THE STANDARDISATION AND REGULATORY ENVIRONMENT RELATING TO THE USE OF PROGRAMMABLE ELECTRONIC SYSTEMS IN SAFETY RELATED APPLICATIONS

PART I - THE ENVIRONMENT

REPORT ON PHASE II STAGE I OF THE ROADMAP PROJECT

ON WORK CARRIED OUT FOR JRC ISPRA

UNDER CONTRACT NO. 14087 - 1998 - 06 F1ED ISP GB

BY

MEMBERS OF

THE EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS

TECHNICAL COMMITTEE No. 7

Reliability, Safety & Security

EWICS TC7

edited by

Ian C Smith

Campbell Love Associates

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS REPORT WAS PREPARED BY THE ORGANISATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED BY JRC ISPRA. NEITHER JRC ISPRA OR ANY MEMBER OF JRC ISPRA, THE ORGANISATION(S) NAMED BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM;

(A)MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS REPORT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B)ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF JRC ISPRA OR ANY JRC ISPRA REPRESENTATIVE, OR THE ORGANISATION(S) NAMED BELOW OR ANY REPRESENTATIVE OF THESE ORGANISATION(S) HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS REPORT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT.

CAMPBELL LOVE ASSOCIATES

EWICS TC7

Comments or questions to this report may be directed to

Udo Voges
Chairman EWICS TC 7
Forschungszentrum Karlsruhe
IAI
Postfach 3640
76021 Karlsruhe
GERMANY
udo.voges@iai.fzk.de

ABSTRACT

This report describes the work carried out during Stage I of Phase II of the ROADMAP Project. The ROADMAP Project is focussed on issues relating to the use of computer based systems in safety related applications. The aim of the Project is to create a guideline document which will assist users and suppliers and other interested parties in navigating through the different standardisation and regulatory environments that currently exist between countries and industrial sectors. While ideally such a guideline would exhaustively cover all relevant sectors in all countries worldwide, such coverage would require much greater resources than were available to the project team. In this part of the project a description of the standardisation and regulatory environments is presented for a total of 17 examples selected from 8 countries and 6 sectors. While the selection made was influenced by the expertise available from EWICS TC7 team members, the resulting mix of countries and sectors provides broad coverage of the area.

The study concludes that while there are many similarities in the regulatory and standardisation environments of the countries included in the report there are also differences. Arguably even more variation exists between sectors, both in the scope of the related standardisation activities and in the degree of regulatory control.

The report records the efforts being made, both within Europe and internationally, to harmonise the standardisation and regulatory environments worldwide but concludes that much still remains to be done. While differences continue to exist between countries and sectors there continues to be a need to provide guidance in this area in a document which is both current and regularly updated to reflect the latest information. This is particularly so in the field of computer based safety systems where technology is subject to rapid change.

This pilot study sponsored by JRC Ispra and carried out by members of EWICS TC7 is successfully demonstrating an approach to the development of such a document.

ACKNOWLEDGMENTS

The Project Team would like to acknowledge helpful discussions held with the following:

R. Tweehuysen	-	TNO Medical Technology Leiden
Chr. van Nimwegen	-	TNO Medical Technology Leiden
R.P. van Wijk van Brievingh	-	Delft University of Technology
Marja-Leena Jarvinen	-	Finnish Centre for Radiation and Nuclear Safety, Helsinki, Finland
Tadeusz Cichocki	-	Adtranz Zwus, Poland

CONTENTS

1. INTRODUCTION

1.1 Preamble

This document describes work carried out by members of EWICS TC7 (the European Workshop on Industrial Computer Systems - Technical Committee 7 Reliability, Safety & Security) under Contract No. 14087 - 1998 - 06 F1ED ISP GB from JRC Ispra. The work carried out was jointly funded by members affiliations and by the funding made available under the contract. The subject matter is "The Standardisation and Regulatory Environment relating to the use of Programmable Electronic Systems in Safety Related Applications". The work reported on was carried out within EWICS TC7 under the title of the EWICS TC7 Road Map Project. This work constitutes Stage I of Phase II of the Road Map Project. The work carried out in Phase I of the project was documented in a report entitled "The Collection and Categorisation of Worldwide Standards relevant to the use of Programmable Electronic Systems in Safety Related Applications" which was issued in July 1996[1].

EWICS TC7 produces guidelines, holds workshops and each Autumn runs a specialist conference - SAFECOMP. EWICS TC7 has been an active group since the mid 70's - there is no restriction to membership - all interested experts are welcome to attend. It meets four times per year. Its membership covers representatives from regulators, industrial users, researchers and members of standards committees.

At the EWICS TC7 meeting held at Brühl in January 1997, it was agreed in plenary session that a proposal should be submitted to JRC Ispra to carry out Phase II of the Road Map project as a standalone activity. It was agreed that the proposal would be submitted by Campbell Love Associates - CLA on behalf of EWICS TC7. The contract with JRC Ispra would be taken on by CLA on behalf of EWICS TC7 and Ian Smith of Campbell Love Associates would project manage the work.

1.2 Driving issues

[1] The Collection and Categorisation of Worldwide Standards relevant to the use of Programmable Electronic Systems in Safety Related Applications - Final Report to JRC Ispra on work carried out under Order EC 9505531 T - by members of EWICS TC7 edited by Meine van der Meulen SIMTECH and Ian C Smith Campbell Love Associates

There exists a large and increasing volume of standards related to the manufacture and use of programmable electronic systems for use in safety related applications. Published documents include national and international as well as sector specific standards. The work involved in searching through and interpreting the wide range of documents available to ensure appropriate compliance is costly and time-consuming. This results either in a high overhead which must be recovered in the price of the end product or to running the risk of the product being non-compliant.

There also exist differences in regulatory requirements both between sectors and countries. For example, the fact that a product is licensed for use within the process industry does not mean that it is automatically licensed for use in the nuclear, rail or aviation industries. Similarly a product licensed for use in one country will not automatically be licensed for use in the same sector in another country.

Internationally, there is pressure to reduce the barriers to trade and to create a more competitive environment through wider deregulation of industry. This makes the need to reduce the regulatory burden on industry more acute. The high barrier to entry, particularly for SME's (Small and Medium sized Enterprises), in markets subject to regulatory control greatly reduces the level of competition created by deregulation. The pressure to reduce the product cost base in a fiercely competitive market requires regulating authorities to collaborate with industry to minimise the costs involved in the regulatory process while still assuring the safety of the public and the environment.

While efforts are being made to harmonise the standardisation and regulatory environment both within Europe and internationally much has still to be done. There is a need to provide guidance in this area in a document which is both current and regularly updated to reflect the latest information. This is particularly so in the field of computer based safety systems where technology is subject to rapid change.

1.3 Strategies

Members of EWICS TC7 sponsored by JRC Ispra are addressing these issues in the Road Map Project. In Phase I of the project, members gathered details of relevant standards and guidance documents. These were then entered by JRC Ispra into a database accessible via the Internet. In light of the large number of documents that exist it is now necessary to provide some way of prioritising the importance of the individual documents. It is proposed that this would be best achieved by identifying those standards and guidelines recognised by relevant Regulatory, Certifying and Testing Organisations or relevant Recognised User Groups for each industrial sector in each country.

The task of achieving a full coverage of all known sectors and countries is beyond the scope of the resources available to the project and so in Phase II a limited set of sectors and countries have been selected to pilot the overall approach. In Stage I of Phase II of the ROADMAP Project, for each selected sector and country the relevant organisations have been identified and a description of the structure of the regulatory environment has been prepared.

This report describes the work carried out by EWICS TC7 members in Stage I of Phase II of the ROADMAP Project and is the final report deliverable under Article 3 of Contract No. 14087 - 1998 - 06 F1ED ISP GB.

In Stage II, the identified organisations will be asked to confirm the description prepared and to identify those standards and guidance documents that they:

1. Mandate or require compliance with.

2. Recommend or approve or endorse.

3. Consider relevant and informative.

2. BACKGROUND

For owners and operators of those systems, plants and processes where a failure can lead to a risk to people or the environment there has always been two potentially conflicting goals. The first goal is to operate the system, plant or process to achieve maximum possible economic performance and the second is to achieve the minimum risk to people and the environment that is practically achievable.

In some organisations the task of achieving each of these goals is deliberately separated. The task of maximising economic returns is given to the management team responsible for the safe and efficient operation of the system, plant or process, while the task of keeping the risk to people and the environment as low as reasonably practical is given to an independent safety department within the organisation, reporting directly to the highest level in the organisation. In this way any conflict between economic operation and safety concerns can be resolved at the appropriate level within the organisation.

For many sectors, there exists legislation governing the operation of potentially hazardous systems, plants or processes. For these sectors, regulatory bodies have been established with the responsibility of monitoring the systems, plants and processes within the sector to assure that the level of risk to people and the environment is kept within bounds stated in an agreed safety and environmental policy. Regulatory bodies have been given powers of enforcement which can include financial penalties for infringements, the criminal prosecution of responsible individuals and even the closure of offending systems, plants or processes.

Quite apart from any penalties imposed by regulatory bodies, the cost of a failure leading to the hazarding of people or the environment can, through litigation, have a severely negative financial impact on the offending organisation.

All the above creates pressures on the users and suppliers of programmable electronic systems for use in safety related applications systems to apply best practice and comply with regulatory requirements at minimum cost. This justifiable aim is made difficult because of the complexity of the existing standardisation and regulatory environment. Differing standards and regulatory requirements exist both between countries and between industrial

sectors. Two key multinational organisations have been active in identifying the problems and in promoting solutions.

In response to a request in 1995 from the ministers of member countries the Organisation for Economic Cooperation and Development (OECD) carried out a fact finding exercise and, in 1997, published a report[2] on regulatory reform. The report covers all aspects of regulatory activity across a wide range of sectors. Regulations which impede innovation or create unnecessary barriers to trade, investment, and economic efficiency; duplication between regulatory authorities and different layers of government, and even among governments of different countries; the influence of vested interests seeking protection from competition; and regulations that are outdated or poorly designed to achieve their intended policy goals were all identified as issues to be addressed.

The World Trade Organisation (WTO) has in place an Agreement on Technical Barriers to Trade (TBT). The TBT Agreement aims to ensure that member country's national regulations and standards do not create unnecessary obstacles to international trade. The Agreement urges, amongst many other points, the use of international standards where feasible.

As evidenced above, work on regulatory reform and on harmonisation of standards is an on-going exercise. Until such times as the aims and objectives of the above initiatives are fully realised there will continue to exist a very real obstacle to free competitive trade caused by differences in the regulatory and standardisation environment between countries and between different industrial sectors.

Members of EWICS TC7 and JRC Ispra have identified a need to aid users and suppliers with a current and regularly updated guideline to help in this regard.

---

[2] OECD Report on Regulatory Reform: Synthesis, 15-Sep-1997, ISBN 92-64-15556-2 and Volume I: Sectoral Studies and Volume II: Thematic Studies, 17-Oct-1997, ISBN 92-64-15519-8

3. SCOPE AND STRUCTURE OF THE REPORT

The aim of the ROADMAP Project is to create a guideline document which will assist users and suppliers and other interested parties in navigating through the different standardisation and regulatory environments that currently exist between countries and industrial sectors. Any attempt to provide an exhaustive coverage of all countries and all industrial sectors would clearly be beyond the resources available to the project. A selection was therefore made of a representative group of countries and industrial sectors to pilot the overall approach.

While the selection made was clearly strongly influenced by the expertise available from EWICS TC7 members, the resulting mix of countries and sectors provides broad coverage of the area. The countries selected were:

Austria	Netherlands
Finland	Poland
France	United Kingdom
Germany	United States of America

Within the selection is the country with the largest Gross National Product (GDP) worldwide, countries within the existing membership of the European Union (EU) having a range of levels of GDP and one country belonging to that group of countries which were formally part of the Eastern Communist Group of countries, scheduled to become a member of the EU.

The industrial sectors selected were:

Medical Devices	Nuclear Power Industry
Rail Transportation	Process Industries
Electric Power Industry	

The above selection includes the nuclear industry, arguably the most tightly regulated example, the rail transportation and process industries, both having a long-standing history of regulation, and the medical devices sector which is currently establishing its regulatory environment.

Another "sector" was included - security. This is, of course, more properly an attribute like safety which would apply across all industrial sectors. Indeed security is a topic area covered in the standardisation and regulatory environments for safety related systems which currently exist in all countries and sectors addressed in this report. However, many of the aspects of standardisation and regulation relating to security matters have historically been addressed by a distinctively separate community of experts. Topics such as cryptographic standards are being developed for sectors not involved in safety related systems but these standards such as those for digital signatures in e-commerce could be used for integrity measures in safety related systems. It was therefore considered appropriate to include those aspects of security in a separate section as a pseudo-sector.

Within the report, Section 1 - the Introduction - explains the imperatives which determined the need for this project. The driving issues are identified and a strategy is outlined for addressing them within the scope of the project.

Section 2 - Background - then further explains the concerns which exist relating to the complexity of the current standardisation and regulatory environments and some multinational initiatives already being pursued.

This section - Section 3 - describes the scope and structure of the report. The main section - Section 4 - provides a description of the standardisation and regulatory environment for each of the selected countries and sectors. For each country and sector information is provided on Background, Regulatory Bodies, Standardisation Bodies and Recognised User Groups. In addition a brief discussion is presented within each segment.

A general descriptive overview is given for the International and European standardisation and regulatory environments.

As mentioned above, Section 4 also contains a special segment on Security, covering particular aspects of this topic not currently dealt with in detail within the existing industrial sector environments.

Section 5 presents an overall discussion of the project findings. Section 6 gives the conclusions and recommendations that have arisen out of the work carried out under the contract.

4. THE STANDARDISATION AND REGULATORY ENVIRONMENT

4.1 General

There has been over recent years an increasing move to harmonise standards for hazardous areas around the world. Top level standards such as ISO 9000 are gaining increasing acceptance worldwide and the global nature of today's marketplace is bringing pressure to bear on all concerned with standardisation and regulation to define universal criteria applicable worldwide for approving products for use in hazardous areas.

4.1.1 International

The two key international standarisation bodies are ISO (the International Organisation for Standardisation) and IEC (the International Electrotechnical Committee).

ISO is a worldwide federation of national standardisation bodies from some 130 countries, one from each country. ISO is a non-governmental organisation established in 1947. The mission of ISO is to promote the development of standardisation and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. ISO's work results in international agreements which are published as International Standards.

IEC was established in 1906 for the purpose of standardisation in the electrotechnical field. Right from the beginning its activities were strongly directed at electrical safety. IEC's work also results in international agreements which are published as International Standards.

These international standardisation bodies are linked in with national standardisation bodies in each of the member countries. Many of the published International Standards appear as separate individual national standards with basically the same text but with a different nationally specific reference and title. Increasingly, however, top level international standards are being universally referred to by their original ISO or IEC reference. Organisations worldwide are seeking certification to ISO 9000, the

International Standard for defining criteria for setting up an acceptable quality management system in an organisation, rather than to individual national standards.

The ISO 9000 series of standards relating to the consistent achievement of acceptable quality in end products is a key top-level standard for the use of computers in safety related applications. Quality is defined as fitness for purpose. If the specification defines an attribute profile for the end product, then the quality management system ensures that the process used to create and test the product results in an end product with the specified attributes. The ISO 9000 series of standards defines the requirements for setting up an appropriate quality management system.

The ISO 14000 series of standards defines the requirements for setting up a corresponding environmental management system. This companion series of standards was formally published by ISO in September, 1996. Like ISO 9000, ISO 14000 provides organisations with the elements of an effective environmental management system, which can be integrated with other management systems to assist organisations to achieve environmental and economic goals.

