EN50125-3	EN60068-2-78	+45°C @ RH=95%	Yes	9.3.5	+40°C @ RH=93%
	Salt mist test	EN50125-3	EN 60068-2-52	Not required	-	9.3.6	2hrs + 22hrs @ 35°C, RH=93%
	Dust test	EN50125-3	EN 60529	≥IP21	Yes	9.3.7	1hr inside dust chamber
Mechanical	Shock	EN50125-3	EN 60068-2-27	2g/11ms	Yes	9.3.10	1000 bumps@400m/s²
	Vibration test	EN50125-3	EN 60068-2-64	5-2000Hz 2,3m/s²	Yes	9.3.12	5-150Hz 15m/s²
ESS (Environmental Stress Screening test)	Thermal cycling	IEC 61163	IEC 60300-3-7	-20°C/+70°C, 10°C/min, 28 cycles, Dwell time 15min	Yes	9.3.13	0°C/70°C, 10°C/min, 9 cycles, Dwell time 30min

Table 3: Differences in the test specifications according to the different standards

The ISA did not approve the execution of two of the climatic tests, as the Indian specifications cater to the climatic condition of the Indian climate. Thus, the following two tests were repeated with the RDSO requirements [Ref.6].

		RDSO requirement		XT° platform Type test result	
		§	Severity level	Severity level applied	Passed?
Climatic	Temperature variations	9.3.1	-10°C/+70°C 7 hours at each T°, 3 cycles	-10°C/+70°C 7 hours at each T°, 3 cycles	Yes
	Dry heat	9.3.2	+70°C for 16 hours	+70°C for 16 hours	Yes
	Cold	9.3.3	-10°C for 2 hours	-10°C for 2 hours	Yes

Table 4: Repeated TT with RDSO specifications

4.3.2 Field trials

Field trials provide the opportunity to test the safety and functionality aspects of the product. Some of the functional characteristics depend on the specific location and mode

of use of the product and hence only lab testing is not adequate to fully ascertain the safe and optimal functioning.

In Italy, to test the functionalities, two types of tests are conducted:

- Simulations, in the laboratory
- Field trials

For both of these operations, a standard and well defined “test suite” which are a sequence of mandatory tests to be performed in the lab and on site to ascertain the functionality and safety of the whole system boundary conditions. These approximate the realistic site conditions satisfactorily.

In India, there appears to be an absence of realistic field tests as of now. This creates situations where manufacturers could potentially commission their products without proper field tests (i.e. after the execution of the test session there is no confidence that all the aspects to be verified were covered in terms of functionality, safety and management of the system in case of temporary failures of one or more subsystems)

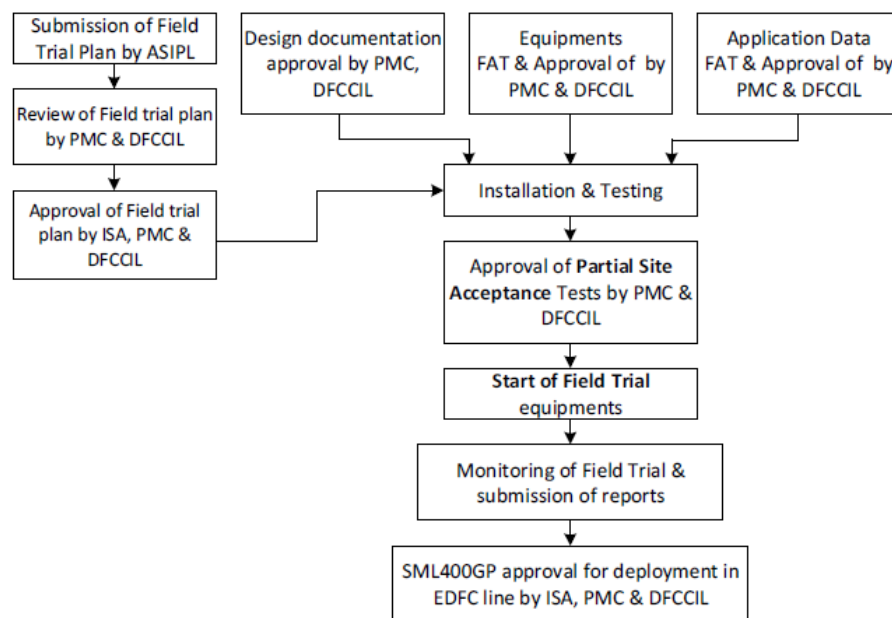


Figure 11: Sequence of activities for field trial and approval of SML400GP Electronic Interlocking system

In the context of the present case study, the contract outlined provision for field trials. However, the manufacturer had countered that since the product is already commissioned in so many places worldwide, it is tried and tested in service and no further testing in India is necessary. In addition according to the manufacturer Deviations from the European standards were also taken in account during the type testing phase. Hence the field trials are unnecessary.

This begs to answer the question, “**Why are field trials necessary?**” or more precisely, “**What are the risks of not performing Field trials?**” The following sections are dedicated to attempt to answer this.

4.3.2.1 What are the risks of not performing Field trials?

In the lab everything is micromanaged. The whole ecosystem is simulated and approximated. The function of an interlocking machine depends overwhelmingly on the station architecture. These functionalities are tested using a model of the station as it is unlikely that the lab has the full array of equipment found in a complex station such as point machines, axle counters, on-line power modules or signals, which are crucial to ascertain proper integration. These might not fully represent realistic conditions on the field. Moreover, in the lab environment, mostly the logic algorithms and communication protocols are tested.

To identify that such tests are indeed enough to conform to the safety requirements, a Hazard analysis approach described in the CENELEC Standards [Ref.1][Ref.2][Ref.4] [Ref.16] for safety related signalling equipment is used in this study.

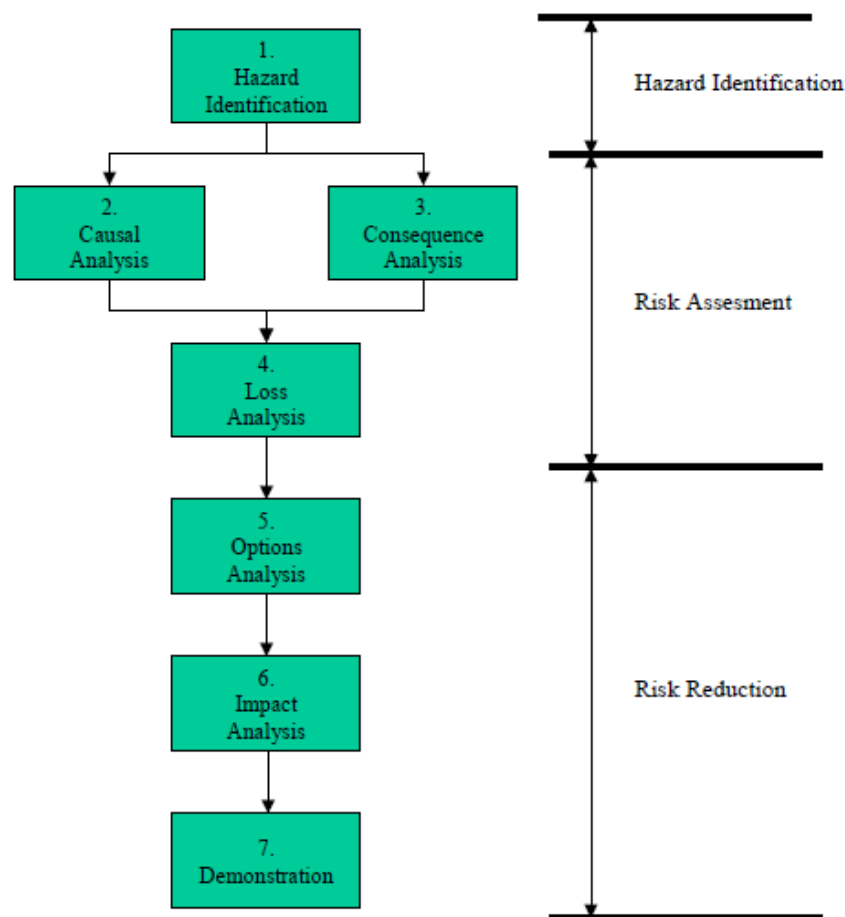


Figure 12: The seven stages of the HA process [Ref.16]

The methodology recommended by the CENELEC is based on a top-down approach to Hazard Analysis. As per the regulations, a Preliminary Hazard Analysis must be performed after the concept phase of the system life-cycle. It is a high-level HA specifically for the standalone product. After the subsequent mitigation (by means of modifying technical parameters, designs, introducing application conditions etc.) the system enters the prototyping phase. As the products constituting the full interlocking system are well defined at this stage and regarded as “Safe”, another deeper Hazard Analysis must be performed to ascertain that all the possible hazards, including the new ones emerging from the realization of the product (which are updated in the Hazard log already provided by the PHA) are identified and mitigated. This step coincides with the integration of the subsystem at hand with the whole signalling and interlocking system. The mitigation can be achieved either by finding a technological mitigation or with the introduction of an operator procedure (i.e. procedural application conditions). The process is illustrated in a labelled diagram in Figure 16.

4.4 Hazard Analysis

Before discussing in the methodology of performing the HA, a preliminary understanding of the modules which make up the interlocking ecosystem is necessary. The SMARTLOCK 400 electronic interlocking device is comprised of many sub-systems. But for simplicity, only the relevant subsystems are considered. These include the logic core, the object controllers and the Human Machine Interface. This device is connected with other subsystems like the Axle counters, Point Machines and Signals. These constitute a basic interlocking ecosystem. It is taken for granted that the system is SIL4 compliant, as it is used for Railway applications [Ref.1][Ref.2]. Figure 17 illustrates the schematic diagram of this simple ecosystem.

