IRSE
Institution of Railway Signal Engineers

INTERNATIONAL TECHNICAL COMMITTEE REPORT No. 6

PROPOSED CROSS ACCEPTANCE PROCESSES FOR RAILWAY SIGNALLING SYSTEMS AND EQUIPMENT

APRIL 2003

INSTITUTION OF RAILWAY SIGNAL ENGINEERS

INTERNATIONAL TECHNICAL COMMITTEE

6TH REPORT

PROPOSED CROSS ACCEPTANCE PROCESSES FOR RAILWAY SIGNALLING SYSTEMS AND EQUIPMENT

Table of content

1 Introduction 5
2 Executive Summary 7
3 System Acceptance Today 8
3.1 Inventory 8
3.2 Process comparison 9
3.3 Analysis 9
3.4 Background knowledge 9
4 Other Industries – System Acceptance and Cross Acceptance 10
4.1 Civil Aviation Authority (CAA) 10
4.2 Maritime & Coastguards Agency (MCA) 12
4.2.1 General 12
4.2.2 Certification / Approvals 12
4.2.3 MCA / Classification Societies Relationship 12
4.3 Lloyds Register of shipping 14
4.3.1 General 14
4.3.2 The Process 14
4.4 Telecommunications – International Standardisation and Cross Acceptance 16
5 Experience Gained 17
5.1 What we can learn from the past that can help us into the new situation 17
5.2 The ERTMS experience 18
5.3 Lessons to be learned from the ERTMS experience 18
5.4 Other Signalling Developments 19
5.4.1 Separation of Subsystem Parts built to Different Safety Integrity Levels (SIL) 19
5.4.2 Train Protection / Train Control and Automatic Train Operation 20
5.4.3 Interlocking 20
5.5 The GSM-R Experience 21
6 Cross Acceptance 22
6.1 Definitions for Cross Acceptance 22
6.2 Roles and responsibilities in the Acceptance Process 22
6.3 A process for cross acceptance 23
6.4 Conditions for cross acceptance 24
6.4.1 Operating environment 24

6.4.2 Physical constraints 24
6.4.3 Traffic 24
6.4.4 Culture 24
6.4.5 Rules 24
6.4.6 Neighbours 25
6.5 Requirements for Cross Acceptance 25
6.6 Confidence in the authority 26
6.7 Guidance for Cross Acceptance 26
6.8 Factors complicating cross acceptance 26
6.9 Examples of successful cross acceptance 27
7 Design for acceptance 28
7.1 Costs and efforts in the acceptance process 28
7.1.1 Railways 28
7.1.2 Supply Industry 29
7.1.3 Safety Authorities 29
7.2 Criteria for an efficient acceptance process 30
7.2.1 Process clarification and definition 30
7.2.2 Generic Application specification 30
7.2.3 Cross acceptance 31
7.3 Supply Industry approach 32
7.3.1 Development following EN 50126 32
7.3.2 Safety case documentation 32
7.3.3 The industry's modular safety case approach 33
8 Legal Issues 35
8.1 Introduction 35
8.1.1 Responsibility of the State 35
8.1.2 Safety Targets for Acceptance 35
8.1.3 Consequences of an Accident 35
8.1.4 Incidents, Mishaps 35
8.2 European Legal Aspects in the Field of Railways 36
8.2.1 Historical Background 36
8.2.2 European Directive 91/440/EC 36
8.2.3 European Directives 96/48/EC and 2001/16/EC 36

8.2.4 European Standards / Norms 36
8.2.5 European Directive 85/374 37
8.3 Definition of Rules 37
8.3.1 Legal provision 38
8.3.2 Other rules 38
9 Integrating new equipment into the railway environment 40
9.1 Interfaces with existing equipment 40
9.2 EMC with existing equipment 41
9.3 System maintenance arrangements: 41
9.4 Operating Rules 41
9.5 Training of operators 41
9.6 Migration 42
9.7 Culture and division of responsibilities 42
10 Conclusions 43
11 Recommendations 44
12 Glossary 45
12.1 Glossary of Terms 45
12.2 Glossary of Abbreviations and Acronyms 49
13 Annexes 52
13.1 Examples of Acceptance Procedures 52
13.2 Examples of Cross Acceptance 53

Figures

Figure 3-1: Matrix on Process Comparison on Mainlines 8
Figure 4-1 The Civil Aviation Authority Model 11
Figure 4-2 P&O, North Sea Ferries and Stena Line 13
Figure 4-3 Lloyds Register of shipping 15
Figure 6-1 Process for Cross Acceptance 23
Figure 7-1 Typical Modular Safety Case Approach 34
Figure 8-1: Typical Systematic architecture of rules 38

1 Introduction

If you are a designer, procurer or approver of signalling systems this report will be of interest to you. It will help you understand the validation, assessment and approval process from an international viewpoint. The intention of this report also is to highlight the process, advantages and constraints for cross acceptance.

This report will address the following main issues:

- Unified processes in safety cases and certification
- Safety Authorities, Notified Bodies and cross acceptance
- Adapting to technical innovation and rates of change
- Platforms, need of platforms and architectures

The IRSE International Technical Committee produced their first report more than ten years ago. In this first report the fundamentals of safety appreciation procedures as a basis for cross acceptance were addressed. In the meantime CENELEC has produced a number of European norms for safety applications within the railway industry and some CENELEC safety standards for railway signalling are now circulated and partly in force for IEC standards in the context of globalisation.

Further experience shows that the processes for the approval of safety cases and the associated certification of applicable equipment are still not unified within Europe and thus cross acceptance is still not common practice. However, the supply industry has modified their development process to suit the requisites specified by the relevant norms, such as EN 50126 (IEC 62278), EN 50128 (IEC62279), and EN 50129.

Within some countries cross acceptance is already practised, even before the introduction of EN 50126, EN 50128, and EN 50129, whereas elsewhere the introduction of a system already approved in another country requires an almost completely new approach to the safety case. Another issue seems to be with the documentation, which ranges from the extremes of requiring as much as possible to, as little as practicable. This has much to do with the ability of the engineers involved during the development life cycle to determine the reasonable width and depth of documentation, since the norms cannot be used as a manual to determine the volume.

The IRSE wishes to encourage a culture of new signalling technology application which can be recognised internationally by manufacturers, safety authorities, consultants and railway operators, and to develop processes whereby usage in national railway organisations is made much easier in order to achieve rapid deployment.

This Report has examined current processes in various countries to establish both the strengths and weaknesses that exist, and to then set down a best practice 'code of conduct' by which countries should be encouraged to operate in the future. In some sections of this report references have been made to Interoperability and TSI. This is intended to demonstrate how important and useful cross acceptance is going to be rather than addressing the interoperability issues.

The report should be a practical help, giving the reader an insight into what is required and the pitfalls that can be encountered. It is intended to be used by safety authorities, operators and suppliers and seeks to achieve common ground. It should also be seen as a guide and to provide a way forward for the design and installation of new signalling systems within a realistic approval process.