The above two series of standards define a framework within which both legislative requirements and relevant public and plant specific issues can all be addressed. More specific guidance as to the nature of the process necessary to ensure that computer based systems for use in safety related applications meet the requirements specified is provided in IEC 61508. This standard is currently (1999) progressing through the final stages of international review prior to its formal publication as an international standard. In support of this base standard, sector specific standards will be developed, consistent with the overall requirements of IEC 61508 but interpreting and more specifically defining them in relation to the sector covered. The first of these, IEC 61511, is currently (1999) under development for the process industries.

Determining an acceptable level of risk to the public and the environment is a socio-political process. Setting bounding parameters to keep all human and automated activities within the defined level of risk and to ensure compliance is the task of the many regulatory bodies which exist worldwide. Top level agreements relating to environmental issues are the subject of international inter-governmental conferences (e.g. Kyoto 1997). The detailed implementation of strategies to achieve the agreed goals remains the responsibility of individual countries. Within the regulatory environment the setting of bounding parameters and the agreeing of an acceptable route to keeping within them is still largely a national issue. International collaboration through joint meetings between regulatory bodies provides a way of ensuring cross fertilisation of ideas and approaches. Moves to harmonise standards worldwide assist in achieving a corresponding coming together of the worldwide requirements for regulatory compliance.

4.1.2 European

Within Europe, the creation of the European Union and the associated single European market has provided a strong push towards achieving harmonisation across Europe within both the standardisation and regulatory environments. The existence of specific European Community Directives are creating a harmonised regulatory environment and route to compliance (EC Mark). Harmonisation of standards within Europe is being achieved through the creation of a European Standardisation body CEN and CENELEC relating more specifically to electrotechnical issues and so being the more directly relevant to the use of computers in safety related applications.

4.1.3 National

4.1.3.1 Austria

4.1.3.1.1 Background

Nowadays, Austria has only a few national-only standards (e.g. in the railway sector, or in the electrotechnical sector with respect to maintenance of technical equipment). Most standards are taken over (translated or even untranslated with a national cover page only) from international standards.

Responsibility for regulatory control however continues to be vested in internal departments of the Austrian Government.

4.1.3.1.2 Regulatory Bodies

The handling of regulations concerning safety related matters in Austria is shared between the following government departments:

- The Federal Ministry of Economic Affairs is responsible for standardisation in general and mechanical and construction safety. It is also the regulatory body for certification organisations, accreditation, test houses and rules and regulations in the area of electronics and electrotechnics

- The Federal Ministry of Labour, Health and Social Affairs is responsible for the safety of food and health systems. It is also responsible for social welfare, health and labour (including safety and security issues for working people)

- The Federal Ministry for Science and Transport is responsible for the safety of telecommunications and transportation (road transportation installations are also the responsibility of Ministry of Economic Affairs and the Ministry for Internal Affairs)

- The Federal Ministry for the Environment is responsible for environmental aspects

- The Office of the Chancellor (BKA) is responsible for data security

The ministries have departments responsible for these issues, but delegate detailed work on relevant aspects to (accredited or established) experts and organisations serving as their consultants.

4.1.3.1.3 Standardisation Bodies

The national standardisation body for Austria is the Österreichisches Normungsinstitut (ÖN). ÖN is a member of CEN and ISO and its tasks are related to those performed by ISO in general. The national standardisation bodies for Austria for Electrotechnical and especially safety-standards is the "Austrian Electrotechnical Association", der Österreichische Verband für Elektrotechnik (ÖVE), with the Österreichisches Elektrotechnisches Komitee (ÖEK), which is the corresponding national counterpart to IEC. ÖEK and ÖVE are members of CENELEC. Both organisations, ÖN and ÖVE, have some permanent staff, but detailed work on standards is done by volunteers from industry, research, universities etc., organised in working groups associated to committees and subcommittees of ISO, IEC, CEN or CENELEC. Both organisations have members paying member fees and are selling their products (standards, publications, workshops, sometimes conferences).

4.1.3.1.4 Discussion

As already mentioned, Austria has only a few national-only standards. Most standards are taken over from international standards. In the safety area, the ad hoc advisory group who proposed the standard on software safety and robustness in the early eighties, was an Austrian group of ÖVE (for IEC), which led to IEC 61508. In IEC TC56, new work items were just recently proposed by the Austrian corresponding working group. The same is valid for CEN/CENELEC e.g. preEN 50126, preEN 50128, preEN 50129, where Austrian groups have contributed considerably. Austrian research organisations are active in European projects related to dependability of computer control systems in general and in the railway sector (ACRuDA, ENCRESS, ISA-EUNET).

4.1.3.2 Finland

4.1.3.2.1 Background

The lack of standards in the field of programmable safety-related systems has been a handicap. Publishing of IEC 61508 will help very much. Its drafts have been used unofficially. They were also used to compile a guideline:

> Programmable safety-related control system assessment instruction, TTK - recommendation 1-1994, ISBN 952-9588-48-8, 102 p. (In Finnish).

This has been used in application assessments in the process industries by Inspecta Oy (formerly Technical Inspection Centre).

The nuclear sector has its own practice, see 4.4.3.1.

4.1.3.2.2 Regulatory Bodies

a) Governing Authorities

- Ministry of Trade and Industry, which sponsors

- Safety Technical Authority

- Ministry of Social Affairs and Health, which sponsors:

- Department of Protection of Labor

- Food and Drug Authority

- Finnish Centre for Radiation and Nuclear Safety

- Ministry of Transportation and Communications, which sponsors:

  - Civil Aviation Authority (CAA, Finland)

  - Finnish Rail Administration

  - VR Ltd., Finnish Railways

  - Finnish Maritime Administration

b) Inspection bodies

Many of the above authorities also do inspections.

Others are:

- Inspecta Oy (former Technical Inspection Centre)

- VTT State Research Centre, Automation

4.1.3.2.3 Standardisation Bodies

The national standardisation body for Finland is the Finnish Standards Association (SFS). SFS is a member of CEN and ISO. The national standardisation body for Finland for electrotechnical standards is Finnish Electrotechnical Standards Association (SESKO). SESKO is a member of CENELEC and IEC.

4.1.3.2.4 Discussion

The regulatory structure in Finland has a similar form to other countries. All regulation is handled nationally.

In the field of standardisation, particularly of computer-based systems used in safety related applications, Finland is looking to the national adoption of internationally agreed standards, like IEC 61508, as the route ahead.

4.1.3.3 France

4.1.3.3.1 Background

The constitution of the Fifth Republic was approved by public referendum on September 28, 1958. The responsibilities for safety regulation in many of the sectors are laid down in detailed statutes. In general the responsibility for ensuring public safety rests with the government ministers responsible for the individual sectors. Regulatory enforcement is generally the responsibility of identified government agencies.

4.1.3.3.2 Regulatory Bodies

Ministre de l'Economie, des Finances et de l'Industrie responsible for:

Nuclear safety - La Direction de la Sûreté des Installations Nucléaires (DSIN)

Ministre de l'Equipement, des Transports et du logement (Ministry of Capital Works, Transport and Housing) responsible for:

Civil aviation - La Direction Générale de l'Aviation (DGAC)

Rail and road transportation

Ministère du travail et des affaires sociales (Ministry of Work and Social Affairs) responsible for:

Health and safety at work

Ministre de l'aménagement du territoire et de l'environment responsible for:

The environment - La Direction de la Prévention des Pollutions et des Risques (DPPR)

The organisation responsible for the certification of industrial products and services in France is Le Comité Français d'Accréditation (COFRAC)

4.1.3.3.3 Standardisation Bodies

The national standardisation body for France is the Association Française de Normalisation (ANFOR). ANFOR is a member of CEN and ISO. The national standardisation body for France for electrotechnical standards the Union Technique de l'Electricité (UTE). UTE is a member of CENELEC and IEC.

4.1.3.3.4 Discussion

In France the way in which regulatory authority is organised makes the appropriate government minister more directly accountable. Approvals to safety submissions are given in the name of the minister i.e. there is less delegation of authority than in some other European countries.

4.1.3.4 Germany

4.1.3.4.1 Background

In contrast with many other countries, German licensing bodies are in many cases not on the federal level, but on the level of the individual states. It is normally the state that issues licenses for large entities; the federal task being restricted to supervision. Only exceptionally, namely if a state does not obey the law, can the federal authority exercise direct influence. This applies for large industrial installations, e.g. power plants. The responsibilities are in most states or cases with their ministries of the environment and on the federal level with the ministry of home affairs. Before any licenses are issued, usually an assessor is employed by the licensing authority, the respective ministry of the environment. This assessor is a TÜV in most cases. In some areas related research organisations also exist.

The structure described leads to the curious situation that certain installations are approved in some states and not in others.

In Germany, making standards and even more so making guidelines forms an important means of technology transfer. In the related committees views are exchanged and concepts are transferred. Committee members who are also responsible for preparing new industrial projects are informed on existing trends and are confronted with ideas and attitudes they may have not been aware of. Participation in standards development may also result in an advantage over competitors.

A particular example is the use of computer control in areas which traditionally used mechanical, electromechanical or hydraulic control. These industrial areas are not always enthusiastic about the new technology and are reluctant to accept the related regulations.

Currently (1999), a ruling by the German government requires the cost of developing new standards to be paid by industry. The government support for DIN, the national standardisation organisation has been reduced. New standardisation work can only be started if industry support is available.

4.1.3.4.2 Regulatory Bodies

The number of regulatory bodies is quite large; therefore only examples can be given here.

The basis for regulatory bodies is usually given by laws; e.g. regarding the nuclear area Deutsches Atomgesetz (German Atomic Law). In the nuclear area regulatory bodies are:

- The state governments as mentioned above
- The federal government as mentioned above
- RSK, Reaktorsicherheitskommission, advisory body for reactor safety on federal level
- SSK, Strahlenschutzkommission, advisory body on irradiation on federal level

Regarding rail transportation

- Eisenbahnbundesamt, federal railway office, see also 4.3.3.2

Regarding airplanes

- Luftfahrtbundesamt, federal aviation office

For medical equipment

- ECM - Zertifizierungsgesellschaft für Medizinprodukte in Europa mbH, certification company for medical devices see also 4.2.3.1

For Digital Signatures

- Telecommunication Authority
- BSI - Bundesamt für Sicherheit in der Informationstechnik, federal office for security in information technology
- Zertifizierungsstellen, trust centres

In many cases ministries delegate the tasks of assessment and of enforcing standards and guidelines to TÜVs (Technische ÜberwachungsVereine)

4.1.3.4.3 Standardisation Bodies

All standardisation bodies work on the federal level. According to common understanding of the related German laws the state of technology is defined by the existing standards and guidelines. In German court cases distinction between these two is negligible. Therefore standardisation bodies are listed and the guideline making bodies as well. Industry relies more on standards than on guidelines, because they are normally phrased out more clearly. In some cases guidelines are produced first and converted into standards second.

The standardisation bodies are quite numerous. Among those that are relevant in the computer area are:

- KTA, Kerntechnischer Ausschuß, in the nuclear area
- DKE, Deutsche Elektrotechnische Kommission, for industrial computer applications in general
- NAMUR (Normenausschuss Messen und Regeln), for the chemical industry in particular
- NI, Normenausschuß Informatik, for information processing in general
- GGS, Gütegemeinschaft Software, for software quality in general

Other standardisation bodies exist for the areas of mining, shipping, etc.

The national standardisation body for Germany is the Deutsches Institut für Normung (DIN). DIN is a member of CEN and ISO. The national standardisation body for Germany for Electrotechnical standards is Deutsche Elektrotechnische Kommission im DIN and VDE - German Electrotechnical Commission of DIN and VDE (DKE). DKE is a member of CENELEC.

In the computer area DKE is the mirror organisation to IEC and NI is the mirror organisation to ISO. The committees of CEN and CENELEC are in some cases connected to committees of NI and DKE respectively, in some cases, however, independent experts are sent.

It is impossible to name all existing bodies.

Some of these bodies publish their results as DIN standards; e.g. DKE and NI do so.

The guideline producing bodies are also quite numerous. Among those that are relevant in the computer area are:

- DGQ, Deutsche Gesellschaft für Qualität, German Association for Quality
- VDI, Verein Deutscher Ingenieure, Institute of German Engineers
- VDE, Verband der Elektrotechnik, Elektronik, Informationstechnik e.V., Institute of German Electro Technicians
- ITG, Informationstechnische Gesellschaft, Information Technical Association

- GMA, Gesellschaft Meß- und Automatisierungstechnik, Association for Automatic Control

Here as well it is impossible to name all existing bodies.

The progress of technology determines changes of the individual areas and can give rise to overlaps. In some cases of overlapping competence the individual bodies collaborate. It is quite common that standards are taken over from one area to another. An example is IEC 61508 that has been accepted by the nuclear area and which has in turn been based on IEC 880, which is a nuclear standard. Harmonisation is usually reached by common membership in committees. In other cases joint committees are formed.

Recently a result has been published by a joint committee of DGQ, ITG and VDI.

> DGQ-Band 17-01 Zuverlässigkeit komplexer Systeme aus Hardware und Software (Reliability of Complex Systems of Hardware and Software), Beuth Verlag, Berlin, 1998, ISBN 3-410-32889-0

Standards and guidelines are published by Beuth Verlag in most cases.

4.1.3.4.4 Discussion

As German industry is very export oriented, interest in international standards is very high. Usually national standards are withdrawn as soon as international ones come into existence.

In some cases the federal structure creates a problem. Dependent on which party is in power specific industries are liked or not. Such preferences may change with the results of state elections.

Both the federal structure and the large amount of rules that are possibly to be obeyed may be unpleasant to foreign investors.

4.1.3.5 The Netherlands

4.1.3.5.1 Background

The approach to external safety in the Netherlands[3] and to risk management has its roots in the Hinderwet (Nuisance Law) at the end of the 19th century, recently replaced by the Wet Milieubeheer (Environmental Management Law). Further regulations have increased safety in the various industrial sectors, mostly by limiting the probability of accidents.

Some major accidents made clear that the possible consequences of accidents have increased in severity in this century. Reacting to that, the Council of European Communities issued the Seveso-Directive in 1982[4], in order to reduce the possible consequences of accidents for certain industrial activities.

During the same time the Centrale Raad voor de Milieuhygiëne (The central council for environmental hygiene) advised on external safety. It concluded that the government has to cope with the increased consequences of accidents. This LPG-study[5] in 1984 underlined this statement. The government integrated the risk approach in their policy from that moment on.

An important milestone was the Indicatief Meerjarenprogramma Milieubeheer 1986-1990[6] (Indicative Environmental Programme). This programme makes the risk approach compulsory for all activities with dangerous substances in stationary installations. A further elaboration of this approach gives the Nota Omgaan met Risico's (OMR, Coping with Risks), appendix to the Nationaal Milieubeleidsplan (National Environmental Plan)[7], and further elaborated in the NMP+[8].

OMR both gives the approach to risk calculations, and limits on acceptable risk in terms of individual and group risks. In the Netherlands for the acceptable group risk, the frequency of an accident is inversely proportional to the square of the number of people killed in that accident. The limit on individual risk is 10^{-6}/year.

For the time being, risks of different sources are not summed up. Every installation will be separately assessed.

---

[3] This chapter is mainly based on: A. den Breejen, De risicobenadering in het externe veiligheidsbeleid: een berekende zaak, Bouwrecht, nr. 3, maart 1993.
[4] Directive 92/501/EEG (Pb EG 1982, L 230), changed by directive 87/216/EEG (Pb EG 1987, L 85) and 88/610/EEG (Pb EG 1988, L 336).
[5] Tweede Kamer, 1983-1984, 18233, nrs. 1-2.
[6] Tweede Kamer, 1985-1986, 19204, nrs. 1-2.
[7] Tweede Kamer, 1989-1990, 21137, nrs. 1-2.
[8] Tweede Kamer, 1989-1990, 21137, nrs. 20-21.