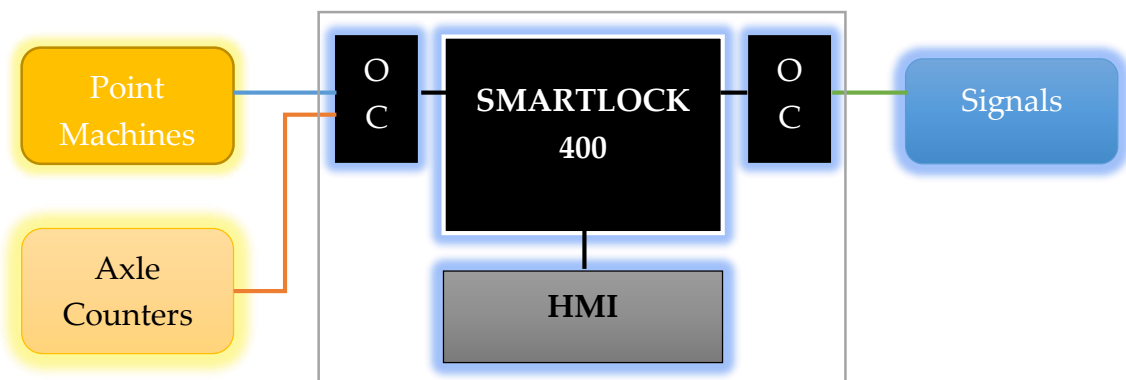


Figure 13: A basic interlocking system

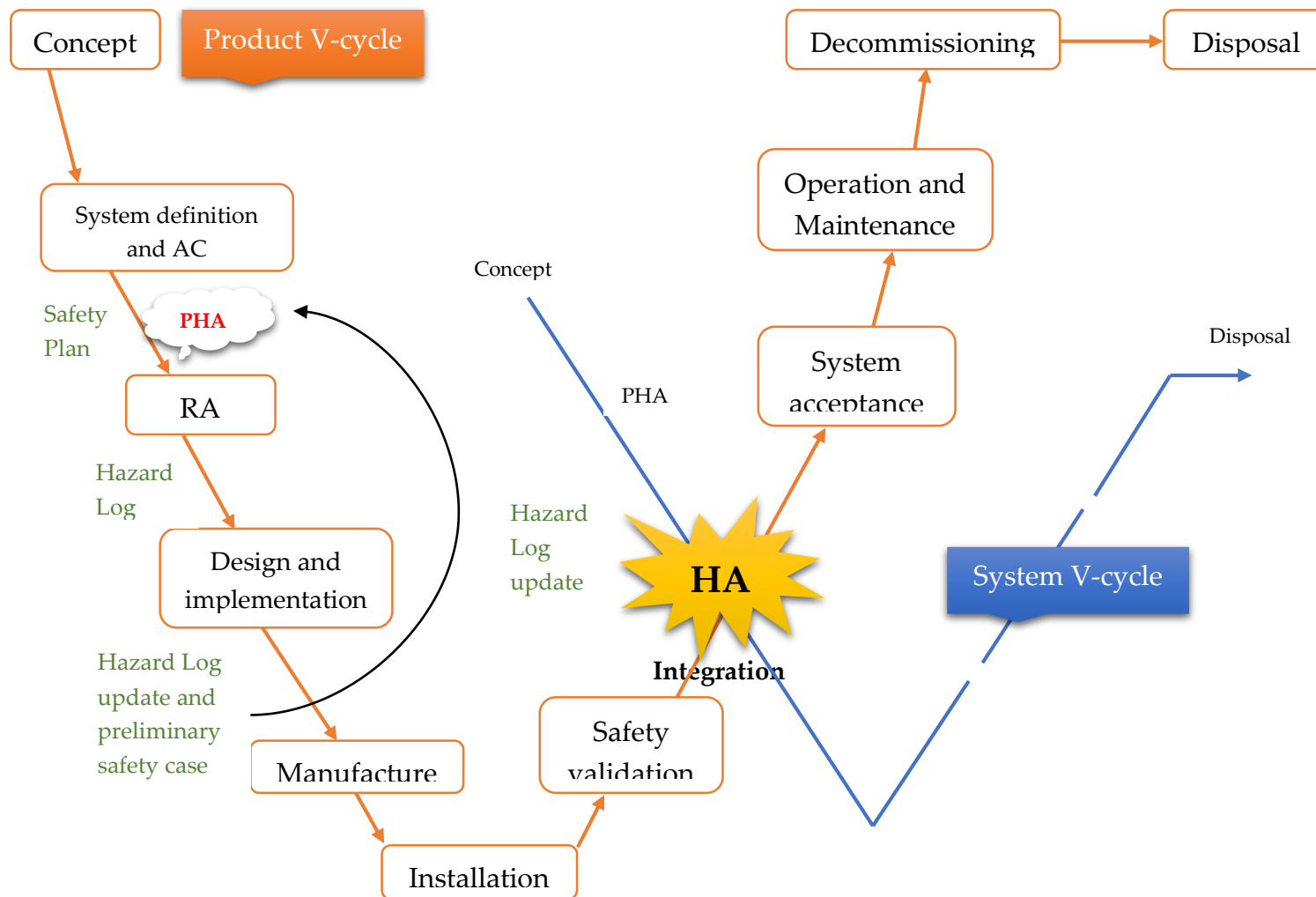


Figure 14: Hazard management at integration of product life-cycle and system life-cycle

For the scope of this study, a scenario is considered where individual SIL4 compliant machines are working together in an interlocking ecosystem. Multiple SIL4 compliant sub-systems cannot necessarily create a SIL4 compliant system. The functioning of these sub-systems, as intended, depends on the safe transmission of communication between them. Thus the interface between these sub-systems are critical for ensuring the safety and reliability of the whole system.

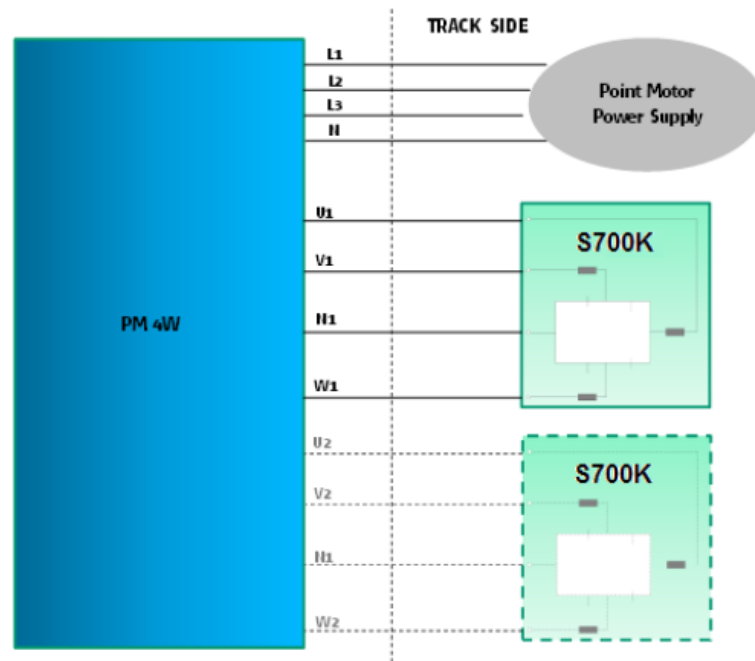


Figure 15: Detailed representation of the interface between the point module (PM4W) with point machine (s700K)
(Source: GPSC)

To demonstrate the argument, an interface hazard analysis is conducted. The purpose of this analysis is the demonstration of the functional and safety compatibility between the PM4W Point Module of SML400GP and the Siemens S700K Point Machines 5.5kN and 7kN, designed to be installed in the application.

The indication 5.5kN and 7kN is referred to the throwing force, i.e. the force necessary to move the switch rail of turnout.

The analysis takes into account both functional than safety aspects, according to

- Object Controller Application Condition [OCGP_AC],
- S700K Siemens Point Machine Operating Manual [S700K_OM],
- Siemens Point Machine Technical Data [S700K_SPEC] and
- Technical Description of Electromechanical point machine [S700K_DT].

As an example of IHA, only one hazard inducing instances (open points) are demonstrated in this chapter. Whenever Interface Compliance cannot be covered by analysis, test descriptions are provided that shall be executed in order to verify the interface compliance.

For these reason, this IHA generates two kind of output:

- Functional and Safety Test descriptions
- Application conditions

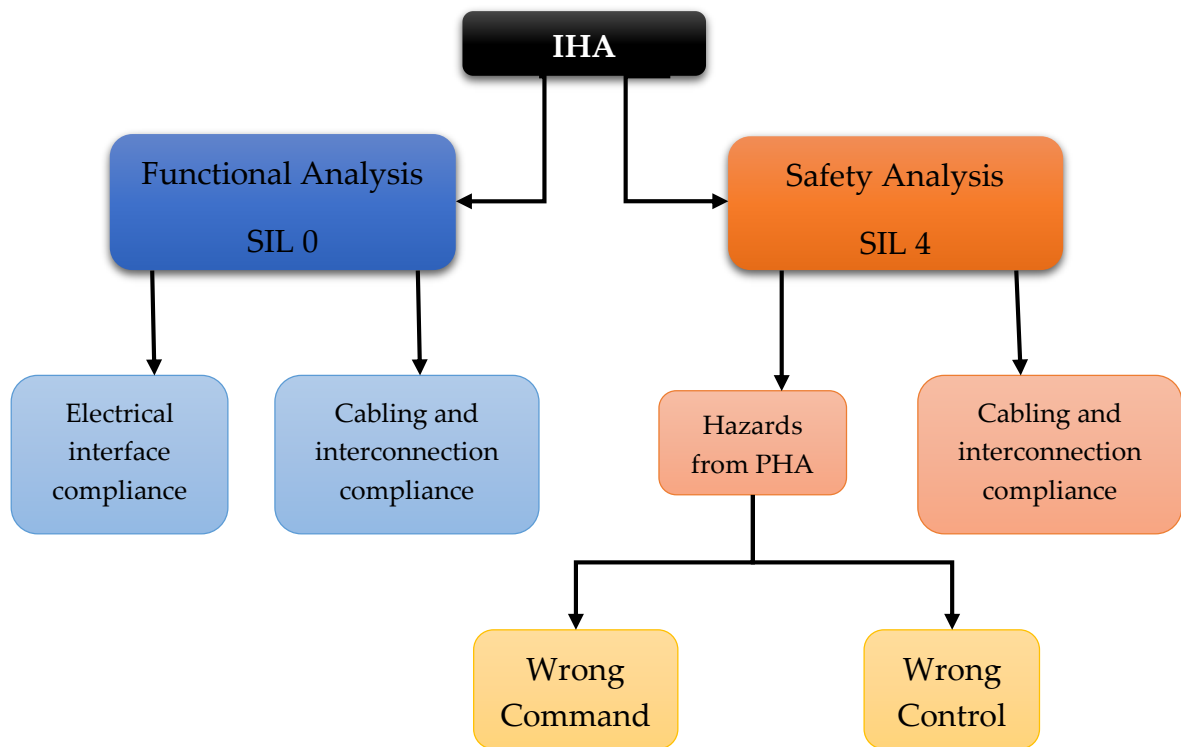


Figure 16: IHA methodology flow diagram

The Interface Hazard Analysis takes into account both functional and safety aspects.

The **functional analysis** is based on the compliance verification of the application conditions classified as SIL0, with particular focus on electrical interface compliance and cabling and interconnection compliance containing functional aspects.

The **safety analysis** is based on the compliance verification of the application conditions, classified as SIL4, with particular focus on hazardous conditions, according to the PHA and HA of the Point Module (PM4W) and cabling and interconnection compliance containing safety aspects.

The two hazardous conditions considered are:

- WRONG COMMAND TO POINT MACHINE.
- WRONG CONTROL OF POINT MACHINE.

Whenever one or more of these information is missing, an open point is raised and a measure is requested through test. This measure is compared with an expected result to verify its compliance. In case of compliance, the open point previously raised is closed because the correct interfacing is satisfied.

The following table lists the Siemens S700K point machine electrical parameters.

ID	Description
S700K_ELECTRIC_PARAM.1	S700K rated voltage shall be 3 x 400/230 V AC, 50Hz \pm 2%; 110 to 136 V DC SIL 0
S700K_ELECTRIC_PARAM.2	Throwing Time: 6 s SIL 0
S700K_ELECTRIC_PARAM.3	Rated Current: 2A SIL 0
S700K_ELECTRIC_PARAM.4	Starting Current: 8A SIL 0
S700K_ELECTRIC_PARAM.5	Maximum Permissible line resistance: 54 Ω SIL 4

Table 5: Siemens S700K parameters

4.4.1 FUNCTIONAL ANALYSIS

The purpose of this section is to verify functional compliance between the PM4W Point Module and the Siemens S700K point machines.

The functional analysis also includes the cabling system based on 4 wires used for interconnection of PM4W board toward the trackside point.

The analysis is only focused on the specific application, based on a 400 VAC three phase Power Supply.

The functional interface analysis is based on the following approach:

- Electrical Interface Compliance:
 - PM4W application conditions vs S700K electrical parameters;
 - S700Kelectrical parameters vs PM4Wapplication conditions
- Cabling and interconnection Compliance:
 - PM4W application conditions vs cables features;
 - S700Kelectrical parameters vs cables features.

4.4.1.1 Electrical Interface Compliance

For demonstration purposes, only one parameter is considered and the analysis is carried out based on that.

ID	Application Condition Description
S700K_ELECTRIC_PARAM.1	S700K rated voltage shall be 3 x 400/230 V AC, 50Hz \pm 2%; 110 to 136 V DC.