Members of IRSE ITC

Wim	Coenraad	Holland Railconsult	Netherlands
Biagio	Costa	RFI SpA	Italy
Adrian	Exer	Siemens Schweiz AG	Switzerland
Istvan	Gal	MAV	Hungary
Eddie	Goddard	London Underground Ltd	UK
Gunnar	Hagelin	Bombardier	Sweden
Yuji	Hirao	Railway Technical Research Institute	Japan
Shigeto	Hiraguri	Railway Technical Research Institute	Japan
Clive	Kessell	Centuria Comrail Ltd	UK
Joerg	Kiefer	Siemens Schweiz AG	Switzerland
Lassi	Matikainen	VR Track Ltd	Finland
Fernando	Montes	Dimetronic, S. A. (Invensys Rail)	Spain
Heinz	Pfleger	ÖBB (since retired)	Austria
Jacques	Poré	Alstom Transport	France
Christian	Sevestre	SNCF	France
Peter	Stanley	Ingenica Consultants Ltd	UK
Klaas	Stolte	Alstom Transport	Netherlands
Joachim	Stutzbach	Siemens AG, Transport Systems	Germany
Karl-Heinz	Suwe	Signal & Draht	Germany
Helmut	Uebel	Alcatel SEL AG	Germany
August	Zierl	ÖBB (replaced Mr Pfleger)	Austria

Corresponding members of IRSE ITC

Urs	Dolder	SBB	Switzerland
Florian	Kollmannsberger	DB AG	Germany
Joe	Noffsinger	GE Transportation Systems	UK
Denny	Pascoe	Ansaldo Signal Ltd	USA

2 Executive Summary

Signalling is a prisoner of history in that operating rules evolved "without any synchronisation" within countries and signalling philosophy was designed to fit the operating rules. Whilst the higher order rules are essentially similar, the rules at application level are different between countries, and whilst some are similar, no two countries are exactly the same.

Signalling systems and equipment have traditionally been designed and supplied for the home market. Export opportunities were largely limited to those nations that had overseas colonies or strong overseas influence, where sales were easy to achieve. Smaller but similar opportunities existed for countries which shared a common language.

Since signalling systems were essentially part of the infrastructure, the opportunities for through train services between neighbouring countries were not unduly restricted by the dissimilarity of signalling systems.

With most countries having their railway system, along with other essential service industries, under state control, the price pressure to reduce the cost of new signalling systems was not as intense ten years ago as it is now. Signalling supply companies enjoyed a comfortable market and could make reasonable margins.

This 'cosy' state of affairs has had to change for seven main reasons:

- The growth of the high-speed train networks, particularly in Europe, offering seamless travel across borders.
- The higher speeds of trains have forced the need for in cab signalling systems.
- The privatisation of railways and the consequential demand for 'better value for money' has triggered a need to contain and reduce the cost of signalling systems.
- The globalisation of the signalling industry because home markets were no longer able to sustain a profitable business.
- The encouragement by the EU to develop a standard signalling system for the future.
- The divergence of ownership in some countries of infrastructure from train operations and the granting of usage rights to other train operators as a means of stimulating competition.
- The emergence of the 'safety case culture', which has driven up the cost of system acceptance procedures.

Further to this the Railway industry as such is loosing market share to competitors such as lorries and airlines and there is a need for the Railway industry to find ways of lowering costs for design, development and operation of signalling systems as well as all other systems.

The increased complexity of systems puts a strain on the development resources of the supply industry. Innovation cycles in technology are getting shorter and shorter. The resources required by the safety case, assessment and acceptance processes are immense. There is a real risk that technology is obsolete by the time it reaches the market and suppliers will not be able to afford to stay in this business.

This report shows how the principles of cross acceptance can be used to contain the cost of system acceptance by avoiding unnecessary and unproductive repetition of effort.

The IRSE believes that this report identifies principles and processes for cross acceptance of signalling products that should be adopted by railways and safety authorities. As an international cross-industry professional organisation with membership from the supply industry, railway and infrastructure operators and consultants, the IRSE is uniquely placed to unite the industry in the development and promotion of formal codes of practice for cross acceptance.

3 System Acceptance Today

3.1 Inventory

An inventory was made of system acceptance procedures today. Presentations of procedures in Austria, Switzerland, The Netherlands, Germany, Great Britain, France, Finland, Hungary, Italy, Japan, Spain and USA were received and analysed. The processes for these and other countries are summarised in Figure 3-1, and all presentations are available in Annex 13.1.

	Safety Authority	Design Authority	(Generic) Safety Case prepared by	Independent Safety Assessor	Safety Case accepted by	Safety Case Standards for new Systems
Austria	Government	GP: Supplier GA: Railway	GP: Supplier GA: Supplier	Government & Specialists	Government	EN 50126 - 9
Belgium	Government	GP: Supplier GA: Railway	GP: Supplier GA: Supplier	Specialists	(Government)	EN 50126 – 9
Switzerland	(Government)	GP: Supplier GA: Railway	GP: Supplier GA: Sup/Railw	Specialists	(Government)	EN 50126 – 9
Germany	(Government)	GP: Supplier GA: Railway	GP: Supplier GA: Supplier	(Government) & Specialists	(Government)	EN 50126 – 9
Spain	Government	GP: Supplier GA: Railway	GP: Supplier GA: Sup/Railw	(Railway) & Specialists	Railway	EN 50126 – 9
France	Government	GP: Supplier GA: Railway	GP: Supplier GA: Sup/Railw.	Railway & Specialists	Government through Railw.	EN 50126 – 9
Finland	Infrastructure Manager	GP: Supplier GA: Infra-Man.	GP: Supplier GA: Supplier	Specialists	Infrastructure Manager	EN 50126 – 9
Hungary	(Government)	GP: Supplier GA: Railway	GP: Supplier GA: Supplier	Specialists	(Government)	KM-EMV 15/1987
Italy	Infrastructure Manager	GP: Supplier GA: Infra-Man	GP: Supplier GA: Sup/ Infra-Man.	Infra-Man. sup. by Specialists	Infrastructure Manager	EN 50126 – 9
Japan	Government	GP: Supplier GA: Railway	GP: Supplier GA: Sup/Railw	Specialists	Government / Railway	Safety Guidelines (IEC / EN 50126 – 9)
Netherlands	(Government)	GP: Supplier GA: Railway	GP: Supplier GA: Supplier	Specialists	(Government) through Railw.	EN 50126 – 9
Poland	(Government)	GP: Supplier GA: Railway	GP: Supplier GA: Supplier	Specialists	Government	EN 50126 – 9
Sweden	(Government)	GP: Supplier GA: Railway	GP: Supplier GA: Supplier	(Railway) & Specialists	(Government) through Railw.	EN 50126 – 9
United Kingdom	(Government)	GP: Supplier GA: Railway	GP: Supplier GA: Sup/Railw	Specialists	(Government)	EN 50126 – 9 & Yellow Book