The risk approach is also applied to nuclear installations and the dispersion of chemical substances in the environment.

Recent accidents like the crash of the El Al Boeing again raised the awareness of the possible large consequences of accidents, and the Ministers involved stated they would intensify the research on external safety.

The risk approach has also found its way to transport of dangerous chemicals, on roads as well as on water. Also, it is used in the risk plan of the safety of the high speed train link to Paris.

4.1.3.5.2 Regulatory Bodies

The main responsible entity is the Ministry of VROM (Public Health, Country Planning, and Environment). Some responsibilities can be transferred to provincial and local administration.

Before getting permission to build an installation, companies must report on the level of risk and how they cope with these. When this is not satisfactory, they will not have permission for their activities. In special cases they might have permission for these activities withdrawn at some later date.

4.1.3.5.3 Standardisation Bodies

The national standardisation body for the Netherlands is Nederlands Normalisatie-Instituut (NNI). NNI is a member of CEN and ISO. The national standardisation body for the Netherlands for Electrotechnical standards is Nederlands Elektrotechnisch Comité (NEC). NEC is a member of CENELEC and IEC.

The approach to external safety is based on law, no standardisation bodies are involved.

4.1.3.5.4 Discussion

The risk approach already is commonly accepted and used in the Netherlands. It proves to be a good instrument for assessing and controlling risk. Its use spreads to other application domains, like public transport.

The limits on group risk are rather severe, especially when compared to other countries. In most other countries, the limit on the frequency of accidents is inversely proportional to the number of people killed, not with its square.

4.1.3.6 Poland

4.1.3.6.1 Background

The first standardisation works in Poland were initiated by electricians. The regulation committee appointed in 1899 by the first organisation of Polish electricians may be considered to be the first standardisation team on the territory of Poland, as the Polish state did not exist at that time. Progress in the electrification required some form of standardisation for dissemination of knowledge in the field of constructing and safe operation of electrical systems and equipment as well as assuring their interfacing.

Polski Komitet Normalizacyjny -PKN (Polish Standardisation Committee) was established in 1924 in the Ministry of Industry and Trade. In 1972 PKN was merged with the Glowny Komitet Miar (Central Committee of Measures) and as a result Polski Komitet Normalizacji i Miar (Polish Committee for Standardisation and Measures) was formed. In 1979 it was transformed into Polski Komitet Normalizacji Miar i Jakosci - PKNMiJ (Polish Committee for Standardisation, Measures and Quality). Parliamentary Act of April 3, 1993: O utworzeniu Glownego Urzedu Miar (On establishing Central Office of Weights and Measures) liquidated the PKNMiJ effective from January 1, 1994. The issues formerly in charge of the PKNMiJ have been taken over by Glowny Urzad Miar (Central Measures Office) and Polskie Centrum Badan i Certyfikacji — PCBC (Polish Centre for Testing and Certification).

4.1.3.6.2 Regulatory Bodies

According to the current legal status, the functions of regulatory bodies in Poland are performed by the Ministers supervising a given branch of state administration (ministry) who by way of ordinances lay down the regulations which should be complied with in construction and operation of systems and equipment assigned to a given branch. These regulations may be issued directly by the respective Minister or by the bodies supervising the construction and operation of systems and equipment, subordinated to a given Ministry. For instance, the Ministry of Transportation and Naval Economy supervises Glowny Inspektorat Kolejnictwa (Main Inspectorate of Railways) and the corresponding bodies in civil aviation. The Ministry of Health and Social Welfare supervises the medical equipment. Urzad Dozoru Technicznego - UDT (Technical Inspection Office) subordinate to the Ministry of Economy supervises systems and equipment which may be hazardous to human life or health or to the property and environment in the following areas:

- steam boilers,

- liquid or gas tanks,

- acetylene generators,

- limited range transportation equipment, such as overhead cranes, hoisting winch, equipment for vertical, horizontal or diagonal transfer of persons, such as cabin conveyors or escalators.

Similar systems and equipment to the above mentioned that are used in railways, naval and military area, are supervised by the following specialist technical inspection bodies:

- railway technical inspection bodies and marine navigation technical inspection bodies, subordinated to the Ministry of Transportation and Naval Economy,

- military technical inspection bodies, subordinated to the Ministry of National Defense.

After PKNMiJ was dissolved, on the basis of Parliamentary Act: O badaniach i certyfikacji (On Tests and Certification), issued on April 3, 1993, Polskie Centrum Badan i Certyfikacji — PCBC (Polish Centre for Testing and Certification) started to operate on January 1, 1994. The Centre is subordinate to the Prime Minister.

According to the Act setting out PCBC:

1. Domestic and foreign products which may become hazardous or are used to protect the human health and environment are subject to being registered for certification with safety mark reserved by the PCBC and should be labeled with that mark.

2. Services which may create hazards or which are rendered to save human life, health and environment are subject to obligatory certification to be provided with the quality certificate.

The list of products and services which are subject to the above mentioned obligation is set by the Director of PCBC in consultation with the appropriate State administration branches and other bodies which are charged with the issues of occupational safety as well as protection of human life, health, property and environment. This obligation does not apply to systems and equipment subordinate to the above mentioned UDT and specialist technical inspection bodies, civil aviation equipment, ships and other floating units together with their outfit, provided with valid Polski Rejestr Statkow (Polish Register of Ships) certificates as well as pharmaceuticals, medical materials and services.

The basis for assessment of the products and services by PCBC are Polskie Normy — PN (Polish Standards) implemented for obligatory use (cf. Chapter 4.1.3.5.3) and legal regulations (e.g. ordinances issued by respective ministers). PCBC performs its functions through accredited testing laboratories and certifying units.

4.1.3.6.3 Standardisation Bodies

In accordance with the Parliamentary Act of April 3, 1993: O normalizacji (On standardisation), the Polish national standardisation system consists of PKN, as a collective body subordinated to the Prime Minister, Biuro Komitetu (Bureau of the Committee) as an executive body of PKN and Normalizacyjnych Komisji Problemowych - NKP (Standardising Problem Commissions), appointed by PKN, conducting standardising works and responsible for the contents of standards. PKN is financed from the national budget and is the only organisation authorised to issue the PNs (Polish Standards). Apart from being charged with domestic standardisation activities, PKN represents national interests in the international and regional standardising organisations and participates in their works. In this sense PKN is a member of international standardisation organisations IEC and ISO with full rights and an affiliated member of European standardisation organisations CEN and CENELEC.

The above mentioned act liquidated Normy Branzowe - BN (Sectoral Standards). The only national standards are presently PNs which may be used voluntarily except for the following cases:

1. when the appropriate Minister, in consultation with PKN, orders obligatory use of given standards, in particular related to:
    - protection of human life, health and property, as well as occupational and use safety
    - environmental protection
    - products ordered by state bodies
2. if the use of given standards is specified in parliamentary acts.

It has been accepted as the principle that the national standards in Poland are to be based on international standards after translation into Polish and possible adaptation.

4.1.3.6.4 Discussion

Among 53 certifying units accredited with PCBC and 191 testing laboratories accredited with PCBC and belonging to state-owned and private companies, military institutions as well as industrial research institutes and universities (http://www.piap.waw.pl/pollab/lab-akr/lista.html) and also 411 testing laboratories concentrated in the Polish Testing Laboratories Club POLLAB (http://www.piap.waw.pl/pollab/lista/listy.html), there is not even a single unit or laboratory which has assessing and certifying software or programmable systems in its scope of duties. However, this situation may change in the near future.

4.1.3.7 The United Kingdom

4.1.3.7.1 Background

The basis of British Health and Safety Law is the Health and Safety at Work Act 1974. The Act established the Health and Safety Commission (HSC) and the Health and Safety Executive (HSE) and made them responsible for regulatory control.

Within the United Kingdom Government, the Department of the Environment, Transport and the Regions (DETR) formed in 1997 is responsible through Executive Agencies within the Department or through Non-Departmental Public Bodies (NDPB's) for regulatory activities relating to Health and Safety and the Environment. The Department also has 10 Government offices for the regions.

The following are NDPB's sponsored by the DETR:

Environment Agency (EA) - Environmental Protection

Civil Aviation Authority (CAA) - Air Transportation Sector

Health and Safety Commission (HSC) - Advisory Body

Health and Safety Executive (HSE) - Regulatory Body

4.1.3.7.2 Regulatory Bodies

Vehicle Certification Agency - Road Transportation sector

Health and Safety Executive (HSE)

- Mines Inspectorate - Mining sector
- Railway Inspectorate - Railway sector
- Nuclear Safety Directorate - Nuclear sector
- Offshore Safety Division - Process sector
- Explosives Inspectorate - Process sector
- Chemicals and Hazardous Installations Division - Process sector
- Civil Aviation Authority - Air transport sector

4.1.3.7.3 Standardisation Bodies

The national standardisation body for the United Kingdom is the British Standards Institution (BSI). BSI is a member of CEN and ISO. The national standardisation body for the United Kingdom for electrotechnical standards is the British Electrotechnical Committee of the BSI (BEC). BEC is a member of CENELEC and IEC.

Another relevant standardisation body is:

Institute of Electrical Engineers (IEE) - covering electrical, electronics, computer engineering and computer science.

4.1.3.7.4 Discussion

Over the years there has been a continuous movement towards bringing together all the regulatory bodies for the different sectors together under one government department. With the formation in 1997 of the Department for the Environment, Transport and the Regions this has largely been achieved.

On standardisation, the UK as a member of the European Union is actively involved in seeking to harmonise standards throughout the European single market. Over the years the UK has been heavily involved in international standardisation efforts and has adopted many resulting international standards as national standards.

4.1.3.8 The United States of America

4.1.3.8.1 Background

In the United States of America, the protection of the public health and safety, and the environment is delegated by congress to executive and administrative agencies. In 1934, congress enacted the Federal Register Act to establish an orderly system and procedure for creating and enacting regulations proposed by these executive and administrative agencies. The passing of the act led to the creation of the Office of the Federal Register, which publishes the Federal Register, where proposed rules and regulations are first published for public review. After due allowance for public comment the proposed rule or regulation becomes finalised at which point the rule or regulation becomes legally enforceable.

In 1937 the Code of Federal Regulations (CFR) was established. The CFR arranges all final rulings by subject. Each book of this multiple volume collection focuses on the regulations of one to three agencies or programmes. The Code of Federal Regulations is arranged by Title and Part number. To further identify a specific passage, citations often refer to Section and Paragraph.

4.1.3.8.2 Regulatory Bodies

Executive and Administrative Agencies responsible for safety are:

US Department of Transportation (DOT) which sponsors

- The Federal Railroad Administration (FRA) - rail sector
- The Federal Aviation Administration (FAA) - air transport sector

US Department of Labor (DOL) which sponsors

- The Occupational Safety and Health Agency (OSHA) - all sectors

US Department of Health & Human Services which sponsors

- The Food and Drug Administration (FDA) - food & drug & medical sectors
- The US Environmental Protection Agency (EPA) - all sectors

US Nuclear Regulatory Commission (NRC) which is an independent agency covering the nuclear sector

Title 10 of the US Code of Federal Regulations contains Nuclear Regulatory Commission regulations.

Title 14 of the US Code of Federal Regulations contains Federal Aviation Regulations (FARs).

Title 29 of the US Code of Federal Regulations contains OSHA Regulations.

4.1.3.8.3 Standardisation Bodies

The national standardisation body for the USA is the American National Standards Institute (ANSI). ANSI is a member of ISO.

Other relevant standardisation bodies are:

Institute of Electrical and Electronic Engineers (IEEE) - covering electrical, electronics and computer engineering and computer science. (IEEE standardisation groups have members from all over the world, so their standards have an international approach)

Instrumentation Society of America (ISA) - covering instrumentation and control.

The American Society of Mechanical Engineers (ASME)

The American Association of Motor Vehicle Administrators (AAMVA)

The American Society for Testing and Materials (ASTM)

4.1.3.8.4 Discussion

The USA has in place a well established legal framework for regulation. The Code of Federal Regulations sets down in considerable detail the legal requirements for regulatory compliance.

There are also a large number of well established standardisation bodies producing supporting standards and best practice guidelines. Generally these bodies have concentrated, in the past, on developing material targeted at the internal US market to meet the environmental and safety requirement within the USA. A number of the standards have been used and adopted by other countries. While the USA has had a continuous involvement in the making of international standards, in recent times, in recognition of the growing global nature of the marketplace, the USA has become much more active in this field.

4.2 Medical

4.2.1 International

4.2.1.1 Background

The international scene for medical systems is not officially unified on one level. Some areas are covered by international standards, e.g. from IEC and ISO, but the regulation and certification is mostly done only at a national level without mutual recognition and acceptance. There is no integrated, common and uniform approach to it. Only within the EU, is a harmonised approach being started which covers all nations within the EU (see 4.2.2).

4.2.1.2 Regulatory Bodies

On the international level, there exists no single regulatory body which deals with medical devices and provides approval on a world wide scale. All regulation and certification is done on a national level. Sometimes, the certification within one country is recognised by another country (e.g. within the EU, see 4.2.2), sometimes some mutual agreement exists, like between the USA and the EU (see 4.2.3).

4.2.1.3 Standardisation Bodies

The international standardisation bodies concerned with medical devices and equipment are

- IEC - International Electrotechnical Commission
- ISO - The Organisation for International Standardisation
- CEN - The European Committee for Standardisation

4.2.1.4 Recognised User Groups

The user groups can be separated into the manufacturers (as users of the standards) and the users of the medical devices. There exist different groups organised as associations, societies etc.

- Medical Users groups:

  Society for Minimally Invasive Therapy

  European Association for Endoscopic Surgery

Many of the organisations have subgroups dealing with special aspects. In addition, many international organisations have regional and national counterparts with similar scope and structure.

4.2.1.5 Discussion

The international scene is dominated by the USA and the EU. It seems that what receives approval in these countries is also very likely to be approved in other countries worldwide. This is especially true as long as approval is based on international standards from IEC and ISO. However, as far as is known, some national bodies are always involved (except in the EU, see 4.2.3)

4.2.2 European

4.2.2.1 Background

The European community is taking a new approach by providing the framework for a single certification procedure for medical devices which will be valid all over Europe. This approach is initiated by a set of European directives giving the general framework, but which need to be detailed by additional standards to be developed by CEN/CENELEC as harmonised standards.

4.2.2.2 Regulatory Bodies

There is no central European body as a regulatory body, but the Medical Device Directive (MDD) requires that each body within the European Community which wants to be a regulatory body for medical devices becomes a Notified Body. Each of these Notified Bodies in turn is able to certify medical devices, and the certification is valid not only within the country of the specific Notified Body, but all over the European community.

On the other hand, only medical devices which are certified by a Notified Body are allowed to be sold and used within the EU.

The governing law for the medical area is the European Community deciding on the directives.

The additional standards to be used are under the direction of CEN/CENELEC as the European standardisation body.

4.2.2.3 Standardisation Bodies

The Medical Devices Directive makes no special mention of computer based systems and how to deal with their certification. Only basic global statements are included which are also valid for computer based systems.

The officially recognised European standardisation body for medical devices is CEN/CENELEC.

4.2.2.4 Recognised User Groups

No recognised user groups have been identified.