ANALYSIS

This technical data is related to the point machine rated voltage of 230/400Vac at 50Hz necessary for the activation. 110 to 136Vdc is not applicable for the interconnection with PM4W.

Static Analysis

230/400Vac at 50Hz three phase voltage is compliant with the typical PM4W output voltage however, for the point machine, no information are provided for the minimum and maximum voltage values.

For this reason an open point has been raised and a functional test is requested to verify the compliance between PM4W and the point machine.

Required Test

The functional test requested to verify the compliance between PM4W and the point machine is designated the ID: [FUNC_TEST_01]

The description of the test is included in Appendix D.

Analysis Result

[FUNC_TEST_01] has been done with positive results and hence the open point raised previously has been closed.

4.4.1.2 Cabling Interconnection Functional Compliance

PM4W AC vs Cables features

This section considers as input the Application Conditions classified as functional that are generated by PM4Wsystem and complied by Cables features.

Application Conditions analysis

Following the Application Conditions involved is taken into account:

[OC-GP_PM4W_AC_4020]	A short circuit involving at least one of the phases U or V is detected and current is cut as soon as 50A is reached. The short circuit between W and N PM4W outputs is not protected (see Figure 4). In this case, external protection shall be provided at system level (i.e. 8A 'Schurter' fuse 8020.5020 on L3 or Neutral wires).
----------------------	---

ANALYSIS

This application conditions considers short circuit protections adopted in case of short circuit fault on U and V phases and on W and N phases of PM4W.

Static Analysis

To detect a short circuit fault on U and V phases, PM4W implements a protection measuring the currents on L1 and L2 wires on channel 1 and on channel 2. These measures are provided to FPGAs and, after, to CPUs that shall disable the two PMC cells to stop the point motor as soon as 50A current is detected.

On W and N phases there is not protection implemented, for this reason the fuse SCHURTER 8A 8020.5020 is used.

According to fuse datasheet, 8020.5020 typology fuse is

- 6.3x32mm with 8A of rated current,
- 500V of rated voltage,
- 2600mW of power dissipation,
- 285 I2t of melting and
- Breaking capability of 1500A without being destroyed or causing an electric arc.

Required Test

[FUNC_TEST_02] has been planned to verify the short circuits protections implemented for PM4W, see Appendix D for test plans.

Short circuit on U and V phases is done to test the protection implemented measuring the L1 and L2 phases currents.

Short circuit of W and N phases is done to test the fuse intervention.

Analysis Result

The open point is CLOSED and [FUNC_TEST_02] is done with positive result.

Moreover, the following Application condition is exported:

PM4W_S700k_IHA_AC4	The Specific Application shall verify that on W and N phases of all PM4W is present the 6.3x32mm Schurter fuse 8020.5020 typology with 8A of rated current, 285 I ² t of melting and a breaking capability of 1500A.	SIL0	Specific Application
--------------------	---	------	----------------------

4.4.2 SAFETY ANALYSIS

The purpose of this section is to demonstrate that, taking into account the application conditions considered safety related, it is possible to interface the PM4W module with the S700K Point Machine.

The analysis performed considers also the possible hazards that can affect the point machine management in a Railway system.

The hazards that will be considered are:

- WRONG COMMAND TO POINT MACHINE
- WRONG CONTROL OF POINT MACHINE

4.4.2.1 Wrong Command to Point Machine

Hazard Description

This hazard considers the unsafe malfunctioning of PM4W that commands the trackside object in an erroneous/undue permissive state.

Application Conditions Analysis

The Application Conditions considered for this analysis are related to the interface between the Trackside Object Point Machine (including Cabling) and the PM4W system, with particular focus on undue activation of the Point Machine when the Point Module Board is into no-permissive state.

ID	Application Condition Description
[OC-GP_PM4W_AC_4009]	The Point Machine shall ensure that point movement cannot be possible in case of point motor voltage less or equal to 80V single phase AC or DC.

ANALYSIS

The objective of this analysis is to demonstrate that the S700K point machines are compliant with the Application Condition of PM4W, classified with SIL4 safety level, in order to guarantee no motion of the Trackside Object Point Machine when PM4W output voltage is equal or less than 80V.

Static Analysis

S700K technical data state that the powering voltage for motor activation shall be:

- 400 V AC, 3~ 50/60 Hz
- 110 V DC to 136 V DC

According with the above technical specifications, voltage values equal or lower than 80VAC are not able to allow point movement. However a test shall be required in order to confirm the static analysis and verify that no undue movement occurs.

Required Tests

The static analysis requires confirmation by laboratory test in order to ensure fully compliance between PM4W and S700K.

The TEST ID, required to confirm static analysis, is [SAFE_TEST_01]. Please refer to Appendix D for the test plan and report.

Analysis Results

The static analysis related to the object condition states that 80VAC power supply provided by PM4W does not lead to undue activation of point machine. However the static analysis requires a confirmation by laboratory test.

[SAFE_TEST_01] has been done applying 80VAC single phase and no point motor motion has occurred.

PM4W		S700K		Compliance	Note	Status	Required Test
Description	Value	Description	Value				
L1, L2, L3, N Point Motor Power Supply	<i>Min</i> (-15%) 195.5/340 V _{AC} PhaseVAC	Power supply voltage	<i>Min</i> NOT DEFINED	OK	The typical value of point motor power supply provided by PM4W is compliant with the one of S700K point machine reported also in S700K_ELECTRIC_PARAM.1 taken from [S700K_DT] and [S700K_OM]. However, no information have been provided for the minimum and the maximum point machine power supply. For this reason, the compliance with minimum and maximum	OPEN OP_IHA.7 CLOSED	FUNC_ TEST_0 1
U1, V1, W1, N1 (U2, V2, W2, N2) Point Machine voltage (Point Cell Command)	<i>Typ</i> 230/400 V _{AC} PhaseVAC		<i>Typ</i> 230/400 V _{AC} 3Phase	OK			

	Max	(+10%) 253/440 V _{AC} PhaseVAC	Max	NOT DEFINED	OK	<p>values of S700K shall be tested to complete and confirm the analysis considering voltage drop on cables length.</p> <p>[IF_FUN_TEST-001] has been done with positive results for S700K 5.5kN in Alstom site while for S700K 7kN the tests have been done in Glogovat site. See §8 for tests done in Glogovat.</p> <p>About the power supply interruptions, the PM4W has been tested in the OC-GP type tests campaign scope while they are not considered for the interfacing with the point machines because the motor is not sensitive to the interruptions with duration of ms.</p> <p>The Motor is involved in the Movement function that is not safety-related, moreover the Motor is powered on demand (not continuously powered), and a possible power supply deviation affecting the switching causes the interruption of the switching revealed by the missing of detection of position (for the required position).</p>	
--	-----	---	-----	----------------	----	---	--

Table 6: Three Phase AC Motor Interface Compliance

4.4.2.2 Wrong Control of Point Machine

Hazard Description

This hazard considers the unsafe malfunctioning of PM4W that sends to Signalling Computer incorrect/undue permissive state of the inputs acquired from the interfaced point machine.

Application Conditions

The Application Conditions considered for this analysis are related to the interface between the Trackside Object Point Machine (including Cabling) and the PM4W system (section PPM), with particular focus on missing detection of incorrect/not-allowed Point Position.

Following is the Application Condition involved:

[OC-GP_PM4W_AC_4008]	<p>Point Machine shall guarantee mechanical contacts closure only in case of correct final position of Point (NORMAL or REVERSE or STAR) is reached; so it shall guarantee mechanical contacts opening in all other positions. When Point Machine is not in a correct position, mechanical contacts shall not be in a valid position in order to make the PM4W able to detect UNLOCKED (see the schemes in Figure 5).</p> <p>These constraints are verified for Siemens S700K 5,5kN, Siemens S700K 7kN, VoestAlpineHydrostarCombi and Thales L700H (IHA [16][17][18]). In case different point machines are used, the same verification and validation activities shall be repeated.</p>
----------------------	--

ANALYSIS

Objective of the Analysis

The objective of this analysis is to verify the correct operation between PM4W and S700K Point Machine, in order to move the point into the allowed conditions: NORMAL and REVERSE. The integrated system (PM4W with S700K) shall be able to detect different point positions and consequentially generate LOCKED NORMAL, LOCKED REVERSE, STAR CONFIGURATION and, in case of control loss, UNLOKED state to send at Signalling Computer.

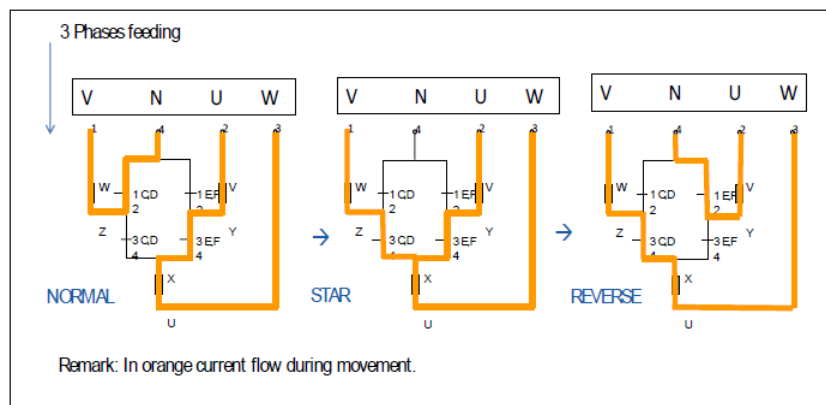


Figure 17: Point Machine NORMAL to REVERSE movement

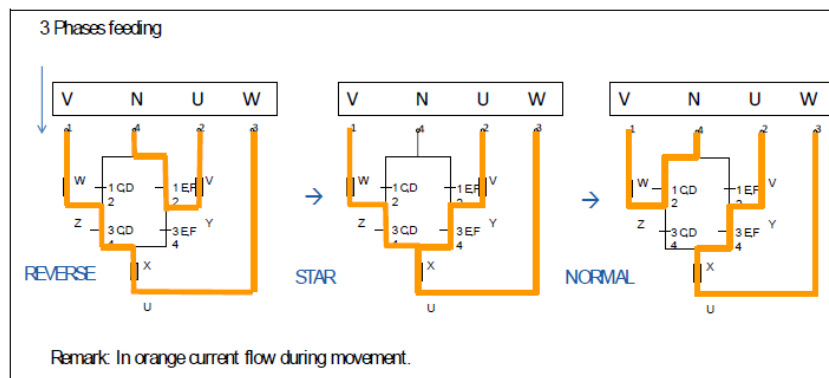


Figure 18: Point Machine REVERSE to NORMAL movement

Static Analysis

The verification of this application condition requires a laboratory test in order to verify fully functional and safety compliance between PM4W and S700K Point Machine.

Required Tests

The test required by static analysis is SAFE_TEST_02. Appendix D reports the detail description of this test.

Analysis Results

COMPLETE/CLOSED and SAFE_TEST_02 has been done with positive result.

4.4.2.3 Cabling Interconnection Safety Compliance

PM4W AC vs Cables features

This section considers as input the Application Conditions classified as safety that are generated by PM4Wmodule (see [OCGP_AC]) and complied by Cables features.

Application Conditions analysis

Following the Application Conditions involved are listed:

ID	Application Condition Description
[OC-GP_PM4W_AC_3016]	The cables and filters interfaced to PM4W shall be compliant to the exported constraints listed in Table 2. These constraints are listed in §2.2.1.2 of OC-GP Installation Manual (Ref. [5])

ANALYSIS

This section reports the safety compliance of cables connected to PM4W environmental characteristics.

Whenever static comparing analysis leads to no total safety compliance, laboratory test will be required in order to verify the correct interfacing between PM4W and S700K (including Cabling).