Legend: (Government) = Organisation closely related to the ministry; GA = Generic Application; GP = Generic Product; Infra-Man = Infrastructure Manager; Railw = Railway; SUP = Supplier; sup = supported

Figure 3-1: Matrix on Process Comparison on Mainlines

3.2 Process comparison

The acceptance processes bear a remarkable resemblance. In almost all countries the safety authority is either located within the ministry of transport, or an independent organisation closely related to that ministry. The system and design authority for generic products is in all countries the supplier; for generic applications it is either the railway itself, or the infrastructure provider in those countries where that function has been separated from the operation of train services. The supplier prepares product related safety cases; in the case of generic applications it is usually the task of the supplier and sometimes of the railway or the infrastructure manager. In most cases independent safety assessors are employed to assess the safety cases. The responsibilities for acceptance of the safety case and system acceptance vary somewhat. Usually the ministry of transport or an independent organisation closely related to that ministry accepts the safety case; otherwise the infrastructure manager / railway accepts the safety case and seeks approval from or recommends to the safety authority that a system be accepted for use in service. In almost all European countries, the CENELEC standards EN 50126 - 50129 are used as a basis. It should be noted that the existing installed base or changes to the installed base do not generally meet the CENELEC standards. While most countries accept the possibility of cross acceptance of systems or parts of assessments, it is clear that this is very much left to the discretion of the railway or safety authority. The exception seems to be within the German speaking countries as they freely accept systems approved by EBA, which is being extended to a growing number of cases in the Netherlands and Finland.

3.3 Analysis

A first analysis would suggest that cross acceptance of platforms for safety systems, on the level of the Generic Product Safety Case including related software e.g. the operating system, pose the least problems. Design strategies and system architectures for the use of processor based systems in signalling applications are well established and there appears to be a consensus on their acceptability, which is reflected in EN 50128 and EN 50129.

Unfortunately this is very different at the application level. For historical reasons, rules and regulations and implementation details of seemingly similar functions vary widely across the various railways and this in turn necessitates different application designs for each country and/or railway. It is interesting to note that in countries that report cross acceptance of each other's systems freely, i.e. Germany, Austria and Switzerland, they have rather similar operating rules and practices!

3.4 Background knowledge

Cultural and legal obstacles, as well as financial consequences prevent railways from changing operating rules and procedures to those used in other countries.

A further problem of generic application cross acceptance is the fact that systems or products are never developed from scratch, and new railways are rarely built in a "Greenfield environment". Most system designs and system acceptances are based on implicit knowledge of operating rules and conditions, legal context etc. that are "pre-conditions" for the safety of those products and systems in the particular operational environment. This knowledge that is supposed to be part of the "cultural baggage" of the senior engineers involved in the process, is often hardly documented at all. However, foreign assessors and indeed all parties involved in a systems lifecycle, may not be aware of these implicit suppositions and conditions and discover the risks and constraints "the hard way". Taking into account the potential civil and criminal liabilities to the assessor or system authority, this explains why cross acceptance is limited in practice to evidence from parties that are known, respected and trusted.

4 Other Industries – System Acceptance and Cross Acceptance[1]

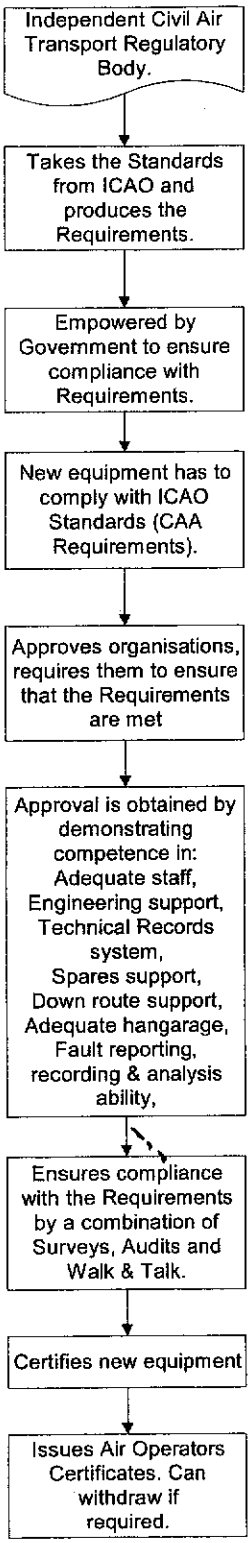
This section gives examples as to how other regulators function for the approval of aircraft, ships and telecommunications. The examples quoted are based on UK experience.

4.1 Civil Aviation Authority (CAA)

- Air transport is a relatively young industry. It is dynamic by nature and constantly striving to 'do things better'. It has the advantage of not having brought with it the 'kit and baggage' of historically questionable activities or organisations, e.g. the Classification Societies in the shipping industry.
- Despite its relative youth it is mature in the way it conducts itself and handles the relationships with peer groups and the Regulatory Body.
- The stance of the CAA is one of to encourage rather than to dictate, but it has powers of severe sanction and would use them if required. Perhaps just as importantly, the operators recognise this and work openly with the CAA rather than against them.
- Self-reporting is an important part of the system.
- Economics are seen as an integral part of ensuring that the operation is safe, a grounded aircraft (for whatever reason) is bad economics.
- As an independent organisation the CAA is able to discharge its obligations objectively and dispassionately.
- The formation of ICAO and the resulting harmonised Standards plus the respect in which the members are held has helped to produce a professional and mature industry.
- Ad-hoc surveys plus the visibility of walk and talk results in perceived involvement and commitment of the CAA. This complements the scheduled surveys and encourages a 'safe culture'.
- The combined CAA/AAIB model is one that could benefit other transport systems.

---

[1] The content of this section has been taken from other reports and reflect views of other authors than IRSE ITC. It should not be taken as an official position of IRSE.



Key Points.

An independent body.

Monitors by a mixture of;
Audits,
Surveys,
Walk and Talk.

Values Walk and Talk far more than Audits, people clear up for Audits so you don't get a true picture of what is actually happening. Aims at using some 60% of survey staff time on Walk and Talk!

Has teeth and is not afraid to use them by putting non-compliance notices on operators with rigid compliance timescales. Failure to comply could result in the aircraft having its Certificate Of Airworthiness removed i.e. it cannot fly.

Is independent from, but works with the AAIB to get the best remedial action from incident results.

Always Approves new aircraft before accepting on to the UK Register.

Encourages mature and professional discussions between manufacturers, operators and themselves.

Encourages a self reporting regime used by the operators to supplement their own Mandatory Occurrence Report system. (Usually discounts up to 30% of self reported occurrences.)

Is an integral part of the Joint Airworthiness Authority (JAA) which is the EU Regulatory Harmonisation body.