4.2.2.5 Discussion

Regulation and standardisation of the medical devices sector is still developing both within Europe and worldwide. Unlike more established sectors, there was not a strongly national regulatory and standardisation environment in place prior to the establishment of the European Union. The starting point for regulation and standardisation of the medical devices sector within in Europe is issuing of European Directives and the work of CEN/CENELEC. This should lead to a harmonised European approach from the very beginning.

4.2.3 National

4.2.3.1 Germany

4.2.3.1.1 Background

Prior to the European Medical Device Directive which came fully into effect by 14 June 1998 the introduction and use of medical devices was regulated in Germany by the MedGV (Medizingeräteverordnung, 14 Januar 1985).

Medical devices are divided into four classes:

- Class I: Devices with minimum risk potential
- Class IIa: Devices with low risk potential
- Class IIb: Devices with high risk potential
- Class III: Most critical devices.

The intended purpose of the device is decisive for its classification. A product will always be grouped in the highest applicable product class, i.e. will always be required to adhere to the strictest standards.

4.2.3.1.2 Regulatory Bodies

As of March 1998, there are 22 Notified Bodies in Germany which are recognised as certification bodies for medical devices according to 93/42/EEC:

Bayerisches Landesamt für Maß und Gewicht, München

DEKRA Certification Services DCS GmbH, Stuttgart

DIN CERTCO Gesellschaft für Konformitätsbewertung mbH, Berlin

DQS Deutsche Gesellschaft zur Zertifizierung von Managementsystemen mbH, Qualitäts- und Umweltgutachter, Frankfurt

ECM Zertifizierungsgesellschaft für Medizinprodukte in Europa mbH, Aachen

EUROCAT Institute for Certification and Testing, Darmstadt

Institut für Mikrotechnik und Medizintechnik der Technischen Universität Berlin, Prüfstelle für Medizinische Geräte, Berlin

Landesamt für Meß- und Eichwesen Brandenburg, Potsdam

Landesamt für Meß- und Eichwesen Thüringen, Ilmenau

Landesgewerbeanstalt Bayern, LGA Zertifizierungsstelle, Nürnberg

mdc medical device certification, Memmingen

MEDCERT Zertifizierungs- und Prüfungsgesellschaft für die Medizin GmbH, Hamburg

MPA NRW Materialprüfungsamt Nordrhein-Westfalen, Dortmund

Physikalisch-Technische Bundesanstalt (PTB) Zertifizierungsstelle für Medizinische Meßgeräte, Braunschweig

RW-TÜV e.V., Zertifizierungsstelle für Gerätesicherheit, Aufzüge und Medizintechnik, Essen

Technischer Überwachungsverein Südwestdeutschland e.V., TÜV Cert-Zertifizierungsstelle, Mannheim

TÜV Berlin Brandenburg e.V., TÜV Cert-Zertifizierungsstelle für Medizinprodukte, Bonn

TÜV Product Service GmbH, Zertifizierungsstelle, München

TÜV Rheinland Product Safety GmbH, Köln

Verband Deutscher Elektrotechniker (VDE) e.V., VDE Prüf- und Zertifizierungsinstitut, Offenbach

ZDH-Zert Verein für Qualität im Handwerk und in der gewerblichen Wirtschaft e.V., Zertifizierungsstelle für Medizinprodukte, Rottweil

4.2.3.1.3 Standardisation Bodies

The standardisation bodies within Germany which are concerned with medical devices are:

DKE
Deutsche Elektrotechnische Kommission
Stresemannallee 14
D-60596 FRANKFURT

DIN
Deutsches Institut für Normung e.V.
Burggrafenstr. 6
D-10772 BERLIN

Within these bodies there are several subgroups dealing with different aspects of medical devices as well as with general aspects also relevant for medical devices.

DKE is a member of CENELEC and IEC. DIN is a member of CEN and ISO.

4.2.3.1.4 Recognised User Groups

No recognised user groups have been identified.

4.2.3.1.5 Discussion

Germany has established the largest number of notified bodies recognised as certification bodies for medical devices according to 93/42/EEC of any member country in the European Union. Drawing on the work carried out by the Food and Drugs Administration in the USA, Germany is active within the EU in establishing a robust regulatory environment for the growing market in medical devices.

4.2.3.2 The Netherlands

4.2.3.2.1 Background

The development of medical devices has changed the medico-technical practice in health care considerably over the last three decades. New technologies have become available and have moved into a growing number of medical application domains and with increasing introduction of new or modified systems.

The Act on Medical Devices (from 1970) [9] formed the legislative framework for market approval of medical devices. If covered by the Act, a category of devices had to be approved on the basis of specific requirements. The development of these specific market approval requirements was costly and only covered a few classes: condoms, cardiac pacemakers and sterilisation equipment. The Health Care Inspectorate was and still is the competent authority. The Health Care Inspectorate has no financial means at all to initiate device tests.

Accreditation of certifying bodies was not established before the European Directives on Medical Devices were adopted. Until then, some organisations, like KEMA and TNO, explored their opportunities, but with limited missions, e.g. electrical safety and endurance testing, and quality systems. Attempts to launch a specific certification scheme, such as a Medical TNO approval, failed in early stages. A pragmatic approach has been to adopt pre-market approval decisions from foreign notifying bodies, such as the Food and Drug Administration (USA) in particular.

The governmental policy of legislation development regarding medical devices is and has been lead by the pursuit of harmonisation within the European Union. The recent Medical Devices Directives (general + active implants) therefore provide the current legal framework fully enforced since June 14, 1998.

The Directives prescribe that manufacturers must notify competent authorities in member states as soon as they learn about (safety) problems in the application of their products. As said above, the Dutch competent authority is the Health Care Inspectorate. For this purpose, the TNO is running the NOTIS[10] Bureau were all class I devices must be registered by the manufacturer. Class I devices are CE self-approved by the manufacturer. The other classes II and III of medical devices must be approved by notified

[9] Wet op de Medische Hulpmiddelen, 1970
[10] NOTIS = NOTification and Information System

bodies who maintain their own registries and can be identified by the number accompanying a CE approval label.

In hospitals, users of medical devices are required to report device-related incidents to the internal clinical incident review committee. There is no legal requirement to report such incidents to an external bureau or the competent authority. Nevertheless, the European Directives require that each member state sets up and maintains a medical device reporting system. In the Netherlands, the NOTIS Bureau will provide this function on behalf of the competent authority.

At European level, the DIMDI (D) is building the EUDAMED as the European medical device reporting system that is to be fed by the member state systems.

To date, the implementation of the two European Directives on Medical Devices leads to a central role of TNO as national source of knowledge on assessment of and field experiences with medical devices. The national medical device reporting system, compulsory within the EU per June 1998 is being set up and will be maintained by this organisation.

Notified bodies are accredited in one or more of the domains of competence: active implants, medical devices, EMC, quality systems. At present, TNO Certification has been accredited for active implants, medical devices and EMC. KEMA has been accredited for medical devices and quality systems.

Until then, the Dutch Normalisation Institute as reference for medical device assessment has adopted international standards. The major modifications of the philosophy on safety in IEC 60513 (1994-01) on "Fundamental Aspects of Safety Standards for Medical Electrical Equipment" demonstrate the leeway of the medical sector regarding coherent system safety concepts. There still is a gap to bridge with the IEC 61508 (draft) standard.

4.2.3.2.2 Regulatory Bodies

Responsibility for market approval of medical devices rest with the Inspectorate of Health Care as the competent authority and is based on the Medical Devices Act (1970).

Radiological devices are licensed under the strict Acts on Radiological and Ionising Radiation Systems.

In practice the assessment and acceptance of medical devices is left to market mechanisms of users and user organisations, industrial parties and accredited licensing bodies. Unless and until serious incidents occur, the doctor still decides on what devices will be employed in medical practice. In the case of

an accident, the Inspectorate of Health Care may initiate an investigation and intervene by as far as the withdrawal of the device approval.

Until the European Directives came into force, the procedure to obtain a market approval for a medical device was almost lacking and mainly administrative. The competent authority policy was to follow FDA approval, but the check was less than marginal.

Regarding medical devices, accredited national notifies bodies are:

TNO Certification (Delft): active implants, medical devices, EMC

KEMA (Arnhem): medical devices, quality systems (ISO 900x, EN 46000)

Certification of software in PEMS is up to now not yet possible. A certification protocol is being developed by TNO.

4.2.3.2.3 Standardisation Bodies

Nederlands Normalisatie Instituut (NNI[11])

Nederlands Elektrotechnisch Comité (NEC[12])

4.2.3.2.4 Recognised User Groups

Industrial users of standards and regulations are organised in NEFEMED and SOMT (Foundation for Entrepreneurs in Medical Technology).

The Federatie Het Instrument is an industrial organisation for promotion of medical devices realising a platform were manufacturers, users, researchers and educators meet annually. Within the health care sector, numerous user organisations have been established mainly for professional advancement. Relevant to medical devices, user organisations exist at different levels and are linked closely to general hospital institutions.

The NVKF is a professional organisation of clinical physicists that is involved in the development of new technologies and advanced application of medical devices.

The NVTG is a professional organisation of engineers and technicians in health care.

---

[11] Kalfjeslaan 2, Postbus 5059, NL - 2600 GB Delft. http://www.nni.nl
[12] Kalfjeslaan 2, Postbus 5059, NL - 2600 GB Delft. http://www.nni.nl

The VZI is a professional organisation of hospital-based medical device engineers and as such directly involved assessment of medical devices in the field: the hard way.

The WIBAZ originated from medical instrumentation departments in academic (teaching) hospitals in order to create a national platform for assessment of medical devices based on user experiences.

Other professional groups, organisations of Intensivists, Anaesthesiologists and Intensive Care Nurses have activities aimed at the advancement of their profession, including the clinical use of medical devices and related issues.

The exchange of knowledge, views and experiences among professional groups stemming from distinguishable medical specialities is still very limited.

Until the early nineties, the Working Group on Instrumentation Assessment in Academic Hospitals (WIBAZ) evaluated medical devices on a single device basis with input from user experiences. Current review activities are still required to be checked with WIBAZ. In the same period, the TNO organisation performed comparative device tests on request of the National Hospital Institute. This ended when the NHI stopped financing these performance and safety tests. The TNO Medical Physical Institute performed their devices tests[13] following the regulations of the Medical Devices Act, and if lacking, the IEC 601 standards. In case that these international standards did not provide guidance, the ECRI[14] (USA) was consulted.

Today, general hospital institutions are organised in the NZf and the Organisation of University Hospitals[15]. These bodies advise their members in developing strategies for coping with emerging device-related issues, such as the EMC/EMI policy of abandoning the use of mobile phones inside hospitals or the millennium problem.

The input of users, notified bodies and academia on standard development, e.g. IEC 60513 or the IEC 60601 series, has stopped completely since a couple of years, after the Dutch Normalisation Institute started to require payment of a high fee for the right of participation. Consequently, only industrial members can afford to be actively involved in standardisation development.

---

[13] Because the Dutch market is a small one, the organised assessment of medical devices could only cover limited groups of devices.

[14] The ECRI is an organisation that operates independent from manufacturers and is financed by user organisations, mainly hospitals.

[15] Vereniging van Academische Ziekenhuizen (VAZ)

4.2.3.2.5 Discussion

The general scene is that confusion governs all over. The consequences of the European harmonisation regarding medical devices are not yet fully apprehended by end users, new notified bodies have to prove themselves on the market, European regulation includes exclusions, and the millennium bug demands priority attention.

4.2.3.3 The United States of America

4.2.3.3.1 Background

In the USA, the policies concerning the medical sector were stated in the first two main publications of the Food and Drug Administration (FDA) in 1938 and 1947, the "Federal Food, Drug and Cosmetic Act", and the "Requirements of the United States Food, Drug and Cosmetic Act".

Over the years, the documents were revised and additional aspects and even documents were added. One such aspect was the "Good Manufacturing Practice Regulations" for different products and areas.

These federal laws and regulations are used for interstate shipment as well as for imports, and even consumers use them as a reference to check how they are protected by the law.

In order to make the exchange of goods easier between the USA and the European Union, it is anticipated that the regulations being outlined in the European Union e.g. in the Medical Device Directive of the EC, will be harmonised with the FDA regulations.

4.2.3.3.2 Regulatory Bodies

Based on the laws enacted by the United States Congress, the Food and Drug Administration (FDA) issues regulations and guidance documents. The FDA is currently organised into five major programme centers:

- the Center for Biologies Evaluation and Research
- the Center for Drug Evaluation and Research
- the Center for Food Safety and Applied Nutrition
- the Center for Veterinary Medicine
- the Center for Devices and Radiological Health (CDRH)

The last one listed is responsible for medical devices and therefore is the one most concerned with programmable electronic systems.

Important amendments to the above mentioned "Federal Food, Drug and Cosmetic Act" are:

- the Safe Medical Devices Act of 1990, which enhances the premarket approval authority and provides for postmarket approval requirements and additional regulatory authority over the manufacture, sale, and distribution of devices,

- the Medical Device Amendments of 1992, which delayed tracking requirements, clarified statutory provisions for medical device reporting (MDR) and postmarket surveillance study requirements.

The US Federal regulatory body is

US Department of Health and Human Services
Food and Drug Administration (FDA)
Center for Devices and Radiological Health (CDRH)
9200 Corporate Boulevard
Rockville, MD 20850
USA

Within the FDA-CDRH, special attention is given to the evaluation in the

Office of Device Evaluation (ODE)

and to small companies in the

Division of Small Manufacturers Assistance (DSMA)

4.2.3.3.3 Standardisation Bodies

For different aspects there exist several standardisation bodies covering partially overlapping areas. These are on the national level.

- AAMI - Association for the Advancement of Medical Instrumentation

- ANSI - American National Standards Institute

- IEEE - Institute for Electrical and Electronics Engineers

- ISA - Instrument Society of America

These bodies are cooperating with the related international standardisation bodies, e.g.

- IEC - International Electrotechnical Commission

- ISO - International Organisation for Standardisation

4.2.3.3.4 Recognised User Groups

The following are some of the recognised user groups in the USA:

- the American Hospital Association (AHA)
- the Medical Electronics Manufacturers Division (MEMD) of the Electronic Industries Association (EIA).
- the Health Industry Manufacturer's Association (HIMA)
- the Association of Medical Diagnostics Manufacturers (AMDM)
- Medical Device Manufacturers Association
- Association of Medical Device Reprocessors
- International Society of Healthcare Central Supply Materials Managers
- American Society of Healthcare Central Service Professionals
- Association for the Advancement of Medical Instrumentation

and for a professional focus,

- the American College of Clinical Engineering (ACCE).

4.2.3.3.5 Discussion

The FDA tries to be in good contact with manufacturers, users and the general public, using modern technology like email and fax on demand. In the USA, a classification of devices is being done in three classes, while in the EU there are four classes. In order to make the exchange of goods easier between the USA and the European Community, it is anticipated that the regulations being outlined in the European Community e.g. in the Medical Device Directive of the EC, will be harmonised with those of the FDA. The negotiations on the Mutual Recognition Agreement (MRA) between the USA and the EU were completed on 20 July 1997, but not yet put into force. A guidance document on the mutual recognition concerning medical devices is being developed by the FDA (FDA/CDRH: Guidance for Staff, Industry and Third Parties - Third Party Programmes under the Sectoral Annex on Medical Devices to the Agreement on Mutual Recognition between the United States of America and the European Community (MRA) - Draft 1998-07-02).

4.3 Rail

4.3.1 International

4.3.1.1 Background

The rail sector has cooperated internationally since 1922 to achieve interoperability between rail networks in different countries around the world. While much has been achieved e.g. standardisation of gauges etc., there still remain outstanding problem areas. These arise partly because of the history of national standardisation and regulation and partly from a traditional splitting of responsibility for signalling regulation and standardisation from that for train control.