Static Analysis

This application condition makes reference to some environmental aspects that shall be satisfied by cables interfaced with the product.

To analyse this application condition, the Alstom OC-GP application conditions has been reported in the following Table 7 of this document.

Moreover, Table 7 reports a comparing analysis between the PM4W constraints and the electrical requirements of cables in order to verify the cables compliance with the PM4W system for Point Machine Command and Control.

Type	PM4W Constraint	Cable Specification	Compliance	Note
Climatic	The use of DILMP20 CONTACTOR ASSEMBLY code DTR0000323604 is limited to -5°C÷55°C	NA	NA	-
EMI/EMC (Comply with EN 50121-4)	400Vac power supply interface shall be filtered to conducted emitted disturbances with a filter FINMOTOR 1740.012.M or equivalent.	NA	NA	-
	H15 PM4W Guest cable shall be shielded to comply with 4KV surge level (without shield surge immunity level shall be 2KV).	3500 V CS2YabY-F (unshielded cable)	OK	OP_IHA.4 has been closed.Theapplication condition shall be exported to OC-GP Installation Manual.
		3500 V CS2YEAIAbY-F (shielded cable)	OK	OP_IHA.4 has been closed.Theapplication condition shall be exported to OC-GP Installation Manual.
	For 24Vdc (PM4W Contactor power supply) cable lengths above 3m, a surge protection on 24Vdc interface shall be provided by means of varistors similar to DTR0000324499 varistor 85Vdc, 4500A.	Missing information about system integration	OK	OP_IHA.5point has been closed in this document release.
	24V (PM4W Contactor power supply) cable shall provide two turns on ferrite Fair rite 0431176451 DTR0000302202.	Missing information about system integration	OK	OP_IHA.5point has been closed in this document release.
	F48 PM4W Guest cable shall be shielded (see note). Note: Not shielded F48 PM4W Guest cable with 4 turns on ferrite Fair rite 0431176451 DTR0000302202 protects the interface to fast transient disturbances. The filter is not sufficient to limit radiated disturbances that in this case are 3dB over the mask limit.	Missing information about system integration	OK	OP_IHA.5point has been closed in this document release.
	230Vac PS cable shall provide two turns on ferrite Fair rite 0431176451 DTR0000302202.	Missing information about system integration	OK	OP_IHA.5point has been closed in this document release.
	230Vac PS power supply interface shall be filtered to conducted emitted disturbances with a filter CORCOM 3EK1 or equivalent.	Missing information about system integration	OK	OP_IHA.5point has been closed in this document release.

Table 7 – PM4W and Cable Compliance of environmental characteristics

Required Test

No laboratory test is required.

Analysis Results

COMPLETE/PARTIALLY CLOSED

The previous analysis raised open points that are closed.

4.4.3 Overview

The analysis shows that at least some tests are required in the field to ascertain the functioning of the machines as intended. Infact, the manufacturer's opinion about the field trials were countered by the ISA with a technical note with "open" status. Thereby a new field trial plan was proposed by the manufacturer and was approved by the ISA. The field trials are commencing soon on the eastern corridor of the DFFCI project.

This instance also demonstrates the importance of an ISA in the safety assessment and authorisation process of placing products in service in the railway sector.

5 Conclusion

The primary philosophy regarding the procedure for obtaining an APIS in both the railways in Italy and India are similar. Both these systems follow the CENELEC defined product life-cycle approach for the RAMS management, but differences start emerging in the methodology which is followed.

The Indian system is in its developmental phase, slowly evolving towards a more robust and unique system catering to the requirements of the nation in this fast paced global economy. The RDSO specifications, at the moment, are not covering all aspects of the safety conformity process. Thus, the European standards must be incorporated to fill the gaps. However, in doing so, some undesirable outcomes emerge as these standards often clash stating different specifications which result in ambiguity over which specification is to be followed.

Moreover, as the analysis demonstrated, without the proper execution of field tests before commissioning, the safe and sound functioning of the products as well as the whole system could possibly be compromised. Infact, without the tests on field the safe integration of different sub-systems cannot be fully ascertained and it could potentially lead to a hazard.

It is the opinion of the author that the RDSO specification, which generally not being erroneous, still invokes some ambiguity which could be minimised by incorporating a well-structured and more organised approach. The Italian approach from a broad perspective, at this moment appears to be better equipped to handle the complex task of conforming to a high level of safety and authorise the use of products with a structured and organised methodology involving rigorous testing and analysis. However, a deeper analysis reveals that satisfying the numerous normative can sometimes blow up and result in a loop; the harmonisation of the specifications are desirable. The Indian approach is minimalistic in this regard, with just one primary guideline (RFP). Thus the two systems have huge potential to collaborate, exchange experiences and improve themselves.

Italcertifier, is collaborating to point out pathways to upgrade the whole architecture of the specifications and management of the Indian Railways in terms of procedures, technologies and know-hows. RDSO has been revising some of its specifications and incorporating changes in the standards to march towards a safer and more efficient system. As the trend continues, hopefully with other ISAs too, the near future will witness the Indian specifications and the processes for authorising the placing of railway products in use to be at par with their European counterparts.

6 References

Index		Version	Title
[Ref.1] - EN 50126-1		2007	Railways applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS process, CENELEC
[Ref.2] - EN 50126-2		2007	Railways applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety, CENELEC
[Ref.3] - Guidelines		2017	Linee guida per il rilascio dell'autorizzazione di messa in servizio di veicoli e sottosistemi strutturali e dell'autorizzazione all'utilizzo di applicazioni generiche, prodotti generici e componenti, ANSF
[Ref.4] - (EU) 402		2013	Regulation (EU) 402/2013 on the CSM for risk assessment and repealing Regulation 352/2009
[Ref.5] - Dir. 191		2010	Attuazione della direttiva 2008/57/CE e 2009/131/CE relativa all'interoperabilità del sistema ferroviario comunitario.
[Ref.6] - SPN. 144		2006	Safety and Reliability requirements of electronic signalling equipments, RDSO
[Ref.7] - SPN. 203		2011	Electronic Interlocking for big yards, RDSO
[Ref.8] - IEC 60068-2		2017	Environmental testing – Test and guidance, IEC
[Ref.9]		-	https://www.ansf.it/agency-english , ANSF
[Ref.10]		-	http://www.rdsi.indianrailways.gov.in/ , RDSO
[Ref.11]		-	https://www.scribd.com/document/53312590/SSL-SML400-A4
[Ref.12]		-	https://www.cenelec.eu/ , CENELEC
[Ref.13]		-	http://www.italcertifier.com/aboutus.php , ITCF
[Ref.14]	(EU) 57	2008	Directive 2008/57/EC of the European Parliament of the Council of 17 June 2008 on the interoperability of the rail system within the Community
[Ref.15]	(EU) 49	2004	Directive 2004/49/EC of the European Parliament of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification
[Ref.16]		2003	CENELEC Phase 3/Guidelines for Hazard Analysis, UIC
[Ref.17]	EN 50128	2011	Railway applications: Software for railway control and protection systems, CENELEC
[Ref.18]	EN 50129	2010	Railway Applications – Communication, signalling and processing systems -Safety related communication in transmission systems, CENELEC

Appendix A

RAMS tasks along life-cycle phases [Ref.1]

<i>Phase</i>	<i>Phase</i>	<i>Clause</i>	<i>General tasks</i>	<i>RAM tasks</i>	<i>Safety tasks</i>
1	Concept	7.2	Investigate scope, context and purpose of the system. Investigate the environment of the system.	Investigate the general RAM implications of the system. Investigate previous RAM requirements and past RAM performance of similar/related systems. Investigate current RAM policy and targets of the relevant railway duty holders. Define the scope of the RAM management requirements for subsequent system life-cycle RAM tasks.	Investigate the general safety implications of the system. Investigate previous safety requirements and past safety performance of similar/related systems. Investigate current safety policy and targets of the relevant railway duty holders. Investigate safety legislation. Define the scope of the safety management requirements for subsequent system life-cycle safety tasks.
2	System definition and operational context	7.3	Define the system and its mission profile. Define the system boundary. Define the scope of operational requirements. Establish the organisation.	Establish the RAM policy. Establish the RAM plan.	Establish the safety policy. Establish the safety plan.
3	Risk analysis and evaluation	7.4		Perform Risk Analysis. Update RAM Plan.	Perform risk analysis. Establish hazard log. Update Safety Plan. Establish Independent Safety Assessment Plan.

<i>Phase</i>	<i>Phase</i>	<i>Clause</i>	<i>General tasks</i>	<i>RAM tasks</i>	<i>Safety tasks</i>
4	Specification of system requirements	7.5	Specify system requirements	Establish RAM requirements specification. Update the RAM plan. Establish validation plan for RAM requirements.	Establish safety requirements specification. Establish safety-related application conditions. Update hazard log. Update the safety plan. Establish validation plan for safety requirements.
5	Architecture and apportionment of system requirements	7.6	Define the system architecture. Identify the requirements for integration of pre-existing sub-systems/components. Define acceptance criteria and processes for sub-systems/components.	Allocate RAM requirements to sub-systems/components. Update the RAM plan. Update validation plan for RAM requirements.	Perform hazard analysis. Allocate safety requirements to sub-systems/components. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements.
6	Design implementation and	7.7	Design sub-systems/components. Prepare operation and maintenance procedures. Define training measures for operation and maintenance. Define and establish manufacturing process for producing sub-systems and components. Define and establish system integration process. Prepare installation and commissioning procedures.	Plan RAM tasks of further phases. Perform RAM analysis. Update the RAM plan. Update validation plan for RAM requirements.	Plan safety tasks of further phases. Perform hazard analysis. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Prepare safety case.

<i>Phase</i>	<i>Phase</i>	<i>Clause</i>	<i>General tasks</i>	<i>RAM tasks</i>	<i>Safety tasks</i>
7	Manufacture	7.8	Implement and operate manufacturing process.	Establish RAM assurance arrangements. Update the RAM plan. Update validation plan for RAM requirements.	Establish safety assurance arrangements. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Update safety case.
8	Integration	7.9	Integrate sub-systems and components. Demonstrate system functionality. Test and analyse system. Arrange system support arrangements.	Establish integration report for RAM requirements. Update the RAM plan. Update validation plan for RAM requirements.	Establish integration report for safety requirements. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Update safety case.
9	System Validation	7.10	Establish validation report. Establish process for the acquisition and evaluation of operational and maintenance data.	Establish RAM validation report.	Establish safety validation report. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Update safety case.
10	System acceptance	7.11	Record an acceptance record. Verify the acceptance record.	Assess RAM validation.	Establish Independent Safety Assessment Report. Assure endorsement of safety-related application conditions.

<i>Phase</i>	<i>Phase</i>	<i>Clause</i>	<i>General tasks</i>	<i>RAM tasks</i>	<i>Safety tasks</i>
11	Operation, maintenance and performance monitoring	7.12	Provide all information necessary to formulate plans/procedures for operation and maintenance. Implement operation and maintenance procedures. Record changes in the system configuration.	Implement and maintain FRACAS process for the acquisition and recording of RAM performance data. Maintain FRACAS and periodically review FRACAS records. Establish records to trace the RAM tasks undertaken. Reports of RAM performance analysis and evaluation.	Implement and maintain process for the acquisition and recording of safety performance data. Perform an impact analysis in case of changes and reapply process if needed. Records to trace the safety tasks undertaken. Establish reports of safety performance analysis and evaluation.
12	Decommissioning	7.13	Establish decommissioning plan and related report.	Identify the RAM impact of decommissioning and disposal.	Identify the safety impact of decommissioning and disposal.

NOTE Change Control or Configuration Management activity applies to all project phases.