A founder member of the International Civil Aviation Organisation (ICAO).

Pro-active by nature in that they try to see problems looming and take corrective action rather than react to an incident.

Mature, requires 'grown up' talking rather than blame apportionment.

Figure 4-1 The Civil Aviation Authority Model

4.2 Maritime & Coastguards Agency (MCA)

4.2.1 General

The MCA is the official watchdog for all things maritime in the UK. The impression is of a benevolent rather than aggressively watchful regulator. It has strong ties with the International Maritime Organisation (IMO) and uses the IMO when there are differences of opinion with other shipping nations. In essence the IMO is a forum for getting basic rules agreed and for getting acceptance on international minima for safety at sea. As a matter of principle the UK and other similarly responsible maritime nations exceed the minima.

4.2.2 Certification / Approvals

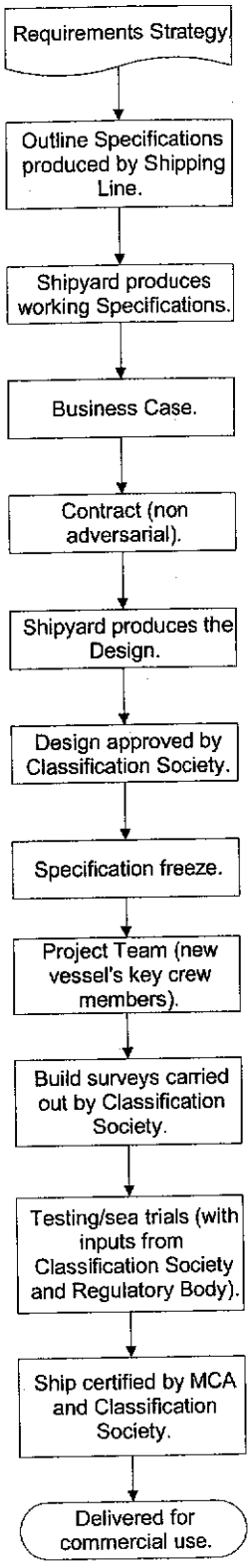
The issue of Certificates is normally divided this way:

- Classification Societies for International Tonnage, Load Line (Plimsoll Line), Oil Pollution, Passenger Ship Safety/Hull/Machinery/Control & Electrical and Safety Construction.
- MCA for Stability/Damage/Inclining Tests, International Safety, Document of Compliance, Safety Management, Fire Safety, Navigation and a variety of safeties related issues.

4.2.3 MCA / Classification Societies Relationship

- The MCA approves and licenses the Societies.
- The MCA audits the processes, control systems and quality systems of the Societies annually.
- The MCA uses the Societies extensively in terms of surveys of shipbuilding and routine maintenance/operations.
- There are 6 licensed Classification Societies in the UK.
- In general, for new or novel pieces of equipment, the MCA will authorise its initial use. Once it has become the norm the authority for the certification process for inclusion in a vessel is invested in the Classification Society.
- To become MCA licensed and approved, the Societies have to demonstrate adequacy in terms of:
    1. Worldwide network.
    2. Adequate numbers of suitably trained and experienced surveyors.
    3. An acceptable quality system.
    4. Independence from shipyards and shipping lines.
    5. An acceptable management organisation and control structure.
    6. Recruitment and training.
    7. Prominence within the maritime culture.

There is a listing available that defines precisely the division of responsibilities for certification.



Key Points.

Clear UK regulatory requirements, (some confusion with other countries and EU requirements).

Passive Regulatory Body, (Maritime and Coastguards Agency-MCA).

The MCA does not appear to be regarded as a watchdog with big teeth, or it does not give the impression of being prepared to use them during design and build.

The position of the Classification Societies could be questioned in that they could be seen as not truly independent. Also, there is nothing to stop the Shipping Line from going to another one if they don't like the answers they are getting, 'you can get an MOT anywhere!'

The internal Quality Audit process is not too aggressive. They tend to rely on the Classification Societies and the MCA to 'keep the Shipyards honest'.

The New Build Team (Project Team) is made up of key members of the new ships crew e.g. the Chief Engineer.

Certification is generally split such that the Classification Societies certify the structure and main equipment, the MCA certifies other, mainly safety related, equipment.

P&O management seem generally unimpressed by the Classification Societies and their relationship with the MCA. They feel that it results in a confusing regulatory situation. They much prefer the situation in the USA where the US Coastguards acts as the sole regulator.

Figure 4-2 P&O, North Sea Ferries and Stena Line

4.3 Lloyds Register of shipping

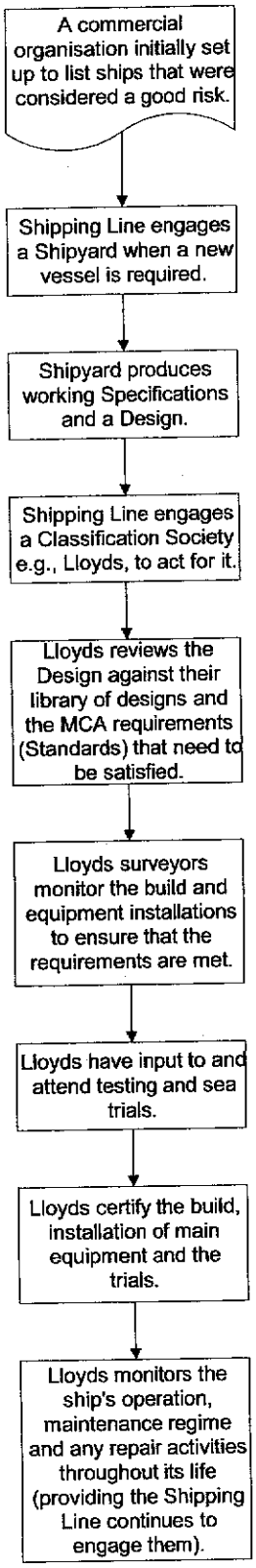
4.3.1 General

This started as a commercial organisation that was set up some 300 years ago as an agency that listed and rated ships for seaworthiness. This led to shipping lines using them as an acceptable reference for insurance purposes.

From this they have grown into an organisation that works closely with the shipyards, the shipping lines and the Maritime & Coastguards Agency in defining ship building Standards and ensuring that ships are built and maintained to the Standards. Lloyds Register is a Classification Society.

4.3.2 The Process

- A shipping line engages a shipyard to construct a new ship.
- The shipyard designs or uses an existing series as the new ship concept.
- The shipping line engages a Classification Society (Lloyds) to ensure that the design is sound and to monitor the build to ensure that the final product is correctly put together and certified.
- Lloyds review the original design against its design and standards library to make sure that the concept is acceptable and gives the go ahead to commence build.
- The Classification Society positions its surveyors at the shipyard. They follow the built process from start to finish and work with the MCA surveyors to ensure that the vessel is acceptable.
- Once the ship is commissioned and operating, Lloyd's surveyors are present during routine maintenance and off schedule checks or repairs (like following a collision for example) to ensure that the work is carried out in a way that satisfies the standards. If the surveyor considers that the work is unsatisfactory they can produce reports that could, if not actioned correctly, result in the withdrawal of the ship's certificate. This would result in the ship being unable to legally put to sea.