4.3.1.2 Regulatory Bodies

There is no international regulatory body for this sector.

4.3.1.3 Standardisation Bodies

In 1922 the International Union of Railways UIC (Union Internationale de Chemin de Fer) was founded to establish interoperability rules and standards for railway systems crossing national borders.

The UIC has worked out common operating rules in international passenger and freight traffic. They have started a global infrastructure planning and have founded ERRI, the European Railway Research Institute, for joint research and testing. In the information technology sector the first harmonisation activities have been done within the Hermes network. Also for passenger transport in international trains a common reservation and billing system etc. has been established. For freight transport the railway cars have been standardised, a quality level has been established (Eurorail Cargo).

The main task of the UIC is to force the harmonisation of the railway infrastructure. One major task is on technical interoperability. The UIC works on the harmonisation and standardisation of the equipment and the rolling stock. The UIC publishes for this task the ”UIC technical leaflets”.

In the area of high speed trains because of an EC requirement, the UIC work on the realisation of interoperability for high speed trains. In co-operation with the European standardisation body CEN/CENELEC and in the framework of AEIF, in co-operation with industry, UIC are drafting the Technical Specifications for Interoperability (TSIs), the ETCS specifications.

4.3.1.4 Recognised User Groups

Apart from the UIC there are no identified international user groups for this sector.

4.3.1.5 Discussion

Modern technological developments have resulted in a close interaction between train control systems and signalling systems. This is particularily true of systems involving the use of computers. Traditionally standards relating to signalling were developed separately to those related to train control. As a result trains operating across some borders may still have to conform to two different regulatory requirements as, for example, between Sweden and Denmark.

4.3.2 European

4.3.2.1 Background

Within Europe regulation at the European level is via Directives issued by the European Commission. European standards are developed by CEN/CENELEC. There has of course been a long history of achieving interoperability across borders between neighbouring countries within Europe. There still remain however differences in requirements between countries e.g. on information systems and on braking systems, which remain to be dealt with.

4.3.2.2 Regulatory Bodies

The EC has formulated 15 directives, which are mandatory for all member countries, who have to adapt their national rules according to the directives. A number of these directives apply to railways and related products. The standards according to these directives are made by CEN/CENELEC and ETSI, and have after approval by voting among members to be taken over by national standardisation organisations.

4.3.2.3 Standardisation Bodies

For Europe the standardisation body for the railway is located at CEN/CENELEC (EN standards). ETSI issues ETS standards.

There the main task for railways is covered by the subcommittee SC9XA.

This subcommittee works out the standards for the ERTMS system in accordance with the TSI worked out by the AEIF. Industry, railways, research organisations and test centres are all involved in the work of this subcommittee.

CENELEC TC9X is responsible for Railway Applications (RA) together with CEN TC256. Up to now TC9X has issued over 30 standards and is actively working on 110 new proposals. It is also very active in maintaining issued standards. TC9X has the following subcommittees:

- SC9XA Communication, Signalling & Processing System
- SC9XB Rolling stock
- SC9XC Fixed installations

With many working groups, some relevant are:

- TC9X-WG1 Electronic equipment
- TC9X-WG4 EMC
- TC9X-WG5 System
- TC9X-WG5A Systems
- TC9X-WG5B RAMS (- prEN50126)
- TC9XA-WGAI Software (- prEN50128)
- TC9XA-WGA2 Safety related electronic systems
- TC9XA-WGA3 EMC
- TC9XA~WGA4 Traction/Signalling compatibility
- TC9XA-WGA6 Safe data transmission

Examples of activities in the TC9X are:

1. Make a survey on the needs for a future EN on ETCS European Train Control
2. Studying procedures for demonstrating SIL
3. Studying the concept of mutual recognition of test results
4. Making guide for the use of terminology for testing procedures
5. Method of linking a type of railway operation to a Safety Integrity Level (SIL)
6. Hazardous failure rates and SIL. Definitions and methodology

4.3.2.4 Recognised User Groups

Union des Industries Ferroviaires Européennes (UNIFE),

Apart from the UNIFE there are no other identified European user groups for this sector.

4.3.2.5 Discussion

While harmonisation of standards between countries within the European Union is being pursued within the rail sector through sector specific committees under CEN/CENELEC, there still remains the split of responsibilities separating national signalling from train control. This is a problem area which will become more marked as the move to greater automatic control of trains leads to greater interaction and interdependence between the signalling systems and the onboard train controllers.

4.3.3 National

4.3.3.1 Austria

4.3.3.1.1 Background

The first continental public railway was built in Austria from Linz to Budweis (1828 – 1832), but operated by horse-driven vehicles, not steam engines. The first steam-engine driven railway from (Vienna-) Floridsdorf to Deutsch Wagram was built 1837. Imperial "Priviledges" were the basis of building railway lines and defining certain rules of operation, governmental regulations ("Verordnungen", having legal impact and interpreting laws in respect imperial "priviledges") provide some legal framework for operations even in a technical sense. Operation of railways was ruled by regional "instructions", derived from English rules, but different between railway organisations. Severe accidents lead in 1851 to the first regulation for all Imperial Austrian countries ("Eisenbahnbetriebsordnung für alle Kronländer", Wien 1851). In 1872 signalling rules were standardised throughout Imperial Austria (predecessor of the "Dienstvorschrift V2"). In 1877 operational procedures for railway traffic were standardised (predecessor of "Dienstvorschrift V3"). In 1899 operation of trains keeping "blocking distance" became obligatory. In 1906 a new regulation for signalling on main and secondary lines was introduced and in 1909 the "Regelblatt 5007" for a standard railway interlocking system was issued. The "Dienstvorschrift V2" (Regulation V2 for Signalling) of the Austrian Federal Railways (ÖBB, formerly BBÖ) was issued 1925 and the general "Dienstvorschrift V3" (regulation for railway operation) was issued 1930. Both were reissued several times (1951, 1962, 1980, 1986), always accompanied by changes in signalling and operational procedures.

In 1841 Imperial Austria started the first governmental railway building programme, in 1842 the first "General Directorate for National Railways" (Generaldirektion der Staatseisenbahnen) was founded. The Ministry of Trade became the regulatory body for the all Austrian Railways in 1856. 1896 a separate "Ministry of Railway Transport" was founded. After the first World war, with the end of the Austrian-Hungarian Monarchy, the remaining railway lines were regulated by a "Department of Transportation" (later on "Federal Ministry of Transportation"). After the second World War, the "Ministry for Nationalised Industry and Transport" was responsible as regulatory body for Austrian railway (and related) transport systems, such as cable cars, shipping lines, telecommunications, etc. In 1995, because of major changes in the organisation of railways and national PTTs (privatisation, EC rules for competition, new providers), the state being no longer "owner" of these organisations and its role being reduced to that of a regulatory body

only, the remaining activities of the "Ministry of Transport" were integrated in a "Ministry of Science and Transport"[16].

4.3.3.1.2 Regulatory Bodies

The regulatory body for railway is located at the Federal Ministry of Science and Transport (Supreme Transport Authority). The group for railways is responsible for judicial, administrative, technical and economic aspects of the transportation type "rail" (railways, cable cars, etc.) They are the representative of the government in the international bodies e.g. OTIF (Organisation for International Railway Transport, Bern), OITAF (International Organisation for Cable Cars).

4.3.3.1.3 Standardisation Bodies

In Austria the main standardisation work in the dependability area is done by ÖVE, the Austrian Electrotechnical Association. ÖVE is the Austrian national organisation for IEC and CEN/CENELEC work and is officially representing Austria in the respective working groups and committees, including the mirror committee for the CEN/CENELEC SC9XA, IEC SC 65A, IEC TC 56 etc. The members of this committee and its subgroups and working groups are from industry, railways, test centres and research organisations. For major issues, such as IEC 61508, separate working groups have been installed (MR 65 SC.1) besides the committee responsible for the TC or SC work.

4.3.3.1.4 Recognised User Groups

User groups which are relevant are mainly from the ÖIAV (Österreichischer Ingenieur- und Architektenverein – Austrian Engineers and Architects Association), who has installed working groups for transportation issues, railways etc., or from industry associations like the FEEI (Federation of electronic and electrotechnical industry). Another group of organisations are from the transport industry with members from industry, transport organisations and research, like the ÖVG (Österreichische Verkehrswissenschaftliche Gesellschaft - Austrian Association for Research in Transportation), ÖGV (Österreichische Gesellschaft für Verkehrspolitik – Austrian Association for Transport Policies). These organisations understand themselves as "pressure groups" for certain interests and progress in transportation.

---

[16] Christian Hager, Eisenbahnsicherungsanlagen in Österreich, Bd.1 , 2, Verlag Pospischil, Wien; 1994 and Das Buch der Bahn, 1987, Österr. Verkehrswerbung.

4.3.3.1.5 Discussion

In Austria no national standards are related specifically to safety critical software-intensive systems. Standards related to dependability and safety in general are: one generic standard OeNORM M8103 and two railway standards OeVE-T3 OeVE-T3a.

4.3.3.2 France

4.3.3.2.1 Background

The first two railway lines opened in France were between Paris and Versailles. The line which ran along the right bank of the Seine was opened in 1839 and the one along the left bank opened the following year. The network grew steadily and by 1855, apart from a few unimportant lines, all the main lines radiated out from the capital forming a kind of star shape whose central point was Paris.

In 1938, major French railway companies merged into the French National Railways - Societe Nationale de Chemin de Fer (SNCF).

SNCF is a "Public Establishment of an Industrial and Commercial Character" or EPIC, being entirely state owned but with a legally autonomous status. Apart from the rail core organisation, SNCF has full or part ownership of 357 other companies connected with transport, freight haulage and hotels.

In 1997 a new EPIC, the French Railways Infrastructure Authority (RFF), was established to assume the management and development of and investment in, the national rail infrastructure. Under the new arrangements, the government accepted future responsibility for infrastructure finance. Ownership of the infrastructure together with the associated debt was transferred from SNCF to RFF. Currently (1999), maintenance and operation is subcontracted to SNCF's infrastructure department. In this aspect, the situation in France differs from that in several other European countries where infrastructure has been completely separated from operation.

4.3.3.2.2 Regulatory Bodies

The transport system owner has to submit all Automatic Passenger Protection Equipment (APPE) for ministerial approval (Ministry of Transport)(statutory order of March 1942, in particular articles 31 and 31b).

It is the responsibility of the owner to provide the safety case that allows the safety authority to license the system.

The safety Authority appoints an independent assessor to perform, in parallel with the development lifecycle of the system, a safety assessment. The assessment includes :

- safety management and organisation,
- safety requirements and compliance,

- safety target and integrity level,
- compliance with standards and required techniques,
- safety case
- other safety issues (exploitation, maintenance, installation ...).

It is possible for the independent assessor and for the owner to appoint further experts.

4.3.3.2.3 Standardisation Bodies

The French Standardisation Organisation is AFNOR. In railway applications, the assessment has to comply with AFNOR 71-011, 012 and 013.

4.3.3.2.4 Recognised User Groups

No recognised user groups have been identified.

4.3.3.2.5 Discussion

While the railway network in France has been reorganised to open the network to allow competing railway companies to operate in France, the process has still some way to go. As a result the French regulatory and standardisation environment in this sector has not changed significantly over recent years.

4.3.3.3 Germany

4.3.3.3.1 Background

The railways of Germany were nationalised in 1920 to form the Reichseisenbahn, but after the Second World War, the railways were split again, one each for East and West Germany. After the re-unification of the two halves of Germany, the Deutsche Bundesbahn (German Federal Railroads) and the Deutschen Reichsbahn (German National Railroad) merged once again. According to the new Railway Act the railways in Germany became privatised and the Deutsche Bahn AG was founded on the first of January 1994.

4.3.3.3.2 Regulatory Bodies

In Germany, the Ministry of Transport - Bundesministerium für Verkehr (BMV) is responsible for the observance of the railway laws (Eisenbahnneuordnungsgesetz). The relevant German Law is the Eisenbahnbetriebsordnung (EBO). In the licensing procedure the BMV is the top supervisory authority of all those involved in the railway system. One of the tasks of BMV is to control the activities of the Federal Railway Authority - Eisenbahn-Bundesamt (EBA).

Prior to 1994 the former Deutsche Bundesbahn was self-regulating. Licensing and certification was performed by the Bundesbahn itself. Railway components were tested by the manufacturer, by the Bundesbahnzentralämter (BZA) and by the Güteprüfdienst (quality testing department) of the Bundesbahn. This is now the responsibility of the EBA. The EBA is a federal authority responsible for the licensing procedure and the supervision of the Federal Railway (Deutsche Bahn AG) and for foreign railway operators using the railway tracks in Germany. There are also Non Federal Railways and for which the relevant State Government is responsible. The State Government Department responsible is Landesbevollmächtigter für Bahnen (LfB). There is also an authority responsible for short distance public transport called the Technische Aufsichtsbehörde (TAB) which is also a part of the State Government.

In seeking approval for a railway system or for the use of an item of equipment a Safety Case has to be created. The Safety Case has to be assessed by an independent assessor. According to the Eisenbahnneuordnungsgesetz (German railway law) the EBA is the accrediting board for all parties which apply for acceptance as institutions for independent testing or for quality control. Individual railway components can be tested and certificated by EBA using the services of an accredited independent testing organisation such as TÜV EURO RAIL.

Following any change to the system which may impact on the safety case the owner of the system is required to submit an appropriately modified safety case which must be independently assessed before being approved by the EBA.

4.3.3.3.3 Standardisation Bodies

Standards for the Railway systems in Germany were formerly created and issued by the department responsible for internal quality assurance (Bundesbahnzentralämter BZA) within the former Deutsche Bundesbahn. Mü 8004 is a collection of requirements, principles, and guidelines created as an internal standard of the Deutsche Bundesbahn . EBA has declared that Mü 8004 be considered as an official EBA document.

4.3.3.3.4 Recognised User Groups

In Germany the principal user group is an association of all groups of suppliers to the railways called Verband der Deutschen Bahnindustrie (VDB).

4.3.3.3.5 Discussion

In common with a number of other countries, Germany's rail system is undergoing a transition from the public sector to the private sector. This brings with it a reorganisation of the regulatory environment. Under the public sector ownership, self-regulation with federal regulators having an overseeing role was in place. Under the new regime, many of the standards developed under the previous regime are being carried over. A measure of self-regulation will continue, however the involvement of appointed testing organisations will gradually increase and a modified regulatory environment will emerge.

4.3.3.4 The Netherlands

4.3.3.4.1 Background

Regulation of railway safety started at the end of the 19th century, with the Spoorwegwet, 1875 (Railways Law). This law builds a framework for the exploitation of railways in the Netherlands. The law itself gives some rules for railway safety, and more important, gives the Minister van Binnenlandse Zaken (Minister of Internal Affairs) the power to issue additional regulation (AMVB=Algemene Maatregel van Bestuur). This resulted in the Algemeen Reglement Vervoer (Rules for Transport) and Reglement Dienst Hoofd- en Lokaalspoorwegen (Rules for Main and Local Railways). These give additional rules for railway safety.

The Spoorwegwet gave birth to the Spoorwegongevallenraad (Council for Railway Accidents). This is a committee that investigates railway accidents and railway safety. Only recently this committee found its end, because of a new law, Wet Raad voor de Transportveiligheid (Transport Safety Council Law). This council has a broader perspective and investigates safety in all transport, except shipping.

Other important legislation can be found in the Wet Personenvervoer, 1987 (Law for Passenger Transport). This law gives a framework for giving permission to transport passengers. The Algemeen Reglement Vervoer (Rules for transport in general) gives rules for transport in general, including safety regulation.