Appendix B

Climatic and environmental test requirements [Ref.6]

S. No	Test		Reference	Electronic Equipment				
				Indoor	Out-door		On board	
					On Track	Track side	Inside Cab	Outside Cab
1.	Change of temp test		IS 9000 Part XIV Sect. II	Yes	Yes	Yes	Yes	Yes
	Low temp	-10°C ± 3°C						
	High temp	+70°C ± 2°C						
	Rate of change in temperature	1°C / min						
	Duration	7hrs at each temp. - 10 °C & +70 °C						
	Cycle	3						
	Condition	Fully functional during test						

S. No	Test		Reference	Electronic Equipment				
				Indoor	Out-door		On board	
					On Track	Track side	Inside Cab	Outside Cab
2.	Dry heat test		IEC-571; IS:9000 Part-III Sect 3	Yes	Yes	Yes	Yes	Yes
	Temp	+70°C						
	Duration	16 hrs						
	Condition	Fully functional during test						
3.	Cold test		IS 9000 Part II Sect. III	Yes	Yes	Yes	Yes	Yes
	Temp	-10°C ± 3 °C						
	Duration	2 hours						
	Condition	Fully functional during test.						

4.	Damp heat test (Cyclic)		IS 9000 Part V Sect. 2 Variant 1	Yes	Yes	Yes	Yes	Yes
	Upper temp	40° C ± 2° C						
	Humidity	95% (+1%, -5%)						
	Cycles	6						
	Condition	Fully functional during one hour period towards end of each cycle. Stabilization shall be done at 25° ± 3° C						
5.	Damp heat test (Steady state storage)		IS 9000 Part IV	Yes	Yes	Yes	Yes	Yes
	Temp	40° ± 2° C						
	Humidity	93% (+2% , -3%)						
	Severity	4 days						
	Condition	Fully functional during test.						

S. No	Test		Reference	Electronic Equipment				
				Indoor	Out-door		On board	
					On Track	Track side	Inside Cab	Outside Cab
6.	Salt mist test		IS 9000 Part XI procedure 3	Yes Procedure 3	Yes Procedure 2	Yes Procedure 2	Yes Procedure 3	Yes Procedure 2
	Mist + Damp heat	Procedure 2: 2 hours + 7 days Procedure 3: 2 hours + 22 hours						
	Temp	35° ± 3° C						
	Humidity	93% (+2%, -3%)						
	Hours	22						
	Cycle	3						
	Condition	After this test, electrical parameters shall be monitored in addition to physical checks.						

7.	Dust test		IS 9000 Part XII	Yes	Yes	Yes	Yes	Yes
	Duration	1hour						
	Condition	After this test, electrical parameters shall be monitored in addition to physical checks.						
8.	Water Immersion test		IS 9000 Part XV Sect. 7	No	Yes	No	No	No
	Head of water	0.4 m						
	Duration	24 hours						

S. No	Test		Reference	Electronic Equipment				
				Indoor	Out-door		On board	
					On Track	Track side	Inside Cab	Outside Cab
	Condition	After this test, electrical parameters shall be monitored in addition to physical checks (Ingress of water).						
9	Driving Rain test		IS 9000 Part XVI Test condition 'c'	No	Yes	No	No	Yes
	Water spray for 1 hour							
	Condition	After this test, electrical parameters shall be monitored in addition to physical checks.						

10	Bump test		IS 9000 Part VII, Sec. 2	Yes	Yes	Yes	Yes	Yes
	PCBs/Modules/units in packed condition shall be subjected to bump test as under:							
	No of bumps	1000						
	Peak acceleration	400 m/s ²						
	Pulse duration	6 ms						
	No of axes	3						
	Condition	After this test, electrical parameters shall be monitored in addition to physical checks.						

S. No	Test	Reference	Electronic Equipment				
			Indoor	Out-door		On board	
				On Track	Track side	Inside Cab	Outside Cab
11	Shock test (to simulate the effect of shunting shock)	IS 9000 Part VII Sec. 1	No	Yes Severity 2	Yes Severity 1	Yes Severity 1	Yes Severity 1
	Severity 1: The equipment in operation shall be subjected for 2 minutes to 50 Hz vibration of such nature that the maximum acceleration is equal to 30 m/s ² (amplitude a=0.3 mm). At the end of the test, the assembly shall be subjected to performance test as specified in relevant specification.						
	Severity 2: Peak acceleration: 40 g. Duration of the pulse: 11 m.sec. No. of shocks: 18 Velocity change : Half sine pulse Equipment in unpacked condition shall be subjected to Bump test. In addition to physical checks, the assembly shall be subjected to performance test.	IS 9000 Part VII Sec. 1 Clause 9					
12	Vibration test		TEC (IPT 1001A- revised)	Yes	Yes	Yes	Yes
		Up to & including 75 Kgs. weight					
	Freq. Range	05-350 Hz 5-150 Hz					

S. No	Test			Reference	Electronic Equipment				
					Indoor	Out-door		On board	
						On Track	Track side	Inside Cab	Outside Cab
	Amplitude	± 6 mm constant displacement or 15m/Sec. ² constant acceleration.	± 6 mm constant displacement or 15m/Sec. ² constant acceleration.						
	No. of axes	3	3						
	No of sweep cycle	20	10						
	Total duration	105 min	105 min						
	If resonance is observed	10 min at each resonant freq.	10 min at each resonant freq.						
	Condition	After this test, electrical parameters shall be monitored in addition to physical checks.							

S. No	Test	Reference	Electronic Equipment				
			Indoor	Out-door		On board	
				On Track	Track side	Inside Cab	Outside Cab
13.	Environmental Stress Screening tests (ESS) for Printed Circuit Boards (PCB) & sub systems <i>(The manufacturer shall carry out the following ESS tests on all modules on 100% basis (except bump test) during production / testing in the sequence as follows. Suitable records shall be maintained regarding the compliance of these tests.)</i>		Yes	Yes	Yes	Yes	Yes
13.1	Thermal cycling The PCBs shall be subjected to thermal cycling as per the procedure given below. The assembled boards are to be subjected to rapid temperature cycling as mentioned below in the power off condition.		Yes	Yes	Yes	Yes	Yes
	❖ This temperature cycling from 0° C to 70°C, ½ Hours at each temperature for 9 cycles and 1 hour at each temp. for the 10 th cycle. Dwell time of 1 hour is provided for the last cycle in order to oxidize defective solder joints exposed through thermal stress.						

	<div><div><div><div><div></div><div>Hour</div></div><div><div>Ambient</div><div><div><div><div></div><div>70° C, ½</div><div>1 Hour</div></div></div></div></div></div><div><div><div></div><div>0° C, ½ Hour</div></div><div><div>❖ The rate of rise / fall of temp. shall be minimum 10° C per minute.</div><div>❖ In addition to physical checks, the electrical parameters are also to be monitored after this test.</div></div></div></div></div>						
13.2	Power cycling: The power supply modules shall be subjected to 60 ON-OFF cycles for 1 hour. The ON-OFF switch usually provided in the modules may not be used for this purpose.		Yes	Yes	Yes	Yes	Yes

Appendix C

Type test list from GP TT Plan

SUMMARY OF TYPE TEST PLAN			
Test category	Test		
ELECTRICAL TESTS of power supply	AC voltage variation (stationary)		Radio-frequency electromagnetic field. Amplitude modulated
			Radio-frequency electromagnetic field from digital radio telephones
	Power frequency variation (stationary)	ELECTROMAGNETIC EMISSION TESTS	Conducted emission
	AC voltage variation (dynamic) and voltage interruption (IS 402)		Radiated emission
SUSCEPTIBILITY TESTS TO CONDUCTED DISTURBANCE	AC voltage variation (dynamic) and voltage interruption (EN 61000-6-2)	INSULATION TEST	Measurement of insulation resistance
	Electronic discharge (ESD)		Leak test to impulse test
	Fast transient bursts (EFT)		
	High energy and voltage transient burst (surge voltage)		
	Conducted disturbance induced by radio- frequency fields		
	Conducted disturbance induced by fields at traction frequency (50 Hz)		
SUSCEPTIBILITY TESTS TO RADIATED DISTURBANCE	Electromagnetic field at traction frequency		
	Pulse magnetic field		

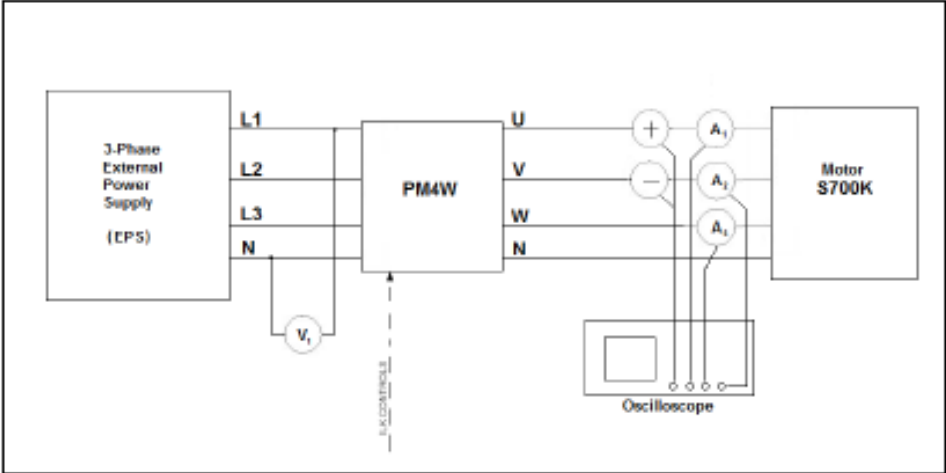
	Leak test to impulse test: RFI Compliance	PRODUCT SECURITY TESTS	Final research of resonant frequencies (sinusoidal scan)
	Dielectric strength test		Shock resistance
	Dielectric rigidity		Temperature increasing
	Dielectric rigidity under operating temperature conditions		Resistance to abnormal heating
			Contact current and protective conductor current
CLIMATIC TESTS	Temperature variation		Dielectric rigidity under operating temperature conditions



	Dry heat
	Cyclic damp heat (1° cycle)
	Cold test
	Cyclic damp heat (2° cycle)
	Low temperature storage test
MECHANICAL TESTS OF VIBRATIONS	Resonant frequency initial research (sinusoidal sweep)
	Stress test with sinusoidal vibrations at resonant frequencies
	Functioning test with random vibrations

Appendix D

Required tests as per the Hazard Analysis

	<div style="display: flex; justify-content: space-between;"> FUNC_TEST_01 Electrical Compliance Operation for Motor Driving </div>
Test Objective	<p>Demonstrate correct operation and fully functional and electrical compliance between PM4W Module and S700K when the external Power Supply (400 V_{AC} three phase) ranges from minimum value to maximum value of voltage and frequency (considering worst cases for cable length).</p> <p>Demonstrate current compliance during position detection.</p>
Test Plan	<p>The following Figure 9 contains a possible set-up used for the test</p> <div style="text-align: center;">  <p>Figure 9 – Setup IF_FUN_TEST-001</p> </div> <p>Three different Operations are considered in order to take into account the three different S700K point machine power supply values.</p> <p>Operation 1</p> <ul style="list-style-type: none"> • Program the External Power Supply (EPS) with minimum voltage value for Power Supply used in Romania application (195.5 V_{AC} 3-phase). • Program the External Power Supply (EPS) with a frequency of 50Hz. • Measure L1, L2, L3 Output Voltage (referred to N) with Voltmeter to ensure that programmed value is respected. • Stand-by the EPS. • Connect the EPS to the powering input of PM4W module as indicated in the setup of Figure 9. • Connect the PM4W with S700K using the maximum length cable configuration to have 54 ohm of resistance line (this resistance value is referred to S700K 5.5kN point machine, for S700K 7kN point machine 34 ohm of resistance line shall be used). • Configure the PM4W system to operate with nominal value 400 V_{AC} 3-phase 50 Hz. The following parameters, provided in [OCGP_AC], shall be set as follows: <ul style="list-style-type: none"> ◦ PS_VALUE = 400 (400 V_{AC}); ◦ PS_FREQUENCY = 50 (50 Hz). • Configure the PM4W system to operate with a maximum timeout of 10s: <ul style="list-style-type: none"> ◦ MOVEMENT_MAX_DURATION = 10 (10s); • Switch-on the EPS from stand-by. • Execute the movement from NORMAL position to REVERSE position.