Key Points.

Lloyds, like all Classification societies, is licensed by the Regulatory Body, the Maritime and Coastguards Agency (MCA).

Lloyds states that it is a charitable organisation, but clearly it is commercially driven.

They enjoy a good (privileged?) relationship with the MCA.

They adopt a holistic approach (cradle to grave) towards the shipping industry.

Lloyds states that in their opinion safety and technical integrity are non negotiable.

They have been given approvals by the MCA that enable them to certify key activities within shipping.

It has been suggested that not all Classification Societies in the UK are as demanding as the more reputable ones, like Lloyds.

Figure 4-3 Lloyds Register of shipping

4.4 Telecommunications – International Standardisation and Cross Acceptance

The work of ensuring that International Telecommunications networks operate successfully across continental and country boundaries is carried out by the International Telecommunications Union – Telecomm Standardisation Unit, (the ITU-T). This body was created on 1 March 1993 and replaced the former International Telegraph and Telephone Consultative Committee (CCITT), the origins of which went back to 1865.

The ITU-T is complemented by the ITU-R to control standards in the radio communication sector, and by the ITU-D to ensure that development work is progressed with the aim of creating new standards for new products and services.

The ITU-T is organised into 14 Study Groups, which are populated by people from all sectors of the industry. The main thrust of the Groups is on common technical standards but also includes software languages, network management centres, tariffs and accounting principles, quality and service performance, and video.

More than 2,600 standards are written covering 60,000 pages. The standards are in the form of Recommendations, which are agreed by consensus and are non-binding. Compliance in practice has not been found to be a problem, since the standards are of a high quality and they ensure interconnectivity of networks across the world. Firms or providers who deviate from the standards effectively ostracise themselves from the international business. Having mandatory powers has thus not been found necessary.

The work of the ITU-T is directed by the World Telecommunication Standardisation Assembly (WTSA) that meets every four years to define general policy, the make up of the study groups and the work program. This is akin to The Council.

The WTSA is supported by the Telecommunication Standardisation Advisory Group (TSAG), which reviews priorities, programs, operations, finances, strategies, the progress of the study groups, organisation and working procedures. This is in effect the controlling Management Committee.

The study groups are given a work program of four years and produce the Recommendations, which are then debated and endorsed by the TSAG and WTSA.

The system works well and the population at large has enjoyed many benefits, since the past thirty years has seen the establishment of easy to use telephone and data networks on an international scale, with GSM providing a similar near world wide usage for mobile radio. Manufacturers think in terms of interoperable and cross acceptance technology, with the competitive edge being targeted at the service and pricing offerings.

5 Experience Gained

The evolution of European Union Directives is drastically changing market views and associated requirements. The liberalisation of railway activities is forcing the Railway industry to structure a different mode of operation, which in turn is demanding new supply requirements based on performance and cost.

The train operators, the railway infrastructure owners and the equipment suppliers are facing significant change in market conditions, which is demanding a scale factor improvement in the way that new train services are developed.

The concept of National Railways is loosing significance because of the new wider concept of a Trans-European Network. The issues that seem to be specific to a country become more and more common to all the European countries, and indeed, similar situations will happen in the rest of the world.

Research and development and project engineering teams supporting the big National Railways are disappearing.

The cross acceptance of railway products is becoming a reality and a necessity throughout countries for both the new Railway Companies as well as for the signalling industry.

Under this new reality, it is convenient to have a look back in time in order to analyse the practises relating to the acceptance of the signalling products between the different countries and to try and extract the most important factors that have contributed to the acceptance of these products and the conditions appertaining to them.

In the past, countries with a large technical capability have led the development of new products supporting not only their own Railways but also their Signalling industries. National standards were created that helped in the development processes, but they also contributed to the creation of significant barriers for product cross acceptance between countries.

Countries without their own signalling industry have adopted a more flexible approach to accepting and implementing technologies and products coming from other countries. A logical process of cross acceptance has evolved based on quality guarantees (including safety) and proven experience of the products. This process has often implied a period of trials in which the generic product has been adapted and in many cases improved to achieve the specific requirements of the country. These changes include environmental conditions and/or different application rules to achieve a validation in accordance with the specific application.

The harmonisation of signalling rules, which may include interlocking rules, is probably a necessary part of getting the same generic application of a product in different countries. The current situation of different rules for different countries means that the introduction of new technology is delayed. The considered view is that cross acceptance should lead to improved project time scales, this being the main benefit rather than lower cost.

5.1 What we can learn from the past that can help us into the new situation

From history it is apparent that as well as signalling systems, the approval processes are not interoperable. The reasons for this need to be questioned, as the evidence as presented by the ITC members would indicate that the approval processes in almost all countries are essentially similar. Most countries do, however, insist that independent approval of the design and functional performance be carried out before new systems are introduced into service.

The demand for faster project implementation and lower costs means that interoperable systems have to be developed which give better performance at a lower price and with technology common to several countries. This will be a significant factor in allowing the Railways to compete more effectively in the transport market.

Initiatives taken by the European Commission like the ERTMS system, or more recently the new UGTMS development project, clearly require procedures to be in place that enable a universal use of the same standardised product provided by the supply industry. These common products require a common Functional Specification accepted by the railways in all countries to cover not only from the technical aspects, but also to try and obtain harmonised operational procedures including Safety Regulations. The suite of CENELEC Standards, which should be used to develop the new products and systems, are seen as the foundation for all of this.

5.2 The ERTMS experience

This way forward is not easy as the experience with the ERTMS is showing.

The genesis of the problem was to try to solve the big issue of having 15 different incompatible Train Protection systems (ATP) in use. It was decided to specify and develop a new unified European Train Control System, which would eventually replace the existing national systems together with the necessary STM (Specific Transmission Modules) to provide a migration path from the current systems to the new.

In agreement between Railways (UIC) and Signalling Suppliers (UNIFE) it was decided to specify the ETCS system as a joint effort. The Railways would write the Functional Specifications (FRS) and the top level System Requirement Specifications (SRS), the suppliers were responsible for the technical specifications for developing the products. In the initial phase, the Railways set up the working group A 200 in order to write the FRS and SRS and subsequently the ERTMS Users Group has been formed to implement the initial projects. The specifications have been delivered to the supply industry as an output. The SRS was found to allow some different interpretations thus leading to the risk that systems designed by different suppliers would not become interoperable, although they were compliant to the specifications. The European Commission, therefore, decided that the best way forward was to give the task of rewriting the SRS to the suppliers. An agreement was reached with the Railways to proceed on this basis but with the proviso of allowing the Railways to review the result through a subgroup.