The Burgerlijk Wetboek (Civil Code) addresses safety in several ways. Most important is the liability for all damage during transport of the passenger (8:105 BW). The liability of Nederlandse Spoorwegen (Dutch Railways) is limited to 300.000 NLG in case of injury or death.

The Lokaalspoor- en Tramwegwet, 1900 (Local Railways and Tramways Law) gives additional regulation for low speed railways. The Minister van Verkeer en Waterstaat (Minister of Transport and Public Works) can give additional safety regulation based on this law.

The Wet Aanleg Lokaalspoor- en Tramwegen, 1917 (Construction of Local Railways and Tramways Law) also covers low speed railways and gives rules for permitting to build and maintain such a railway.

The already mentioned Reglement Dienst Hoofd- en Lokaalspoorwegen, 1977 (Rules for Main and Local Railways) gives rules for all railways where the Lokaalspoor- en Tramwegwet and the Wet Aanleg Lokaalspoor- en Tramwegen are not applicable. These rules are very specific regarding safety of the railways: maintenance, railway crossings, signalling, rolling stock, etc.

The Verdrag Betreffende het Internationale Spoorwegvervoer, 1966 (Treaty on International Railway Transport, COTIF) gives some rules for liability in case of death or injury.

4.3.3.4.2 Regulatory Bodies

Railway safety is the responsibility of the Minister van Verkeer en Waterstaat (Minister of Transport and Public Works). There are two main departments responsible for executing his policy.

The first is the Rijksverkeersinspectie (State Traffic Inspection), part of the Directoraat-Generaal voor het Vervoer (Transport Directorate) of the Ministerie van Verkeer en Waterstaat. One of the parts of the Rijksverkeersinspectie is the afdeling Spoorwegtoezicht (Department Railway Inspection).

The second is the Directie Verkeersveiligiheid en Voertuig (Directorate Traffic Safety and Vehicle), part of the Directoraat-Generaal Personenvervoer (Passenger Transport Directorate) also of the Ministerie van Verkeer en Waterstaat.

As already mentioned the Raad voor de Transportveiligheid, also part of the Ministerie van Verkeer en Waterstaat, investigates accidents in transport, including railway transport.

4.3.3.4.3 Standardisation Bodies

The Netherlands have their own standards organisation, NNI, Nederlands Normalisatie Instituut.

The Netherlands have a strong tendency to conform to international standards. No specific Dutch standards have been identified.

The European Rail Research Institute (ERRI) has its offices in Utrecht and makes standards which are publicly available, but are not compulsory. These standards include standards on various railway safety systems. A catalogue of their work can be obtained at their offices.

If there is standardisation, this can be found at design level within Dutch Railways. This however lacks legal basis.

Nederlandse Spoorwegen show strong interest in international regulation and standardisation and cooperate in many international committees, like those from IEC and CENELEC.

4.3.3.4.4 Recognised User Groups

No recognised user groups have been identified.

4.3.3.4.5 Discussion

The Netherlands tend to be very strict in using standards. This means that applicable standards will be used and interpreted literally. This approach makes cooperation with e.g. Germany easy, but may bring difficulties in cooperating with some other countries. The Netherlands engineers in railway safety feel that their way of doing railway safety is very good, and better than in many other countries of the EU. They fear the European legislation because in many cases this means degrading of their existing standards.

As a top level standard IEC61508 will certainly be used by the rail sector in the Netherlands.

4.3.3.5 Poland

4.3.3.5.1 Background

Presently, the only operator of railways in Poland is PKP - Polskie Koleje Pañstwowe (Polish State Railways). The only exception are the proprietary railways in factories, mains, electric plants, shipyards, etc. However, concerning safety those proprietary railways are subjected to the regulations issued by PKP.

Authorisation for exploitation of railway equipment is issued by PKP based on the certificate given by CNTK - Centrum Naukowo-Techniczne Kolejnictwa (Technical and Research Center of Railways).

CNTK is also responsible for new regulations and certification criteria. CNTK is supervised by PKP and PKP has the initiative in case of new regulations.

4.3.3.5.2 Regulatory Bodies

Until 1997 the railway regulations were issued by Dyrekcja Generalna PKP - (General Directorate of Polish State Railways) , Warsaw with close cooperation with CNTK - Centrum Naukowo-Techniczne Kolejnictwa (Technical and Research Center of Railways) in Warsaw (institution supervised by PKP).

Recently, at the Ministry of Transportation, on the basis of the regulation from 27.06.97 (Dz. Ustaw nr 96) was created Glowny Inspektorat Kolejnictwa - GIK (Main Inspectorate of Railways). The objectives of GIK are as follows:

- technical supervision of exploitation of railway tracks and trains and of railway safety

- supervision of development in the domain of railway transportation.

GIK will supervise PKP and other railway operators, will certify (through appointed laboratories) railway equipment and will participate in investigations of railway accidents. It will also issue regulations related to railway safety.

GIK includes the following departments:

- Department of Railway Safety (Departament Bezpieczenstwa Ruchu Kolejowego)

Department of Railway Certification (Departament ds. Swiadectw Dopuszczenia do Eksploatacji)

GIK has its divisions in main cities of Poland: Warszawa, Lublin, Krakow, Katowice, Gdansk, Wroclaw and Poznan.

GIK took over the role of Dyrekcja Generalna PKP (General Directorate of Polish State Railways). So far the activity of GIK is visible only on the level of certification (where it cooperates with CNTK and Main Inspectorate of Labour).

4.3.3.5.3 Standardisation Bodies

The work on railway standards is done mainly by CNTK in cooperation with research institutions and main producers in a given field. For example, in the area of railway signalling equipment, some influential institutions are Transportation Institute of Warsaw University of Technology, Transportation Automatics and Electronics Institute of Radom University of Technology and Adtranz Zwus in Katowice.

4.3.3.5.4 Recognised User Groups

Standards and regulations are used by:

- PKP as the operator of the railway network in Poland
- operators of the proprietary (local) railways
- producers of railway equipment
    - The main producer of the railway signalling and track equipment is Adtranz Zwus in Katowice
    - The main producers of railway cars are Adtranz PAFAWAG in Wroclaw and Siemens Cegielski in Poznan.

4.3.3.5.5 Discussion

In the next years it is expected that Polish State Railways will be subjected to the process of deregulation and privatisation. In this case the above structure will change. There will be several railway network operators and separated (from them) regulatory body and certifying institutions.

4.3.3.6 The United Kingdom

4.3.3.6.1 Background

The railway system in the United Kingdom was nationalised under the provisions of the Transport Act 1947. The various independent railway companies were absorbed into British Railways which came into existence on 1 January 1948. The 1947 nationalisation established both the London Transport Executive and the Railway Executive under the aegis of the British Transport Commission. The British Transport Commission was abolished under the 1962 Transport Act, and British Railways and London Transport became separate Boards answering directly to the Ministry of Transport.

In 1994 British Rail was privatised and The Railways (Safety Case) Regulations 1994 became the governing legislation. A number of private companies were given franchises to operate train services on the railway infrastructure, track and signalling etc. which was to be owned and operated by a new company called Railtrack.

4.3.3.6.2 Regulatory Bodies

Under the Railways (Safety Case) Regulations 1994 all railway undertakings require approval to operate granted by the UK's railway safety authority (HMRI) - the Railway Inspectorate of the Health and Safety Executive. Railtrack as the infrastructure controller holds the Network Licence issued by the Secretary of State for Transport. The Health and Safety Executive accepted Railtrack's Safety Case (RSC) in 1994. All current train and Station operators have had their RSCs accepted by Railtrack. As required under its licence Railtrack has established an internal Safety and Standards Directorate independent of the operational management of the Company. The Directorate is responsible for monitoring Railtrack's compliance to its own Safety Case and the compliance of the train and station operators to their individual RSCs.

4.3.3.6.3 Standardisation Bodies

The process by which mandatory Railway Group Standards are produced, revised, accepted, authorised and issued is managed by Railtrack's Safety and Standards Directorate on behalf of all the Companies involved in the UK rail network. The process for the development of new railway standards in the UK is itself set down in a standard - GA/RT6001: Railway Group Standards Change Procedures.

4.3.3.6.4 Recognised User Groups

In the UK, the Railway Industries Association provides a national focus for standardisation activities e.g. developing a railway specific version of the early IEC SC65a WG's 9 and 10 draft standards for consideration by CENELEC.

The Institute for Railway Signal Engineers provides a forum for related professional activities.

The Railway Forum was established in 1996, to promote the growth and development of the rail system in the UK. It aims to act as the voice of the many companies now working to provide rail services.

The Association of Train Operating Companies (ATOC) is an unincorporated association which is intended to facilitate the development and operation of commercial arrangements between passenger operators and to promote the use of the railway network, including, in particular, the making of journeys which involve the services of more than one operator.

4.3.3.6.5 Discussion

Prior to privatisation the railway system had in place an essentially self-regulatory regime overseen by the appropriate government regulators. Following the privatisation of the railway system in the UK in 1994 this approach has been kept as far as possible by requiring Railtrack through the mechanism of the approval of safety cases submitted by the individual private rail companies. By this means the approach to regulation has been only slightly modified and a degree of continuity has been achieved.

4.4 Nuclear

4.4.1 International

4.4.1.1 Background

The nuclear power producing industry is currently no longer a growth area. The first nuclear power plant in commercial operation started up in 1956. By 1991 over 500 units had been constructed worldwide. Around 400 of these were fully operational, the other 100 having been closed down for a variety of reasons. Over recent years the ordering of new plants has fallen to a negligible level.

4.4.1.2 Regulatory Bodies

The International Nuclear Regulators Association (INRA)

INRA was established in January 1997 and is an association comprised of the most senior officials of the nuclear regulatory authorities of the following countries: Canada, France, Germany, Japan, Spain, Sweden, the United Kingdom, and the United States of America. The main purpose of the association is to influence and enhance nuclear safety, from the regulatory perspective, among its members and worldwide.

The Nuclear Energy Agency (NEA)

NEA is an agency established by the Organisation for Economic Cooperation and Development (OECD).

The Committee on Nuclear Regulatory Activities (CNRA)

Within the NEA, the Committee on Nuclear Regulatory Activities is an international committee made up of senior representatives from regulatory bodies. It was created in 1989 to guide NEA's programme concerning the regulation, licensing and inspection of nuclear installations with regard to safety.

CNRA's main tasks are to:

- exchange information and experience among regulatory organisations
- review developments which could affect regulatory requirements
- review current practices and operating experiences.

The CNRA collaborates with the International Nuclear Regulators' Association (INRA).

4.4.1.3 Standardisation Bodies

The International Atomic Energy Agency (IAEA), headquartered in Vienna and with 126 member States, is the key international organisation for the peaceful uses of nuclear energy and technology. The IAEA, set up in 1957, is an independent inter-governmental organisation within the United Nations system. The IAEA's areas of international cooperation cover all aspects of reactor operations, the nuclear fuel cycle, radioactive waste management, human health and radiation protection, and safeguards.

The IAEA has developed Nuclear Safety Standards (NUSS) for nuclear power plants which were prepared by experts from its Member States. They cover the following five areas:

- governmental organisation of regulation of nuclear power plants;
- safety in nuclear power plant siting;
- safety in the design of nuclear power plants;
- safety in nuclear power plant operation;
- quality assurance for safety of nuclear power plants.

The IAEA's safety standards are mandatory with regard to nuclear activities undertaken with IAEA assistance, but where such assistance is not provided the standards are recommendatory.

4.4.1.4 Recognised User Groups

WANO (World Association of Nuclear Operators)

The mission of WANO is to maximise the safety and reliability of the operation of nuclear power plants by exchanging information and by encouraging communication, comparison and emulation amongst its members.

The World Association of Nuclear Operators (WANO) was formed following the Chernobyl accident and held its inaugural meeting in Moscow in May 1989. With Regional Centres in Atlanta, Moscow, Paris and Tokyo and a coordinating centre in London, WANO links 148 operators of nuclear power plants in more than 30 countries.

The exchange of operating experience information is the basis of WANO's various programmes. Information and event reports are submitted by each operating organisation to its regional centre where they are reviewed for clarity and completeness and then distributed to all WANO members using an international electronic information exchange system.

4.4.1.5 Discussion

The nuclear power industry is arguably the most strictly regulated of all industries. The impact of a nuclear accident can cross national boundaries. Since the Chernobyl accident there has been increased international collaboration in the field of nuclear power plant operation and safety. There is however no single international body charged with regulating the safety of nuclear power plants. The United Nations in conjunction with the IAEA maintain a monitoring and regulatory role in relation to the production of fissile materials.

4.4.2 European

4.4.2.1 Background

The member states of the European Union have the largest number of operating nuclear power plants in the world. In common with the worldwide trend there has been an effective moratorium on the construction of new nuclear power plants in all European countries apart from France.

4.4.2.2 Regulatory Bodies

The role and tasks of the European Commission in the nuclear sector have as their legal basis the Euratom Treaty signed in March 1957. Euratom safeguards concerning nuclear materials are carried out by the Euratom Safeguards Directorate based in Luxembourg. Euratom inspectors work in cooperation with IAEA inspectors in implementing the IAEA agreements in the European Union. Euratom also has established agreed levels for radiological protection within the nuclear power industry in Europe. Licensing of nuclear power plants and other matters relating to the safety aspects of existing and emerging technologies remain the responsibility of individual member countries. A council resolution in 1975 committed Member States and the Commission to a process of progressive harmonisation of Community safety rules and practices. A resolution in June 1992 confirmed these objectives.

4.4.2.3 Standardisation Bodies

The European Atomic Energy Community (Euratom) was established by treaty in 1957. Within the overall workings of the European Commission, Euratom seeks to achieve the harmonisation of standards for the nuclear industry across Europe. Euratom works closely with IAEA signing agreement on behalf of the European Union.

Nuclear standards developed by IEC are considered for adoption as harmonised European standards by CEN/CENELEC.

4.4.2.4 Recognised User Groups

FORATOM is the association of European Atomic Forums, representing the European nuclear industry before the institutions of the European Union.

4.4.2.5 Discussion

Each of the European countries having operating nuclear power plants has a regulatory organisation to monitor and license its nuclear plants. At the European level issues such as siting of new nuclear plant and facilities when emissions could cross national boundaries are addressed. Also at the European level harmonisation of standards across Europe is implemented.

Within Europe Euratom interfaces and represents Europe in nuclear matters with IAEA and other international bodies.

4.4.3 National

4.4.3.1 Finland

4.4.3.1.1 Background

In Finland, the legislation for the use of nuclear energy and for radiation protection was established in 1957. Since then several amendments and new regulations have been issued.

In 1988 a completely revised Nuclear Energy Act was issued, together with a supporting Nuclear Energy Decree.

The Radiation Act and Decree were revised in 1991, taking into account the ICRP Publication 60 (1990 Recommendations of the International Commission on Radiological Protection). Section 2, General principles, and Chapter 9, Radiation work, of the Act are applied to the use of nuclear energy.

Based on the Nuclear Energy Act, the Council of State issued in 1991 the following decisions:

- Decision of the Council of State on the General Regulations for the Safety of Nuclear Power Plants (395/1991)

- Decision of the Council of State on the General Regulations for Physical Protection of Nuclear Power Plants (396/1991)

- Decision of the Council of State on the General Regulations for Emergency Response Arrangements at Nuclear Power Plants (397/1991)

- Decision of the Council of State on the General Regulations for the Safety of a Disposal Facility for Reactor Waste (398/1991).

The general regulations 395/1991, 396/1991 and 397/1991 are applied to a nuclear power plant which is defined to be a nuclear facility equipped with a nuclear reactor and intended for electricity generation, or if such or other nuclear facilities have been placed on the same site, the entity of facilities formed by them. The general regulations are also applied to other nuclear facilities to the extent applicable.