- During point movement acquire and record the following test measurement:
 - Peak Current on A1, A2, A3;
 - Nominal Current (RMS value) on A1, A2, A3;
 - Point Machine Input Frequency and Voltage using voltage probe on U-V phases;
- When Movement is completed and position is locked, measures the TX detection current signal on A1 and A2 probes.
- Execute the movement from REVERSE position to NORMAL position.
- During point movement acquire and record the following test measurement:
 - Peak Current on A1, A2, A3;
 - Nominal Current (RMS value) on A1, A2, A3;
 - Point Machine Input Frequency and Voltage using voltage probe on U-V phases;
- When Movement is completed and position is locked, measures the TX detection current signal on A1 and A2 probes.

Operation 2

- Program the External Power Supply (EPS) with maximum voltage value for Power Supply used in Romania application (253 V_{AC} 3-phase).
- Program the External Power Supply (EPS) with a frequency of 50Hz.
- Measure L1, L2, L3 Output Voltage (referred to N) with Voltmeter to ensure that programmed value is respected.
- Stand-by the EPS.
- Connect the EPS to the powering input of PM4W module as indicated in the setup of Figure 9.
- Configure the PM4W system to operate with nominal value 400 V_{AC} 3-phase 50 Hz. The following parameters, provided in [OCGP_AC], shall be set as follows:
 - PS_VALUE = 400 (400 V_{AC});
 - PS_FREQUENCY = 50 (50 Hz).
- Configure the PM4W system to operate with a maximum timeout of 10s:
 - MOVEMENT_MAX_DURATION = 10 (10s);
- Switch-on the EPS from stand-by.
- Execute the movement from NORMAL position to REVERSE position.
- During point movement acquire and record the following test measurement:
 - Peak Current on A1, A2, A3;
 - Nominal Current (RMS value) on A1, A2, A3;
 - Point Machine Input Frequency and Voltage using voltage probe on U-V phases;
- When Movement is completed and position is locked, measures the TX detection current signal on A1 and A2 probes.
- Execute the movement from REVERSE position to NORMAL position.
- During point movement acquire and record the following test measurement:
 - Peak Current on A1, A2, A3;
 - Nominal Current (RMS value) on A1, A2, A3;
 - Point Machine Input Frequency and Voltage using voltage probe on U-V phases;
- When Movement is completed and position is locked, measures the TX detection current signal on A1 and A2 probes.

Operation 3

- Program the External Power Supply (EPS) with typical voltage value for Power Supply used in Romania application (230 V_{AC} 3-phase).
- Program the External Power Supply (EPS) with a frequency of 50Hz.
- Measure L1, L2, L3 Output Voltage (referred to N) with Voltmeter to ensure that programmed

Expected Results

Input Voltage and Frequency Measurements for Point Machine					
Operation	E1	E2	E3	Frequency	Motion
Operation1	195.5V ^(*)	195.5V ^(*)	195.5V ^(*)	50Hz	Normal to Reverse
	195.5V ^(*)	195.5V ^(*)	195.5V ^(*)	50Hz	Reverse to Normal
Operation2	253V	253V	253V	50Hz	Normal to Reverse ^(**)
	253V	253V	253V	50Hz	Reverse to Normal ^(**)
Operation3	230V	230V	230V	50Hz	Normal to Reverse
	230V	230V	230V	50Hz	Reverse to Normal

(*) The voltage range value considered for E1, E2 and E3 (star voltages) takes into account the power supply minimum voltage values of PM4W and S700K point machine. However, during the test with long cable, possible voltage drop due to cable shall be considered.

(**) Motion is correctly implemented and no cables damage occurs in V_{MAX} operation.

Current Measurements (during point movement)

Operation	A1 _{pk}	A2 _{pk}	A3 _{pk}	A1 _{RMS}	A2 _{RMS}	A3 _{RMS}	Motion
Operation1	<17A	<17A	<17A	<5A	<5A	<5A	Normal to Reverse
	<17A	<17A	<17A	<5A	<5A	<5A	Reverse to Normal
Operation2	<17A	<17A	<17A	<5A	<5A	<5A	Normal to Reverse
	<17A	<17A	<17A	<5A	<5A	<5A	Reverse to Normal
Operation3	<17A	<17A	<17A	<5A	<5A	<5A	Normal to Reverse
	<17A	<17A	<17A	<5A	<5A	<5A	Reverse to Normal

Current Measurements (during point position detection)

Operation	A1	A2	Position
Operation1	-55mA _{peak} ≤ I _{peak} ≤ -45mA _{peak}	+45mA _{peak} ≤ I _{peak} ≤ +55mA _{peak}	Locked Normal
	-55mA _{peak} ≤ I _{peak} ≤ -45mA _{peak}	+45mA _{peak} ≤ I _{peak} ≤ +55mA _{peak}	Locked Reverse
Operation2	-55mA _{peak} ≤ I _{peak} ≤ -45mA _{peak}	+45mA _{peak} ≤ I _{peak} ≤ +55mA _{peak}	Locked Normal
	-55mA _{peak} ≤ I _{peak} ≤ -45mA _{peak}	+45mA _{peak} ≤ I _{peak} ≤ +55mA _{peak}	Locked Reverse
Operation3	-55mA _{peak} ≤ I _{peak} ≤ -45mA _{peak}	+45mA _{peak} ≤ I _{peak} ≤ +55mA _{peak}	Locked Normal
	-55mA _{peak} ≤ I _{peak} ≤ -45mA _{peak}	+45mA _{peak} ≤ I _{peak} ≤ +55mA _{peak}	Locked Reverse

Obtained
Results

Check of configuration file used for the test campaign:

- PS_VALUE set to 400
- PS_FREQUENCY set to 50
- MOVEMENT_MAX_DURATION set to 10

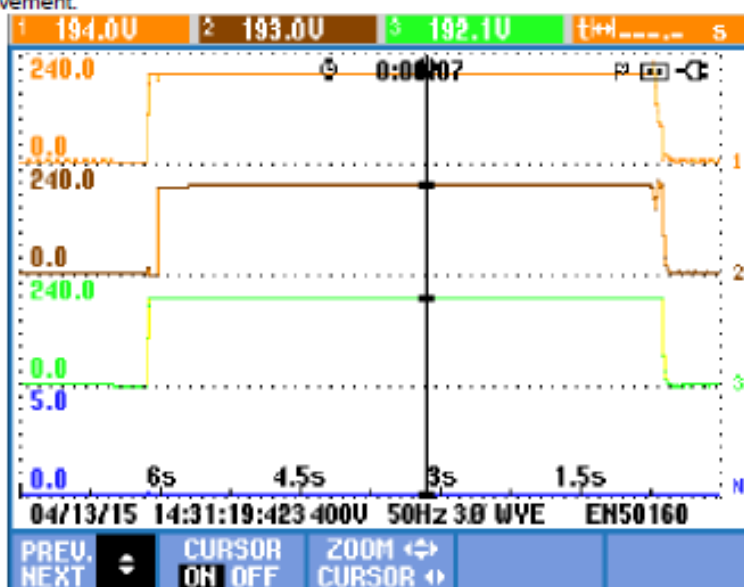
Configuration file used for the tests is annexed to this IHA (see §12). PS_VALUE, PS_FREQUENCY and MOVEMENT_MAX_DURATION parameters for PM4W product are find in the .xml file part related to LRU_TYPE = "LRU_PM4W".

Input Voltage(RMS value) and Frequency Measurements for Point Machine

Operation	E1	E2	E3	Frequency	Motion
Operation1	194V	193V	192.1V	50Hz	Normal to Reverse
	192.9V	193.9V	192.1V	50Hz	Reverse to Normal
Operation2	253V	251.3V	250.2V	50Hz	Normal to Reverse
	251.1V	252.9V	250.2V	50Hz	Reverse to Normal
Operation3	230.9V	230.1V	228.4V	50Hz	Normal to Reverse
	230.2V	231.1V	228.5V	50Hz	Reverse to Normal

Operation 1 – Voltage and Frequency measurements

The following figures contains the voltage (RMS value) and frequency measurements during the point machine movement.



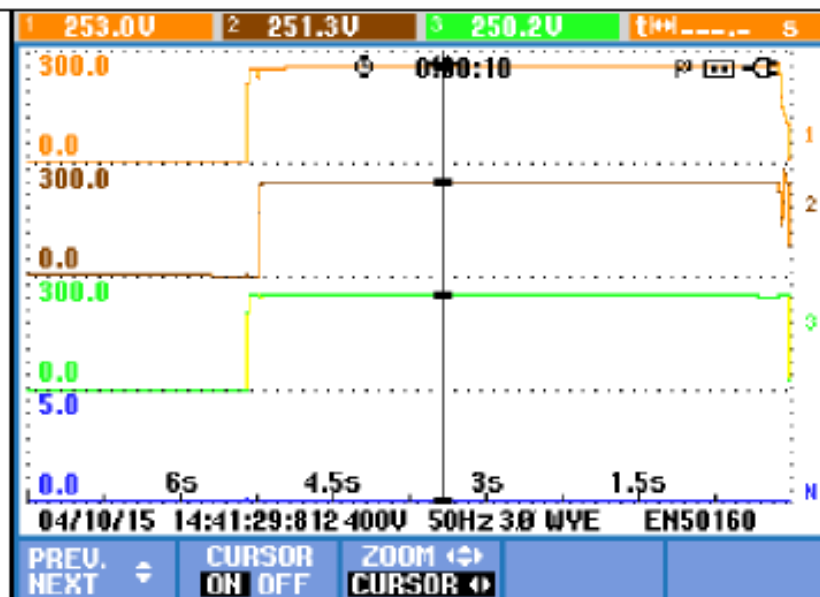


Figure 12 – Operation 2 – Voltage measurements during Normal to Reverse movement

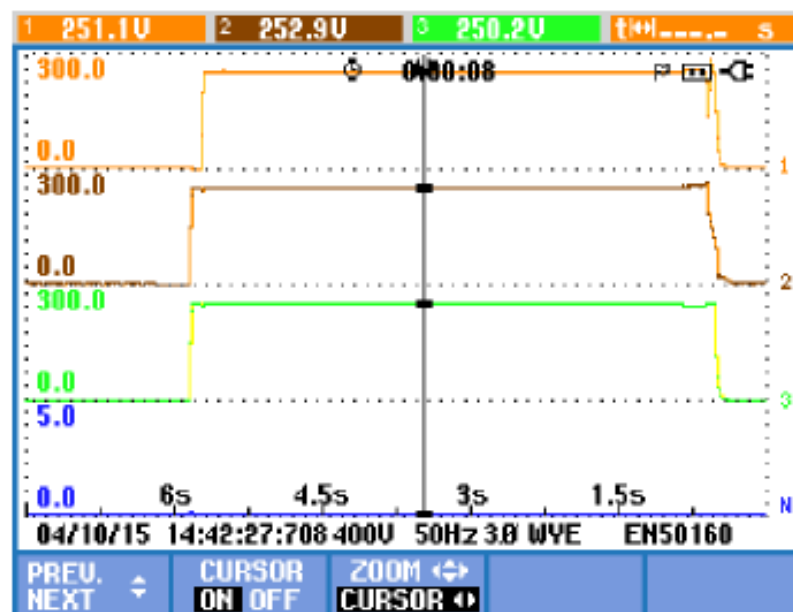


Figure 13 – Operation 2 – Voltage measurements during Reverse to Normal movement

Operation 3 – Voltage and Frequency measurements

The following figures contains the voltage (RMS value) and frequency measurements during the point machine movement.