The European Commission sponsored the equipment for three national short test lines. The suppliers tendered for the lines and in 1998 the orders were placed. Presently, the winners of these contracts and other suppliers are developing the trackside and on-board subsystems of ERTMS/ETCS. Orders for other pilot lines and the first commercial applications followed.

The majority of the pilot lines and the first commercial lines will go into operation in 2003 and 2004. There will be tests of interoperability between trackside and on-board equipment on the test lines. There are procedures in place to introduce the expected changes and improvements in the specifications to ensure that the interoperability is robust (consolidation phase).

5.3 Lessons to be learned from the ERTMS experience

The whole process of co-operation to develop ERTMS has taken a long time, in fact over ten years. This process has needed to consider many other aspects over and above the technical development. These have included operating rules, political battles, international operations and the like. It has, however, to be recognised that the development of earlier train control systems for national application, e.g. LZB, TVM, SSI, also took a long period to implement. LZB as an example took 15 years from conception to production. It must be remembered that ERTMS has been designed as an interoperable system for application on the European High-Speed Network and as such the concept of cross acceptance is built in.

The main lessons learned to date have been:

- ERTMS was conceived as a technical development but it has evolved into much more than that.

- Agreeing the specification and requirements amongst many railways took time and proved very difficult to finalise, even though it was a green field development.
- The need to try and achieve common operating rules was not appreciated in the beginning. It is now seen as essential to unify the rules, especially where operational irregularities exist before the start of any future system development.
- A complex development needs a number of reiterations to achieve stable specifications.
- The safety targets are difficult to define. There is no European common understanding on tolerable hazard rates for such a system or the way to achieve the goal of defining them.
- A legal framework is necessary to enforce interoperability. An operator specific or even a site-specific solution can be made more cost effective than a unified approach, unless the Life-Cycle-Cost (LCC) approach is applied.
- Co-operation between suppliers is better than expected, keeping in mind that they all compete for the same market. It is a process that should be followed for other activities.
- The technical development time for the system has been longer than expected. Part of the reason is the normal optimism of R&D engineers; another factor is the inherent inefficiency and complexity in the managing of such a big group of companies working together.
- The market up to now is not yet as big as expected. It is very important to maintain the market expectations to justify the R&D expenditure of the suppliers.
- Maturity will take additional time. It is not possible to develop, test and re-engineer a system of such a complexity within five years.
- Further teamwork of the whole industry is necessary to achieve the technical and time-scale goals.

5.4 Other Signalling Developments

5.4.1 Separation of Subsystem Parts built to Different Safety Integrity Levels (SIL)

In complex systems, there is normally a mixture of functionality, which has to fulfil a variety of tasks. These can be classified into primary vital tasks on one side of the spectrum and secondary non-vital functions, such as statistical or maintenance requirements, on the other. These groups of tasks normally have different SIL allocations.

It is unavoidable that changes will have to be introduced into systems, and experience shows that changes due to new customer requirements or new technical possibilities are more frequent in the secondary functions, which means lower SIL ratings than in the primary functions. Also if the primary vital tasks have to be changed or enlarged, the separation makes sense.

If all the tasks are implemented within one device or even one software package, there is the need to prove the independence of areas that have been changed from those that have been unaltered, in order not to jeopardise the functionality of the existing design.

There have been many discussions within the Industry on this point and everybody seems to agree that it would be advantageous to separate high-SIL functions from low-SIL functions even at the physical level. The concept introduced by the standards related to Safety Electronic Programmable Systems of Protection and Control, works to provide a collaborative structure, supporting the highest level of safety with simplicity in the design.

The advantages of this have to be evaluated against possible disadvantages like:

- With a physical separation, more hardware is necessary than with a fully integrated system.
- Depending on the system and its complexity, there are additional logical and physical interfaces necessary.

There are two main areas where these ideas have been applied, which have been addressed in the following two sections.

5.4.2 Train Protection / Train Control and Automatic Train Operation

In areas where a high degree of automation is required in order to ensure consistency of operation and improve power saving, ride comfort and risk reduction, automatic operation of trains has been introduced. This is mainly applicable for suburban operation but is also relevant for high-speed operation. There has to be a primary safety function, which prevents trains from running too fast, exceeding the movement authority or going in the wrong direction, which is the Automatic Train Protection (ATP). In addition, there is an automation function, which takes over from the driver and controls the train movement (ATO).

In many applications, the ATP function (high SIL level) supervises the ATO function (low SIL level) and initiates a forced braking in cases where the ATO function has a wrong side failure. In such applications, the two functions are normally physically separated trackside and on-board and employ separate data transmission means.

Other solutions like LZB have chosen a more integrated solution, where an Automatic Train Control System (ATC) supervises the train movement and generates information for the Automatic Speed Control (ASC), normally a separate physical unit, which is then part of the ATO function.

Simplification in the design of the high SIL level vital function is a principle that could allow easier cross acceptance as the non vital function, with lower SIL requirements, will be provided with clear separation and functionality, thus reducing the effort needed to carry out modifications and/or acceptance.

5.4.3 Interlocking

In Interlocking systems, a set of essential core functional requirements can be defined, although the operational rules differ from one railway to another. These functions have not changed for decades and are considered to be very stable and correspond to SIL 4. Additional functional requirements arise if the performance of the interlocking has to be upgraded.

The design philosophy of some interlockings is to keep this core unchanged in terms of basic functionality and technology and adapt only peripheral parts to provide changed or new requirements with the latest technology. However, this solution is not possible in all cases.

The chosen technology must be capable of building the core functions in a safe platform. These functions are usually combined in a modular way, which makes it easy to configure for different applications.

All other less vital functions such as man-machine interfaces (although some part of an MMI may be considered a vital function if the information displayed is formally used to over-ride a signalling perturbation), remote control functions and diagnostic functions are implemented in off-the-shelf PC based equipment, where the technology is easy to handle and understand. This has the advantage of being able to be modified with little risk, and is commensurate with SIL 2. The advantage of this combination of technologies is that the basic safety analysis for the core interlocking does not have to be touched when the update of peripheral functions, caused either by new technological opportunities or updated functional requirements, are to be implemented. Acceptance processes may be made easier and quicker if alterations to the SIL 4 elements are minimised and lower SIL elements are maximised. This would be particularly useful when changes or updates are being introduced.

A design following the principles of separating different modules and events into different machines is seen as advantageous since the hardware cost is negligible compared to the software development. The large costs for validation of high integrity SIL systems is another lesson learned that could contribute to improve the cross acceptance between different Railway Companies.