Detailed safety requirements are provided in YVL Guides. YVL Guides also provide administrative procedures for regulation of the use of nuclear energy. YVL Guides are issued by Radiation and Nuclear Safety Authority (STUK), as stipulated in the Nuclear Energy Act. YVL Guides are rules an individual licensee or any other organisations concerned shall comply with, unless some

other acceptable procedure or solution has been presented to STUK by which the safety level laid down in an YVL Guide is achieved. Taking into account Sections 27 and 28 of Decision 395/1991, STUK may decide that some new requirements are not applied to a nuclear power plant unit already in use.

The legislation also provides the regulatory control system for the use of nuclear energy. According to Section 55 of the Nuclear Energy Act, STUK is responsible for the regulatory control of the safety of the use of nuclear energy. The rights and responsibilities of STUK are provided in the Nuclear Energy Act. Safety review and assessment as well as inspection activities are covered by the regulatory control.

Furthermore, the Nuclear Energy Act defines the enforcement system and rules for suspension, modification or revocation of a license. The enforcement system includes provisions for executive assistance if needed and for sanctions in case the law is violated.

4.4.3.1.2 Regulatory Bodies

According to Section 54 of the Nuclear Energy Act, the overall authority in the field of nuclear energy is the responsibility of the Ministry of Trade and Industry. The Ministry prepares matters concerning nuclear energy to the Council of State for decision-making and, to some extent, grants import and export licenses for nuclear equipment and materials. Among other duties, the Ministry of Trade and Industry is responsible for the formulation of a national energy policy.

STUK is an independent governmental organisation for the regulatory control of radiation and nuclear safety. The current Act on STUK was given in 1983. STUK is administratively under the Ministry of Social Affairs and Health.

It is emphasised that the regulatory control of the safe use of nuclear energy is independently carried out by STUK. STUK has no responsibilities or duties which would be in conflict with regulatory control.

The responsibilities and rights of STUK, as regards the regulation of the use of nuclear energy, are provided in Sections 55 and 63 of the Nuclear Energy Act. They cover the safety review and assessment of license applications, and the regulatory control of the construction and operation of a nuclear facility. The regulatory control of nuclear power plants is described in detail in Guide YVL 1.1 issued by the Finnish Centre for Radiation and Nuclear Safety as the Regulatory Authority for the Use of Nuclear Energy.

STUK does not grant any construction or operating licenses for nuclear facilities. However, in practice no such license would be issued without STUK's statement where the fulfillment of the safety regulations is confirmed.

STUK has the legal authority to carry out regulatory control. STUK has e.g. legal rights to require modifications to nuclear power plants, to limit the power of plants and to require shutdown of plants when necessary for safety reasons.

STUK receives the main part of its financial resources through the government budget. The costs of regulatory control are charged in full to the licensees, but they are re-imbursed to the government. This means in practice that STUK is not financially dependent on licensee solvency.

An Advisory Committee on Nuclear Safety has been established by a decree. This Committee gives advice to STUK on important safety issues and regulations. In addition, an Advisory Committee on Radiation Safety has been established for advising the Ministry for Health and Social Affairs. The members of these Committees are nominated by the Council of State.

The main technical support organisation of STUK is the Technical Research Centre of Finland (VTT). In VTT, about 150 experts are working in the field of nuclear energy.

4.4.3.1.3 Standardisation Bodies

Detailed safety requirements are provided in YVL Guides. YVL Guides also provide administrative procedures for regulation of the use of nuclear energy. YVL Guides are rules an individual licensee or any other organisations concerned shall comply with, unless some other acceptable procedure or solution has been presented to STUK by which the safety level laid down in an YVL Guide is achieved.

4.4.3.1.4 Recognised User Groups

The YVL guides are reviewed by the Advisory Committee on Nuclear Safety before they are issued by STUK.

4.4.3.1.5 Discussion

In the pre-examination material delivered by the licensee to STUK before construction or modification of the plant, the licensee shall precisely define the standards applied during the computer system production process.

4.4.3.2 Germany

4.4.3.2.1 Background

In the nuclear sector regulation started in the late fifties with the construction and operation of the first German nuclear research reactors and facilities. The basis of the regulation is still the atomic energy law, which was made at the same time.

Nuclear regulation in Germany is mainly under the responsibility of the state governments (see section below on regulatory bodies) with the global regulatory directives being issued by the federal government. The federal government as well as the state governments contract expert organisation to assist them in technical questions. On the federal government level this role is mainly taken by the GRS, the Gesellschaft für Reaktorsicherheit, whereas on the state government level the TÜV organisations of the particular states and others are contracted to assist the governments. The federal government also established an advisory commission for reactor safety, the so called Reaktor-Sicherheits-Kommission (RSK) with senior experts recruited individually cross country. Parties mentioned above are involved in the standardisation process by sending individual members to the national nuclear standardisation body (KTA), the nuclear specific working groups of the DKE and the international standardisation organisations like IEC. Through appointment of the federal government, German experts participate in the IAEA work.

4.4.3.2.2 Regulatory Bodies

The general directives for nuclear regulation in Germany are issued by the federal government, Department of Environmental Protection. Detailed regulation and law enforcement is the task of the state governments. The state governments carry out authoritative acts by themselves and contract technical expert organisations, mainly TÜV organisations, for detailed technical supervision and inspection on site in the nuclear power plants.

Both on the level of the federal government and the state governments the departments of Environmental Protection take over nuclear regulation.

The responsibility for regulation has not changed significantly over the years.

4.4.3.2.3 Standardisation Bodies

The framework for nuclear regulation is the German Atomic Energy Law. The RSK-Guidelines define the overall requirements for the design, construction and operation of nuclear power plants. The KTA-Rules refine the requirement

for the individual sectors. In addition to these nuclear specific standards common standards have to be applied whenever there are no specific nuclear standards. In general, application of state-of-the-art technology is required by the authorities.

The Kerntechnische Ausschuß (KTA) is the nuclear specific standard organisation of Germany. Besides that there are sector specific working groups in DKE.

The relevant national standards of the Deutsches Institut für Normung (DIN) and other specific technical standardisation bodies (e. g. Verband deutscher Elektrotechniker) and relevant international standards e.g. of the IEC are also taken in account.

4.4.3.2.4 Recognised User Groups

There is the Technische Vereinigung der Großkraftwerksbetreiber VGB (Association of Power Plant Operators), which publishes technical recommendations for nuclear power plants.

4.4.3.2.5 Discussion

As with other sectors, the delegation of responsibility for regulation from federal government to the individual states and the role of technical expert organisations, such as mainly the TÜV organisations, in carrying out detailed technical supervision and inspection on site in the nuclear power plants, is unique to Germany.

In common with the worldwide trend, there is a moratorium on the construction of new nuclear power plants in Germany.

4.4.3.3 The United Kingdom

4.4.3.3.1 Background

Prior to the announcement of the first civil nuclear power programme in 1955, control of the development of nuclear energy was mainly applied through the Atomic Energy Act 1946 and the Atomic Energy Authority Act 1954.

After the start of the nuclear power programme, legislation was enacted to give powers for the regulation of nuclear safety. This resulted in the Nuclear Installations (Licensing and Insurance) Act 1959 and the Radioactive Substances Act 1960. The Nuclear Installations Act 1959 was succeeded by the Nuclear Installations Act 1965, which included amendments to take account of the international conventions on legal liability. The 1965 Act was subsequently amended by the Nuclear Installations Act 1969 to take account of certain changes to liability arrangements and to increase the financial limits on liability. The two Acts are known collectively as the Nuclear Installations Acts 1965 and 1969.

The Health and Safety at Work Act 1974 established the Health and Safety Commission and its enforcing arm, the Health and Safety Executive. The Act, and regulations made under it, transferred functions connected with the licensing, inspection and accidents at nuclear licensed sites from the Secretaries of State to the Health and Safety Executive.

4.4.3.3.2 Regulatory Bodies

Responsibility for the licensing and inspection of nuclear power stations rests with the Health and Safety Executive. Both those functions are carried out by the Nuclear Installations Inspectorate (NII), part of the Nuclear Power Division of the Health and Safety Executive. The Inspectorate employs qualified inspectors whose duties are to assist in the detailed application of the Nuclear Installations Acts 1965 and 1969, and to assure themselves that the conditions of nuclear site licenses are observed.

4.4.3.3.3 Standardisation Bodies

In the UK, the national standards body the British Standards Institute (BSI) has a nuclear standards group. The group combines the development of national standards with participation in the work of the IEC and European nuclear standards committees.

The HSE and the NII develop and issue guidance documents relating to regulatory and licensing issues.

Standards, still some of which are still relevant, have also been developed in the past by the United Kingdom Atomic Energy Authority (UKAEA) and by the Central Electricity Generating Board (CEGB).

4.4.3.3.4 Recognised User Groups

The Civil Nuclear Power Industry in the United Kingdom evolved from the work carried out in support of the military applications of nuclear fusion and fission processes. In 1954, the United Kingdom Atomic Energy Authority (UKAEA) was established by an Act of Parliament, charged with developing the peaceful use of nuclear power and with establishing the means to achieve the generation of electricity from civil as rather than military nuclear power plants. From that point on, until the privatisation and deregulation of the UK electrical power industry started in 1991, the nuclear power industry in the UK was in the hands of government owned organisations. In England and Wales, the Central Electricity Generating Board (CEGB) had sole responsibility for nuclear power generation and in Scotland, the South of Scotland Electricity Board (SSEB) had the same responsibility. Over the years research and development work carried out by the UKAEA and by the CEGB and SSEB at their own research laboratories provided guidance on good working practice for the design, construction and operation of nuclear power plants. The construction of the UK nuclear power plants was initially shared among competing companies but the size of the market was not large enough to support more than one company and a single construction company, the National Nuclear Construction company (NNC) was eventually created. Various Working Parties were established to bring together the expertise of these different government organisations and in a sense these working parties represented at the time the nearest equivalent to recognised user groups for the UK nuclear industry. The work carried out by these working groups and by the research departments in the various organisations resulted in the production of de facto standards and guidelines which were adopted within the UK nuclear industry. Most of the standards and guidelines came into being prior to there being any other National or International standards on the relevant topics. One example of such a standard is:

CEGB Specification DN5, Radio frequency interference susceptibility testing of electronic equipment. This is currently still the defining requirement for EMC testing of electronic equipment, including computer based equipment for use on UK nuclear power plants.

Since a license to operate a nuclear power plant in the UK is given only after the regulator has been satisfied as to the acceptability of the safety case prepared and presented by the applicant utility, it remains the responsibility of the utility to ensure that any changes to the plant or its mode of operation does not impact adversely on the established safety case. As part of the process of maintaining the integrity of the safety case, the responsible utility

will place strict requirements on suppliers of computer based electronic equipment and thus the utilities themselves represent the single most important recognised user group for the UK nuclear industry.

4.4.3.3.5 Discussion

Despite the privatisation of the nuclear power generation industry in the UK, little has changed in the regulatory and standardisation environment since the business as previously organised and run was moved as a single entity from the public to the private sector.

The most recently commissioned nuclear power plant in the UK was Sizewell "B" which went into full commercial operation in 1995.

4.4.3.4 The United States of America

4.4.3.4.1 Background

The Atomic Energy Act of 1946 established the five-member Atomic Energy Commission (AEC) to manage the nation's atomic energy programmes creating a virtual government monopoly of nuclear technology.

In 1954, Congress passed new legislation that for the first time permitted the wide use of atomic energy for peaceful purposes. The 1954 Atomic Energy Act redefined the atomic energy programme by ending the government monopoly on technical data and making the growth of a private commercial nuclear industry an urgent national goal.

The AEC's regulatory staff, created soon after the passage of the 1954 Atomic Energy Act, established procedures for licensing privately-owned reactors. The 1954 act outlined a two-step procedure for granting licenses. If the AEC found the safety analysis submitted by a utility for a proposed reactor to be acceptable, it would issue a construction permit. After construction was completed and the AEC determined that the plant fully met safety requirements, the applicant would receive a license to load fuel and begin operation.

The Advisory Committee on Reactor Safeguards (ACRS), composed of part-time consultants who were recognised authorities on various aspects of reactor technology, conducted its own independent review of the application.

In 1957, Congress passed the Price-Anderson bill. The Act provided insurance protection to victims of a nuclear accident, but included reforms of the AEC's licensing procedure.

In 1969 Congress passed the National Environmental Policy Act (NEPA) required federal agencies to consider the environmental impact of their activities.

In 1974, Congress passed the Energy Reorganisation Act which divided the AEC into the Energy Research and Development Administration and the Nuclear Regulatory Commission (NRC). This Act, coupled with the 1954 Atomic Energy Act, constituted the statutory basis for the NRC. The Nuclear Regulatory Commission began its operations as a separate agency in January 1975.

4.4.3.4.2 Regulatory Bodies

Responsibility for regulating activities in the nuclear sector in the USA is vested in the NRC. The NRC is an independent agency of the US federal government. In common with all other sectors the primary legal basis for regulatory enforcement is through the provisions embodied in the Code of Federal Regulations (CFR). Those directly affecting the use of computers in safety-related applications in the nuclear industry are mainly contained in Title 10. The most relevant being 10CFR50.59 relating to the carrying out of a modification to the plant or process. Compliance with the relevant clauses within the Code is a legal requirement with penalties for non-compliance being levied by the NRC.

In addition to the provisions contained within the CFR, the NRC issue as and when appropriate documents relating to nuclear regulation (NUREG's). These in general are guidance documents prepared as an aid to compliance and report research findings and studies into relevant topic areas.

Within the NRC the Control and Instrumentation (C&I) Branch is responsible for matters relating to the use of computers in safety-related applications. The license to construct and operate a nuclear facility is granted by the NRC. The operation of and any alterations to the facility is continuously monitored and reviewed by the NRC. In the field NRC staff are present at each individual facility. The field inspectors are organised into five regions.

The review process adopted by the NRC is documented in the Standard Review Plan (SRP) with C&I being covered in Chapter 14. In addition to the detail provided in the SRP, the NRC will from time to time issue Generic Letters relating to concerns relating to a significant number of nuclear facilities. They also issue statements giving the C&I Branch position on specific topic areas and issues.

4.4.3.4.3 Standardisation Bodies

There are a number of organisations which develop standards for the nuclear industry in the USA.

ANSI - the American National Standards Institute is the national standardisation body responsible for administering and coordinating the United States standardisation system.

ANS - the American Nuclear Society - develops standards and guidelines for use throughout the nuclear industry.

IEEE - the Institute of Electrical and Electronic Engineers - develops standards and guidelines relating to the use of electrical and electronic equipment. It also develops nuclear sector specific guidelines and standards.

ISA - the International Society for Instrumentation and Control, previously the Instrumentation Society of America - develops standards and guidelines for the nuclear industry in the field of instrumentation and control.

ASME - the American Society of Mechanical Engineers - develops nuclear standards relating to mechanical properties and equipment.

4.4.3.4.4 Recognised User Groups

INPO - the Institute of Nuclear Plant Operators is a self regulating body funded by the utilities and seeks to achieve improvements in the safe and economic operation of nuclear power plants in the US. Both INPO and NRC give performance ratings to individual power plants. A low rating whether given by NRC or INPO can adversely effect the economic performance of a plant. The plant will suffer from the threat of higher insurance premiums and from the cost of more frequent and more intensive inspections.

NEI - the Nuclear Energy Institute is effectively the US nuclear industry's trade association situated in Washington DC. This organisation, previously called NUMARC, interfaces with the USNRC on behalf of the industry where generic matters are concerned. It is funded by and works for the utilities to address regulatory concerns and is actively working with the industry and NRC to try to reduce the regulatory burden on O&M costs.