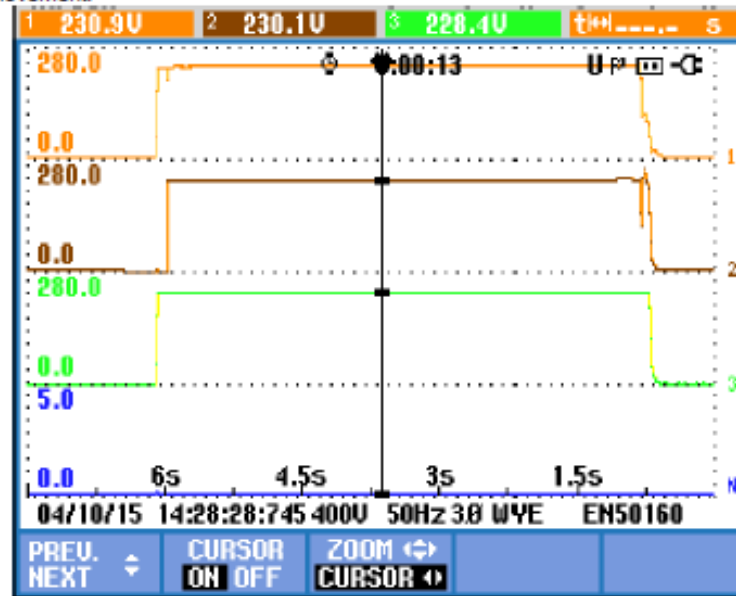


Figure 14 – Operation 3 – Voltage measurements during Normal to Reverse movement

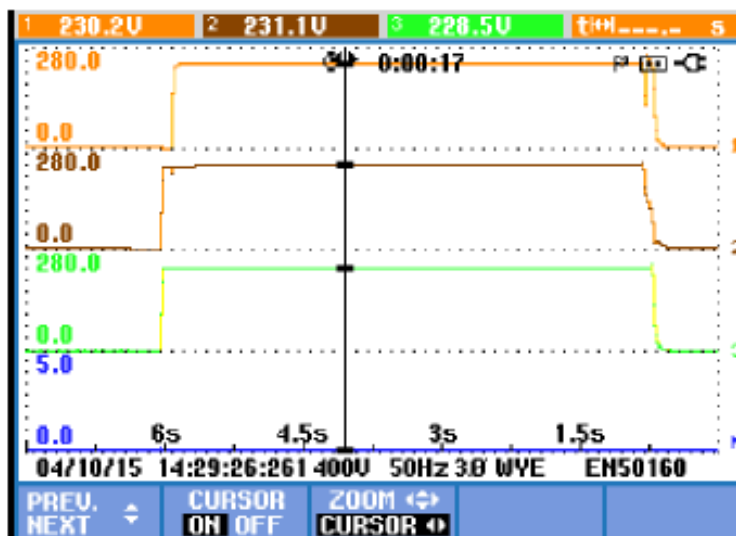


Figure 15 – Operation 3 – Voltage measurements during Reverse to Normal movement

Current Measurements (peak and RMS value during point movement)

Operation	A1 _{pk}	A2 _{pk}	A3 _{pk}	A1 _{RMS}	A2 _{RMS}	A3 _{RMS}	Motion
Operation 1	2.1A	1.5A	2.1A	1.2A	1.2A	1.2A	Normal to Reverse
	1.5A	2.1A	2.1A	1.2A	1.2A	1.2A	Reverse to Normal
Operation 2	8.2A	8.8A	7.7A	4.1A	3.7A	3.9A	Normal to Reverse
	8.5A ^(*)	7.8A	7.7A	3.6A	4.1A	3.8A	Reverse to Normal
Operation 3	6.2A	6.8A	6.9A	2.8A	2.6A	2.7A	Normal to Reverse
	6.9A	6.5A	6.9A	2.7A	2.8A	2.7A	Reverse to Normal

(*) 8.5A is the peak current measure on L1 phase and shown in Figure 22.

Operation 1 – Current measurements

The following figures contains the pick currents measurements during the point machine movement.

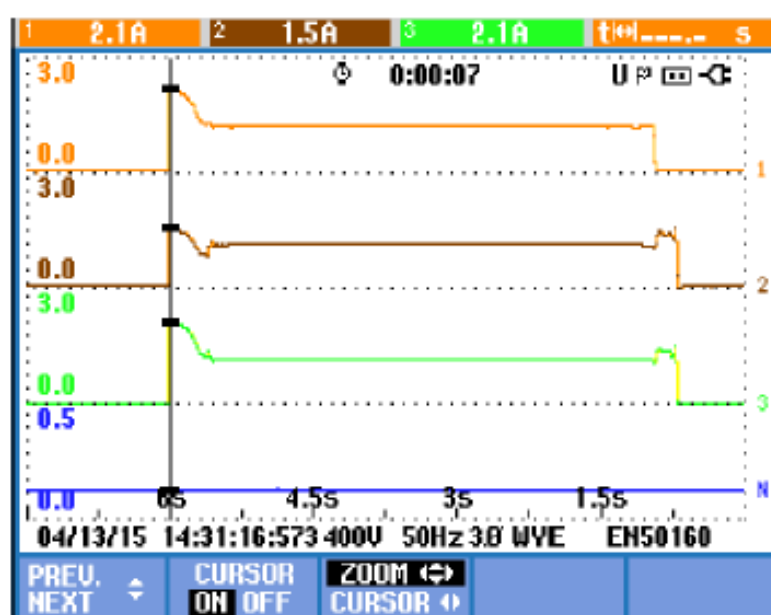


Figure 16 – Operation 1 – Peak current during Normal to Reverse movement

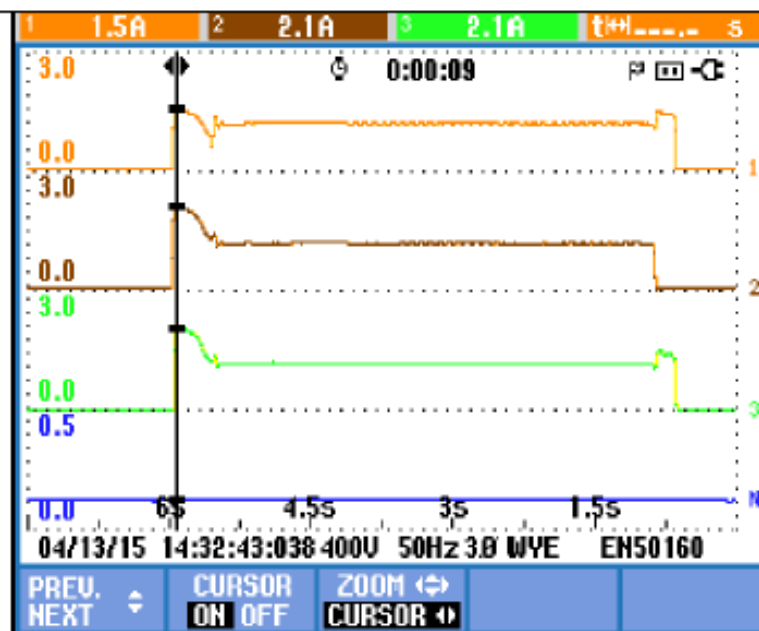


Figure 17 – Operation 1 – Peak current during Reverse to Normal movement

The following figures contain the nominal currents measurements:

Test Objective

Demonstrate that the PMC board can withstand up to 100A output short circuit condition, before output fuse protection.

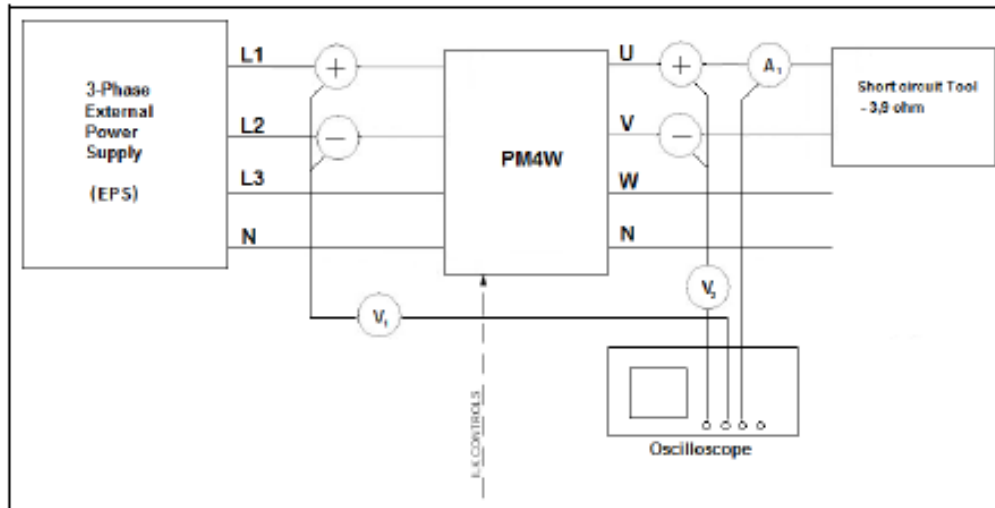


Figure 34– Setup IF_FUN_TEST-002

Test Plan

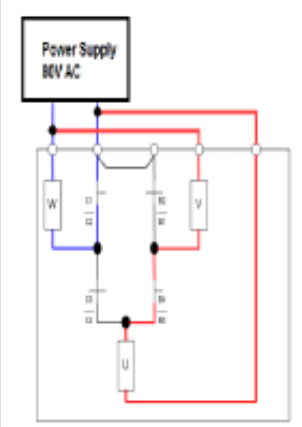
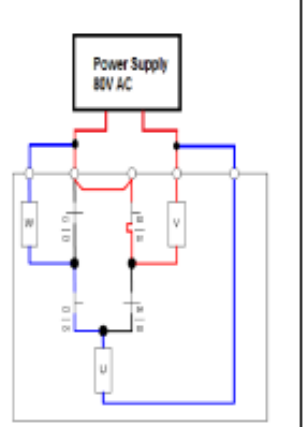
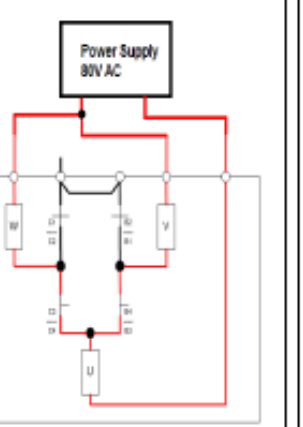
- Program the External Power Supply (EPS) with nominal voltage value for Power Supply used in Romania application (400 V_{AC} 3-phase 50 Hz).
- Measure the Output Voltage with Oscilloscope to ensure that programmed value is respected.
- Stand-by the EPS.
- Connect the EPS to the powering input of PM4W as indicated in the setup of Figure 34
- Connect the PM4W with Short Circuit Tool with 3.9Ω value as indicated in the setup of Figure 34
- Configure the PM4W system to operate with nominal value 400 V_{AC} 3-phase 50 Hz:
 - PS_VALUE = 400 (400 V_{AC});
 - PS_FREQUENCY = 50 (50 Hz);
 - MOVEMENT_MAX_DURATION = 10 (10s);
- Switch-on the EPS from stand-by.
- Execute the Motor Movement Command from PM4W system.
- Acquire and record:
 - the voltage applied V1;
 - the peak current A1;
 - the short circuit duration.