5.5 The GSM-R Experience

GSM-R is a product that embraces Interoperability, Interchangeability and Cross Acceptance. Like ERTMS, GSM-R was borne with the vision of being used throughout Europe and probably elsewhere as well, as a common system to support a whole portfolio of requirements. These range from a full bearer system for ERTMS levels 2 and 3, to a replacement voice communication system for obsolete track to train radio networks, through to a platform for trackside warning systems, shunting radios, etc. The vision includes interconnection with the public GSM systems such that public telephones on trains can be linked into the GSM-R bearer before linking up to the outside world.

The design and supply intention was to have a multiple source of manufacturers, where the equipment would have an on air interoperability and where ground equipment could be mixed between different suppliers. So far, the supply chain looks like:

- Infrastructure – Siemens and Nortel
- Cab Mobiles – Kapsch, Siemens, Telit, Hoerman, Saab and Alstom
- Hand Portables – Sagem
- Note that Sagem also make the rf component for the Hoerman and Saab mobiles

Notified Body approval has been obtained for the basic GSM-R (R-Band GSM) rf component through the independent European GSM Test House (known as 7-Layers) in Dusseldorf. However, there has been no European type approval for the ASCI features where teething problems are still being encountered in both Germany and Sweden. Once these are resolved, it is anticipated that the type approval will be put to a test house and verified by a Notified Body. In the mean time, countries are following a process of self-certification with each railway being responsible for carrying out its own approval tests.

In practical terms, Siemens and Nortel control system and base station equipment is being trialled so that for example, a Siemens base station will work to a Nortel base station controller and vice versa. Some minor problems are arising in the interpretation of the GSM-R standard in terms of Group Call provision.

It is taken as read that any mobile/portable will work to a GSM-R infrastructure provider. This is fundamental to the interoperability requirements. Indeed, the mobiles will work to the public GSM networks providing a roaming agreement is in place.

Another aspect of cross acceptance is interchangeability. For locomotive mobiles, it would be good if the physical harness and the connections to power, aerial, train wiring etc could be standardised. This would enable:

- new trains being built at a factory to be pre-wired with confidence that whatever mobile is chosen, it will fit the space envelope
- when a radio is failed, it can be replaced with a spare from a different supplier.

However, there is no mandate at present for this and mobiles are currently being supplied as complete units with control head and radio rack from the same supplier.

Whilst therefore GSM-R is a model exercise in interoperability, there is still someway to go before interchangeability becomes a workable reality. As to cross acceptance, the evidence so far is that countries adopting the GSM-R technology are accepting the available products without excessive additional testing or verification. Any radio system must undergo extensive commissioning tests to check coverage, performance and any special functions. If GSM-R is a bearer for ETCS, then clearly the testing will be part of the overall signalling test plan. Overall, it would seem that purchase of the GSM-R product will be treated by the railways as an 'off the shelf' standard package, much akin to a commodity.

6 Cross Acceptance

6.1 Definitions for Cross Acceptance

At a high level, the concept of cross acceptance puts forward the scenario 'that if a technology/system operated safely and reliably in one country, then it should be able to do so in another country without the need for back to basics approval tests".

The determination as to what cross acceptance means has to be analysed and set down, then enshrined in some kind of universally accepted code of practice.

Cross acceptance is defined in EN 50129 as "The status achieved by a product that has been accepted by one Authority to the relevant European Standards and is acceptable to other Authorities without the necessity for further assessment".

For the purposes of this report, it is useful to point out that cross acceptance is also applicable if other than European standards were used and in fact this should be strongly encouraged. Furthermore cross acceptance can be applied to subsystems or parts of products as well. The issue of cross acceptance is not only technical. Cross acceptance is also a matter of political and commercial will, trust and engagement, strongly conditioned by the national regulatory framework.

This report deals specifically with "voluntary" cross acceptance, i.e. not regulated by the European directives 96/48/EC and/or 2001/16/EC.

Based on a definition by Railtrack PLC, cross acceptance is defined as:

"A process for accepting and approving equipment for use on a railway administration's infrastructure, based upon an acceptance already given for the same product by another railway administration or acceptance body together with an analysis of the safety issues arising from the application of the equipment in the "targeted" railway administration's environment".

6.2 Roles and responsibilities in the Acceptance Process

The following allocation of roles and responsibilities are put forward outside the regulations coming from the Directives 96/48/EC and 2001/16/EC (Cross acceptance inside this area is already regulated):

- Product certification is required for products (platforms, systems, subsystems, components) on a generic level.
- Product certificates aid in the process of cross acceptance, insofar as they present tangible evidence of prior independent and impartial evaluation of a products properties, adherence to standards, evidence of safety etc. and list the conditions and limitations under which the certificate is valid on a generic level.
- The supplier in the case of generic products (see EN 50129) produces the safety case.
- The supplier / infrastructure manager / railway, in the case of generic applications (see EN 50129) produce the safety case .
- An independent body (independent from the development, see EN 50129) assesses the conformity with all requirements (including safety case) and issues a certificate.
- The railway company or infrastructure manager accepts the product and its certificate.

The safety authority (see Figure 3-1: Matrix on Process Comparison on Mainlines) approves the safety case and / or other evidence of "fitness for use" and authorises the railway undertaking or infrastructure manager to start using the product in the "live railway".