Repeat the previously test with the Short circuit tool on W and N phases and the current probe on W phase.

Note:

These tests are classified as destructive because change of fuse is required for each test.

Expected Results	<table><tr><th>Setup</th><th>A1_{pk}</th><th>Short Duration</th><th>V1</th></tr><tr><td>Load 3,9Ω</td><td>≤100A</td><td>T ≤ 20us</td><td>400V_{AC}</td></tr></table> <p>Each short circuit test leads to fuse replacement.</p>	Setup	A1 _{pk}	Short Duration	V1	Load 3,9Ω	≤100A	T ≤ 20us	400V _{AC}																
Setup	A1 _{pk}	Short Duration	V1																						
Load 3,9Ω	≤100A	T ≤ 20us	400V _{AC}																						
Obtained Results	<p>Check of configuration file used for the test campaign:</p> <ul style="list-style-type: none">• PS_VALUE set to 400• PS_FREQUENCY set to 50• MOVEMENT_MAX_DURATION set to 10 <p>Configuration file used for the tests is annexed to this IHA (see §12). PS_VALUE, PS_FREQUENCY and MOVEMENT_MAX_DURATION parameters for PM4W product are find in the .xml file part related to LRU_TYPE = "LRU_PM4W".</p> <p>The short circuit between U and V phases lead to have an intervention of PM4W when the current is above 50A.</p> <table><tr><th>Setup</th><th>A1_{pk}</th><th>Short Duration</th><th>V1</th></tr><tr><td>Short circuit on U and V phases</td><td></td><td></td><td></td></tr><tr><td>Load 3,9Ω</td><td>52.7A</td><td>15us</td><td>400V_{AC}</td></tr></table> <p>The short circuit between W and N phases lead to have the intervention of protection fuse before to log the test results.</p> <table><tr><th>Setup</th><th>A1_{pk}</th><th>Short Duration</th><th>V1</th></tr><tr><td>Short circuit on W and N phases</td><td></td><td></td><td></td></tr><tr><td>Load 3,9Ω</td><td>-</td><td>-</td><td>-</td></tr></table>	Setup	A1 _{pk}	Short Duration	V1	Short circuit on U and V phases				Load 3,9Ω	52.7A	15us	400V _{AC}	Setup	A1 _{pk}	Short Duration	V1	Short circuit on W and N phases				Load 3,9Ω	-	-	-
Setup	A1 _{pk}	Short Duration	V1																						
Short circuit on U and V phases																									
Load 3,9Ω	52.7A	15us	400V _{AC}																						
Setup	A1 _{pk}	Short Duration	V1																						
Short circuit on W and N phases																									
Load 3,9Ω	-	-	-																						
SW/HW Baseline	BL_PM4W_HW_2.3 BL_PM4W_SW_1.5																								
P/N S700K Point Machine	C25106-A141-A7-6 Point Machine S700K 5.5kN																								
Testing Date	01/04/2015																								

SAFE_TEST_01 - 80V Point Undue Activation Verification	
Test Objective	Demonstrate the safety compliance for no-activation of point motor when 80V _{AC} are applied by PPM circuit on the control wires.
Test Plan	<div style="display: flex; justify-content: space-around;">    </div> <p style="text-align: center;">Figure 37 – IF_SAF_TEST-001 setups for test</p> <p>Operation 1:</p> <ul style="list-style-type: none"> Program the AC Power Supply with nominal voltage value 80V_{AC} 50Hz. With point machine in NORMAL position, apply the 80V_{AC} voltage according to Setup 1 of Figure 37. Verify that the point motor is not activated and no point movement occurs. <p>Operation 2:</p> <ul style="list-style-type: none"> With point machine in REVERSE position, apply the 80V_{AC} voltage according to Setup 2 of Figure 37. Verify that the point motor is not activated and no point movement occurs. <p>Operation 3:</p> <ul style="list-style-type: none"> With point machine in STAR position, apply the 80V_{AC} voltage according to Setup 3 of Figure 37. Verify that the point motor is not activated and no point movement occurs.

Expected Results	<u>Undue Motor Activation Verification</u>		
	Operation	Setup	Point Motor Motion
	Operation 1	Setup 1	No motion
	Operation 2	Setup 2	No motion
Obtained Results	<u>Undue Motor Activation Verification</u> 80V _{AC} voltage single phase are provided to Siemens S700k 5.5kN point machine contacts. The table below summarizes the obtained results.		
	Operation	Setup	Point Motor Motion
	Operation 1	Setup 1	No motion applying 80V _{AC} single phase
	Operation 2	Setup 2	No motion applying 80V _{AC} single phase
SW/HW Baseline	BL_PM4W_HW_2.3 BL_PM4W_SW_1.5		
	P/N S700K Point Machine C25108-A141-A7-6 Point Machine S700K 5.5kN		
Testing Date	10/04/15		

Test Objective

Demonstrate the safety compliance for correct Machine Position Detection (NORMAL, STAR and REVERSE). The system shall be able to detect different point position and consequentially generate UNLOCKED state to send at Signalling Computer. Also stall current, when obstacle is placed between the point rails, shall be measured for electrical compliance completion.

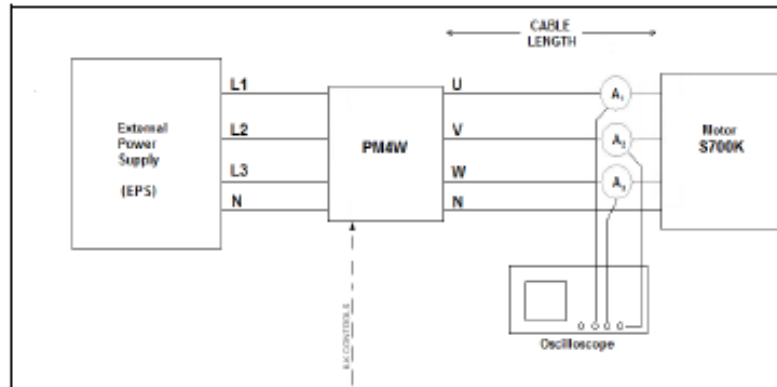
Test Plan

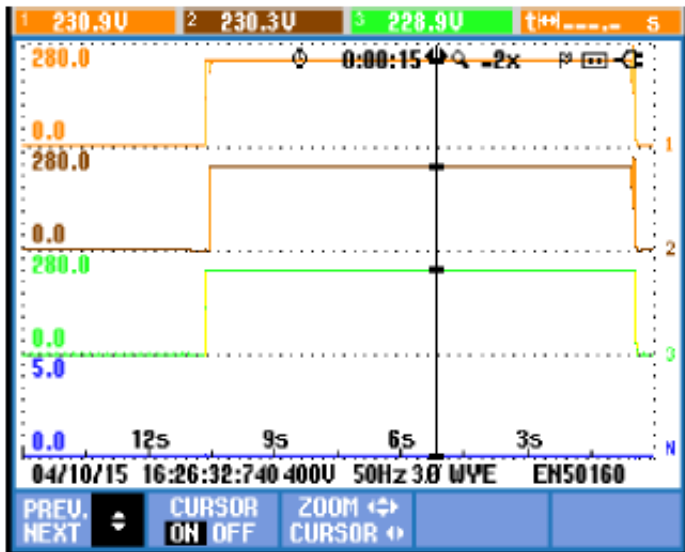
Figure 38 – Setup IF_SAF_TEST-002

Operation 1

- 1) Referring to setup of Figure 38, provide a point machine command from Normal to Reverse with 230Vac three phases voltage, at 50Hz (typical values).
- 2) Verify that, when point machine arrives to final position, the contacts are closed and the control signal is Locked Reverse.
- 3) Provide a point machine command from Reverse to Normal with 230Vac three phases voltage, at 50Hz (typical values).
- 4) Verify that, when point machine arrives to final position, the contacts are closed and the control signal is Locked Normal.

Operation 2

- 1) Provide an obstacle between the point rails
- 2) Referring to setups of Figure 38, start the point machine movement Normal to Reverse.
- 3) When the point machine movement is stopped by obstacle, check that point status is STAR.
- 4) Measure the stall current absorbed by point machine motor.
- 5) Detach aphase cable and check that point machine status is UNLOCKED.

Expected Results	<u>Current Measurements (during Operation 2)</u>					
	<table><tr><th>A1_{STALL} @ 10s</th><th>A2_{STALL} @ 10s</th><th>A3_{STALL} @ 10s</th></tr><tr><td><17A</td><td><17A</td><td><17A</td></tr></table> <p>During Operation 2 the expected IXL acquisition shall be UNLOCKED.</p>	A1 _{STALL} @ 10s	A2 _{STALL} @ 10s	A3 _{STALL} @ 10s	<17A	<17A
A1 _{STALL} @ 10s	A2 _{STALL} @ 10s	A3 _{STALL} @ 10s				
<17A	<17A	<17A				
Obtained Results	<u>Visual inspection during Operation 1</u> Two point machine commands have been applied: Normal to Reverse and Reverse to Normal. The control signals are reported in correct manner: Locked Reverse and Locked Normal.					
	<u>Current Measurements (during Operation 2)</u> The obtained results are: <table><tr><th>A1_{STALL} @ 10s</th><th>A2_{STALL} @ 10s</th><th>A3_{STALL} @ 10s</th></tr><tr><td>2.8A</td><td>2.6A</td><td>2.7A</td></tr></table> <p>A three phase 230/400Vac command has been applied to the point machine as contained in the following figure:</p>  <p>Figure 39 – IF_SAF_TEST-002: Three phases voltage applied RMS values</p> <p>When point machine rails has reached the obstacle, the point position detected is STAR and the stall current measurements on the three phases have been done and the results are shown in the following figure:</p>	A1 _{STALL} @ 10s	A2 _{STALL} @ 10s	A3 _{STALL} @ 10s	2.8A	2.6A
A1 _{STALL} @ 10s	A2 _{STALL} @ 10s	A3 _{STALL} @ 10s				
2.8A	2.6A	2.7A				

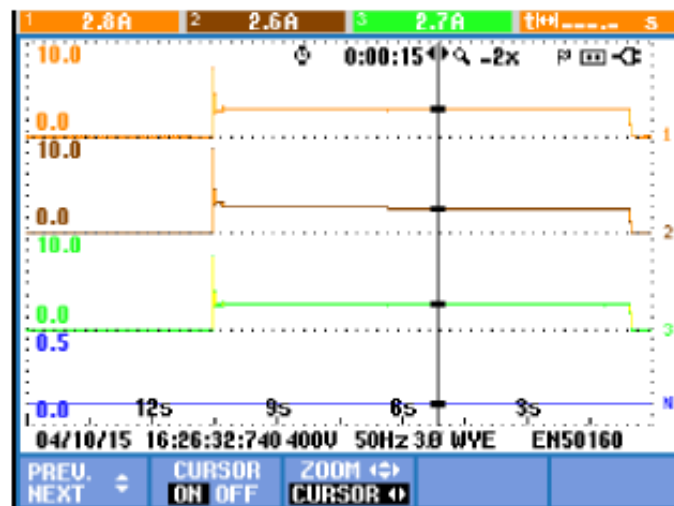


Figure 40 – IF_SAF_TEST-002: Stall currents

After phase detach, the point position is UNLOCKED characterized by all "SC Point State" bits set to 0 and "LIFE" bit set to 1.

SW/HW Baseline	BL_PM4W_HW_2.3 BL_PM4W_SW_1.5
P/N S700K Point Machine	C25106-A141-A7-6 Point Machine S700K 5.5kN
Testing Date	10/04/15