6.3 A process for cross acceptance

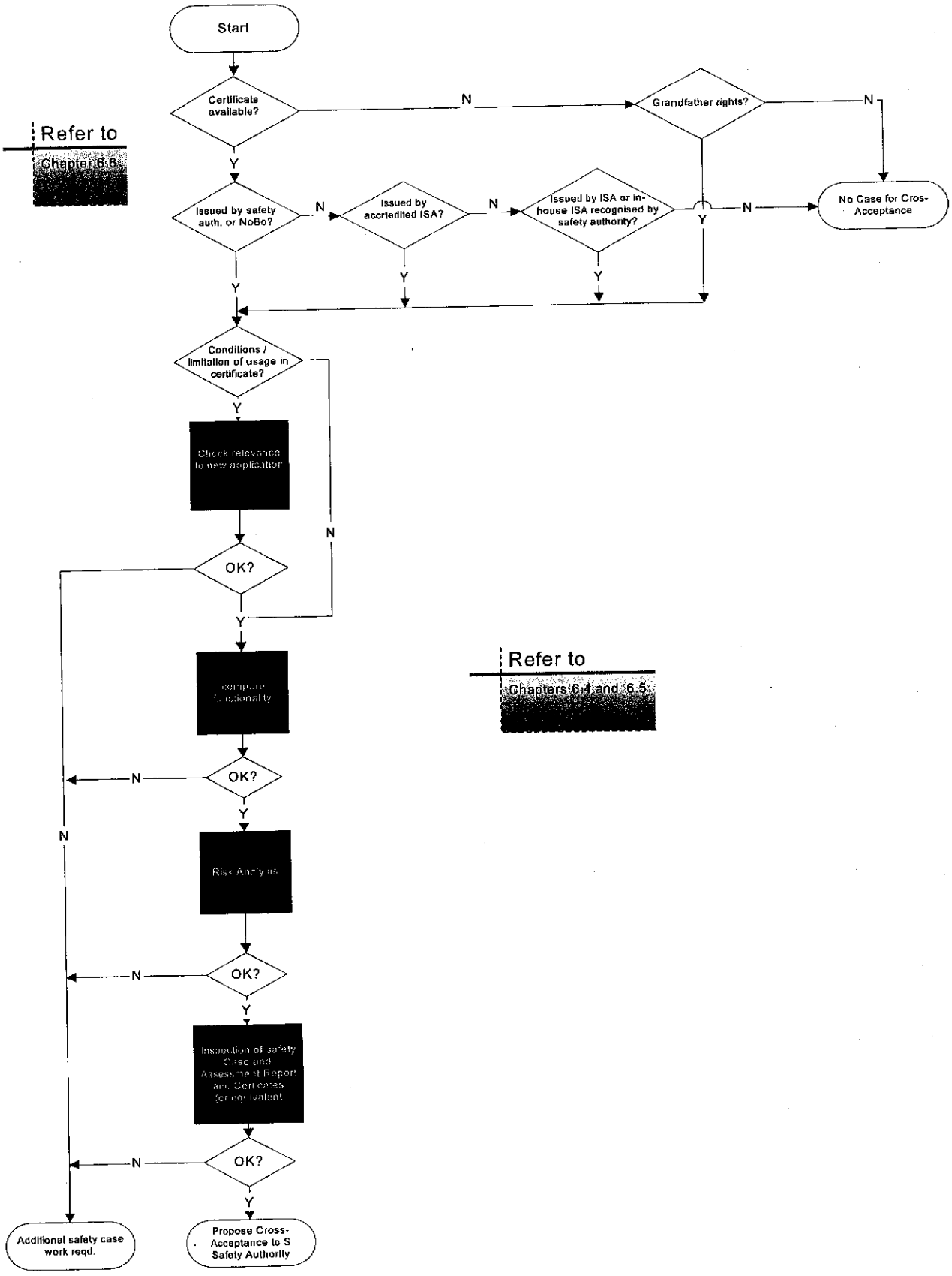


Figure 6-1 Process for Cross Acceptance

In general we will assume that a successful systems acceptance process will result in a certificate or an approved safety case for a product being issued. Cross acceptance of a previously issued certificate will in most cases be proposed by a supplier to a client. This client, in most cases a railway organisation or infrastructure manager, will in turn seek safety approval by the relevant safety authority. In order to achieve this a safety case will have to be presented in which the cross acceptance of the existing certificate (or approved safety case) is justified on a generic level. In simple terms, the new safety case will have to prove that all requirements are covered by the "cross-accepted safety case", that all assumptions, pre-conditions and ensuing application requirements can and have been met by the new "application" of the previously certified product and that the assessor is known and trusted.

It follows then that there is a requirement for certificates (approvals) to be very specific on the assumptions, pre-conditions and limitation of validity of each individual certificate for generic products and generic applications.

6.4 Conditions for cross acceptance

Any form of cross acceptance has to embrace the ultimate need of being able to ensure that the system being introduced is safe in itself and in its considered application.

For successful cross acceptance the following must be considered:

6.4.1 Operating environment

A system can only be considered safe when it fulfils the requirements of being fitted to the particular operations and physical constraints for which it will be used. Any safety case will have to address the elements listed below and demonstrate that any differences between the basic proof of safety and that required for the particular application is not compromised.

6.4.2 Physical constraints

Are the physical constraints the same? If not do they affect the safety case? (e.g. temperature range, access for maintenance, speeds, train frequency, radio coverage, effects on timing, mean time to repair, latent fault detection, etc.). The nature of the power supplies and the EMC environment must also be taken into account.

6.4.3 Traffic

The nature and density of the traffic will dictate the level of risk associated with failures of the equipment both in terms of the severity of an event and its probability. This in turn will set the acceptable level of wrong side failure rate. (An extreme example being the interlocking used on a single-track freight only railway versus a heavy metro. Both could use the same interlocking design but would have a very different generic application safety case).

6.4.4 Culture

The way that the system will be operated, the likelihood that rules will be adhered to, the level of training that can be expected of the operational and maintenance staff, etc. can affect the requirements for the system. The system must be designed to allow for the underlying approach that will be taken by the operators and maintainers and the assumptions built into the original design must be explicit.

6.4.5 Rules

It is unusual for a new rulebook to be introduced with a new system. The assumptions that are built into the old rules, both written and tacit, need to be taken into account. The rule set assumed in the original design, and any need to change the rules, must be made explicit.

6.4.6 Neighbours

Not only the target system must be considered but also the environment into which it will be introduced. This must cover such issues as physical and operational interfaces to neighbouring railways, modes of transport, emergency services, etc.

These points are further considered in chapter 9.

6.5 Requirements for Cross Acceptance

The requirements for cross acceptance can be summarised as

1. The system has been shown to meet the standard of safety prescribed.
2. The required safety standards are sufficient for the particular application.
3. The assumptions made in the original proof of safety are valid for the target system including operational and environmental factors.
4. All external factors that could invalidate the assumptions made have been considered.
5. The safety authority cross accepting a product on the basis of acceptance by a prior certificate must be confident of the independence and expertise of this third party.
6. The existing acceptance must be documented in such a way that the cross-accepting safety authority can be confident that no pre-conditions, assumptions or other factors exist that would impose undue restrictions on the implementation of the product.
7. All existing documentation, including the full safety case, the assessment report and the certificates (or approvals) issued, must be made available to the cross-accepting safety authority, as the latter will still remain accountable. Issues of Intellectual Property Rights can be settled by using Non-Disclosure Agreements.
8. If a safety case certificate is withdrawn or if problems with the product arise, the supplier should inform all customers and wherever possible, the safety authorities and assessors who may have based their acceptance of the product on this certificate.

In practical terms a product is eligible for cross acceptance if one or more of the following conditions are met:

- A safety case conforming to EN 50129 / EN 50128 exists and the product has been authorised for in-service use by a national safety authority.
- A safety case conforming to EN 50129 / EN 50128 exists and an Independent Safety Assessor[2] (ISA) has issued an assessment report that supports this claim. The ISA should be able to demonstrate impartiality in the technical assessment and be accredited by a national accreditation body (e.g. UKAS, DAR, Raad voor de Accreditatie) or an officially recognised safety authority[3], which would do periodic checking on the ISA[4].
- A safety case conforming to an older standard exists[5], the older standard being acceptable to the cross-accepting authority and the product has been authorised for in-service use by a national safety authority.

---

[2] The Independent Safety Assessor is not a protected title, hence, ISAs undertaking cross acceptance work are required to be formally accredited

[3] definition contained within EN 50129, version of May 2002, section 5.3.9

[4] The requirement for accreditation should solve the problem that Independent Safety Assessor is not a protected title.

[5] e.g. MÜ 8004