EPRI - the Electric Power Research Institute is as the name suggests an organisation setup and funded by the utilities to carry out research activities for the benefit of the industry. Through various steering committees the utilities agree with EPRI the direction and content of the forward work programme. Together with NEI, EPRI prepares technical reports on relevant topic areas as an aid to compliance and seeks to have these reports endorsed by the NRC.

Of the 100 currently operating nuclear power plants approximately one half are Pressurised Water Reactors (PWR's) supplied by Westinghouse and one third are Boiling Water Reactors (BWR's) supplied by General Electric. The remainder are PWR's supplied by Combustion Engineering, now owned by ABB and renamed ABB-CE and by Babcock and Wilcox now owned by Framatome. There is an active users group for each of the four vendors.

In addition there are meetings held between C&I engineers from each of the plants in the NRC regions. These are known as Set Point Committees and they typically address concerns raised by the local regional NRC Inspectors.

4.4.3.4.5 Discussion

The regulatory agencies in the USA operate within a very complete and well defined legal framework. The procedures for rule-making and the subsequent incorporation of a rule, once finalised, into the Code of Federal Regulations (CFR) is clearly laid down, allowing time for public comment. In the nuclear sector, a license to operate a plant lays down that the licensee must operate the plant within the Technical Specifications defining the parameters used in the Final Safety Analysis Report to determine the safety of the plant design and must comply with all relevant sections of the Code of Federal Regulations.

A supplier wishing to have an item of equipment approved by the USNRC for use on a nuclear power plant can submit a Topical Report, describing the equipment its application area and its performance to the NRC with a request for a safety evaluation. The USNRC will respond by issuing a Safety Evaluation Report (SER) which will indicate the NRC view of the submitted equipment.

4.5 Process Industries

4.5.1 International

4.5.1.1 Background

The process industries sector is arguably the oldest, longest established industrial sector. As such, custom and practice plays a large part in determining the nature of safety features deployed on plants and processes. This also leads to differences in approach between countries and between companies. Over the years there has been a large measure of self-regulation with the establishment within individual companies of internal regulations and procedures for ensuring the safety of plants and processes. As companies have become more multinational, these internal guidelines and procedures have been modified to cover the range of countries over which the company has operating plants.

4.5.1.2 Regulatory Bodies

There are no identified international regulatory bodies or licensing authorities for this sector

4.5.1.3 Standardisation Bodies

There is no international body specific and exclusively devoted to the development of standards for the process industries. There is however a subgroup within IEC SC65 which is actively developing a sector specific standard, IEC 61511, under the generic standard IEC 61508, specifically for the process industries sector.

4.5.1.4 Recognised User Groups

The International Council of Chemical Associations (ICCA) is a council of leading trade associations representing chemical manufacturers worldwide.

4.5.1.5 Discussion

The process industries have always operated in a highly competitive marketplace. The difficulties inherent in reconciling the goal of achieving best economic performance with the need to ensure adequate levels of safety in such a competitive environment have produced individual company internal selfregulatory guidelines which are fiercely defended to ensure continued competitive advantage. Nevertheless, with companies having operating plants spread over a number of countries worldwide coupled with the global

nature of the marketplace there is a growing move to support international standard making for this sector.

4.5.2 European

4.5.2.1 Background

Within Europe the process industry is subject to European Commission directives in relation to the operation of plants and processes. All member nations of the European Union are bound by these directives, but can apply further national regulations. National associations represent the process industries within an individual country, interfacing between industry and government on matters impacting the industry. At the European level these national associations have grouped together to present a combined interface to the European Commission particularily in relation to the issuing of Directives.

4.5.2.2 Regulatory Bodies

While in Europe there is no regulatory body or licensing authority responsible for licensing and inspection of process industries the European Commission on behalf of the European Union does from time to time issue Directives which are binding on all the member countries. As an example the Seveso Directive had a significant and continuing influence on the safety regulation within Europe of the process industries.

4.5.2.3 Standardisation Bodies

At the European level standardisation activities are the responsibility of CEN/CENELEC. Matters of specific relevance to the process industries are delegated to particular technical committees e.g. CEN/TC 69 Industrial valves.

4.5.2.4 Recognised User Groups

The objective of the European Chemical Industry Council (CEFIC) is to provide a mechanism for structured discussion of issues affecting chemical companies operating in Europe and to represent the industry's position on these issues in order to contribute to the legislative decision-taking process.

4.5.2.5 Discussion

Harmonisation of standards and practices within Europe in the process industries sector is progressing in-line with work being carried out at the international level. European regulation at the level of European Directives is fully functional.

4.5.3 National

4.5.3.1 Germany

4.5.3.1.1 Background

Germany in common with other member countries of the European Union is bound by European Commission Directives. Where Germany differs from other member countries in the EU is in the extent to which regulatory control of the process industries sector is devolved to the individual states within Germany. Thus there exists in Germany regulation at the European level, regulation at the federal government level and regulation at the level of the individual states.

Germany has a well established environment for the development of standards.

4.5.3.1.2 Regulatory Bodies

Federal ministry responsible for safety and environment is

> Ministerium für Umwelt, Naturschutz und Reaktorsicherheit (Ministry for Environment, Environmental Protection and Reactor Safety)

However responsibility for regulation and licensing rests on authorities in the different states.

Responsibility for licensing and inspection rests on following authorities:

- Gewerbeaufsichtsamt
- Amt für Arbeitschutz
- Bezirksregierung

The authorities normally do not have sufficient qualified inspectors; they mainly are involved in the licensing procedures from the administrative point of view. For technical inspections they subcontract testing organisations, like TÜV (Technische Überwachungsvereine) or Germanischer Lloyd (for off-shore equipment).

These authorities grant license for the operation of plants in the process industry. Grants are normally time limited and demand regular inspection (done by third party testing organisations).

4.5.3.1.3 Standardisation Bodies

The standardisation bodies that are relevant in the computer area are:

- DIN (Deutsches Institut für Normung): produces binding standards for all sectors of daily life, including technical applications

- NAMUR (Normenausschuß Meß- und Regeltechnik, Committee for standardisation of I&C systems in chemical industry); this committee produces standards and guidelines for I&C systems; these are 'voluntarily' binding since they are no 'official' standards. But the intention is to transfer the NAMUR ideas and procedures into national and European standards.

- DKE, Deutsche Elektrotechnische Kommission, for industrial computer applications in general

4.5.3.1.4 Recognised User Groups

Chemical Industry Federations;

- Verband der Chemischen Industrie

Plastics Industry Federations;

- VKE: Verband Kunststofferzeugende Industrie

- GKV: Gesamtverband Kunststoffverarbeitende Industrie

Organisations producing guidelines for users;

- Verein Deutscher Ingenieure, Institute of German Engineers

- VDE, Verband der Elektrotechnik, Elektronik, Informationstechnik e.V., Institute of German Electro Technicians

- GMA, Gesellschaft Meß- und Automatisierungstechnik, Association for Automatic Control

4.5.3.1.5 Discussion

The way in which regulatory activities are distributed between federal government and the governments of the individual states is unique to Germany. The status and role of testing organisations within the overall regulatory framework is also unique to Germany. Nevertheless there exists extensive similarities to regulatory and standardisation environments of other countries both within the European Union and worldwide.

4.6 Electric Power Industry

4.6.1 International

4.6.1.1 Background

Safety as a crucial issue of computer applications in such fields as nuclear power stations, space industry, chemical industry, aircraft industry, or railways are well recognised by a wide spectrum of experts in these fields as well as by software and computer systems design community. Awareness of the dependability issues associated with application of computer-based control systems in electric power industry is much less popular. A very small number of publications on the above mentioned subjects, also those present in conference proceedings, journals and books on electric power systems, is conductive to keep such a state.

Electric power industry consists of many different companies involved in the generation of electric power, bulk transmission of energy from power stations to load centres and its distribution to customers. In order to perform their functions and to attain a suitable effectiveness, all units, such as generators, which are used for generation of electric power, transformers, switchgears, high-voltage lines and others components, in spite of the fact that they belong to various companies, are interconnected, forming an electric power system - EPS. Usually this interconnection is now the strongest at the national level, forming a national power system.

Safety related application of computer systems in electric power industry concern mainly some applications in power stations and application of computer control systems in substations and in EPS control centres.

In the most general terms EPS can be partitioned into generating stations and high-voltage networks known as grids. On the other hand, power networks consist of transmission networks or extra-high voltage (EHV) networks which are used to transmit power from generating stations to main load centres and distribution networks of lower voltages, known as high-voltage (HV) networks which are used to transmit power to customers. Both transmission and distribution networks consist of underground cables, overhead lines and substations.

Substations form vital nodes in the HV and EHV networks because, among others, they make possible modifications in the configuration of networks during the operation of the system by means of switching devices that can be controlled by computer-based control systems applied in the substations. Initiation of the control procedure may be performed locally by substation operators or remotely from the EPS control centres.

Safety in case of substation control systems has the following three aspects:

- safety of substation staff,

- safety of substation devices,

- safety of EPS.

Understanding of safety in item (1) and (2) is consistent with the most common understanding of safety considerations as, for instance, in railway applications.

Safety of EPS (item (3)) is a concept that is not determined by the capacity of individual generators, loads, or transmission lines. It is a property that has to be considered at the electric power system level.

Generally speaking, if all generators work synchronously and the voltage and the frequency in EPS is within the required limits, then this is a normal, stable state of an EPS. In case of sudden disturbances, e.g. sudden increase of the load, or disconnecting of an important transmission line due to a failure in a substation computer control system, the stable state of work is disturbed. Each EPS is designed with a certain stability margin. When the disturbance is greater than the stability margin it results in loss of stability and collapse of the EPS, which may be total, and this is called a black-out, or partial. Hazard for stability is equivalent to hazard for safety of an EPS, as economic and social results of the loss of stability by an EPS are always very serious. Major blackouts are rare events, but as it has been stated in one of the publications, their impact can be catastrophic. In fact the events are not so rare. Within the period of 1978-1985 there were 24 big system failures outside the United States and at least 2 in the United States. This is the reason why maintaining stability of an EPS is the main requirement for the EPS planning, operation and control.

Also security issues in EPS become more and more important. Until now computer security in EPSs was derived from traditional physical, administrative, communications, and personnel security techniques. Move from an architecture of "islands of computing" to a networked architecture, provide significant operational benefits for electricity companies, however it also increases the exposure to modification and loss of data.

4.6.1.2 Regulatory Bodies

There are no international regulatory bodies for this sector.

4.6.1.3 Standardisation Bodies

The main standardisation body in this sector is IEC. Within IEC the standardisation procedures in the field of substation control are mainly dealt with by the Technical Committee No 57: Power system control and associated communications.

In the range under consideration the reports of works performed by their international Study Committees are also published by the International Conference on Large High Voltage Electric Systems (Conference Internationale des Grandes Reseaux Electriques a Haute Tension - CIGRE), a permanent non governmental and non profit-making international association founded in 1921 with the head office in Paris. Some reports, papers and guidelines published by the CIGRE Study Committees owing to the fact that they are based upon sound scientific and technical fundamentals and rather good knowledge of the current state of practices in the power industry on a world-wide scale, is treated by electric power system experts in a more or less formal way as guidelines of good practice.

From the formal point of view, the IEEE standards have not a nature of international standards but because of a sound industry and scientific knowledge on which the standardisation activities of IEEE are based in the field under consideration and participation of foreign experts in the standardisation activities of IEEE, in cases where there is not any international standard the IEEE standards in this field may be to a certain extent treated as guidelines for engineering solutions.

4.6.1.4 Recognised User Groups

- national regulatory authorities,

- electric equipment, computer systems and software manufacturers,

- consultants,

- electricity companies,

- industrial power consumers.

4.6.1.5 Discussion

Currently there is not any international standard dealing with design of computer-based control systems for EHV or HV substations. The documentation of the existing practices in the field of design and maintenance of the computer-based control systems used in the electric power industry that can be found in publications is very insufficient to obtain a clear image of these practices. These few existing publications, including CIGRE publications based upon a rather good knowledge of the existing practices,

provide a picture of fairly poor practices which could not rather yield a conclusion that the exhaustive analysis of the issues associated with application of computer systems in EHV substations has been carried out and there is a clear point of view on hazards and risks which are likely to take place. Also the publications, including those of CIGRE, contain remarks on gaps in the awareness that design and maintenance of software-based systems require an approach which differs significantly from conventional equipment.

In many countries, including most European countries, the electric power industry is currently undergoing considerable transformations related to privatisation and transition into the free market of electric power. The free market in power industry is a completely new issue, both in the engineering and organisational aspects. There are reasons to believe that this issue, including privatisation, is something which fully preoccupies the management and engineering staff of electricity companies.

One may believe that under these circumstances the issue of an international standard presenting in a possibly clear and detailed way the approach required for software based solutions might contribute to calling attention of the management of electricity companies to a new approach required by introduction of programmable systems. It seems that such a standard might be based upon the IEC 61508 standard.

4.6.2 European

4.6.2.1 Background

In Europe the interconnected power systems combining the systems of several countries have been operating for a fairly long time. The following interconnected systems are operating synchronously:

- UCPTE/CENTREL: Belgium, Germany, Spain, France, Greece, Italy, Slovenia, Croatia, Federal Republik of Yugoslavia, Former Yugoslav Republic of Macedonia, Luxembourg, The Netherlands, Austria, Portugal and Switzerland /Poland, Czech Republic, Slovakia and Hungary.

- NORDEL: Finland, Norway, Sweden and Denmark.

Energy related policy of the European Union aims to create an open and competitive electricity market in Europe (Directive 96/92/EC). This policy includes formation of trans-European networks.

4.6.2.2 Regulatory Bodies

For the EU countries these are the respective EU bodies which are authorised to set up the regulations in this field, such as European Parliament and Council of the EU.

4.6.2.3 Standardisation Bodies

Standardisation body for the EU countries is CENELEC - European Committee for Electrotechnical Standardisation. It has been officially recognised as the European standards organisation in its field by the European Commission in Directive 83/189 EEC. In its standardisation activities CENELEC closely co-operates with IEC.

4.6.2.4 Recognised User Groups

As in section. 4.6.1.4

4.6.2.5 Discussion

As in section 4.6.1.5

4.6.3 National

4.6.3.1 Poland

4.6.3.1.1 Background

Like in member countries of EU, the electric power industry in Poland is now in the period of large transformations resulting from privatisation of the electric power sector and creating the elements of the free energy market where power supplies and prices will be based upon commercial contracts and not on administrative orders.

In recent years intense and successful work has been carried out in the Polish electric power industry on connecting the Polish EPS with the West European systems cooperating within the framework of UCPT.

4.6.3.1.2 Regulatory Bodies

- Parliament

- Minister of Economy

4.6.3.1.3 Standardisation Bodies

- Polski Komitet Normalizacyjny - PKN (Polish Standardisation Committee)

4.6.3.1.4 Recognised User Groups

- electric equipment, computer systems and software manufacturers,

- consultants,

- electricity companies,

- industrial power consumers.

4.6.3.1.5 Discussion

Neither any standards nor legal regulations in the field under consideration have been issued in Poland. The awareness of differences in approach that is required in design and maintenance of programmable control systems with respect to the approach applied in the case of traditional solutions is rather low and limited to narrow circles. From what it was possible to establish, it appears that the data concerning failures of EPS equipment as well as failures

of the Polish EPS are not collected in a deliberate and systematic way which would make difficult e.g. any analysis of the computer system safety if one would like to apply such an analysis.

However, it should be noted that in spite of the above given facts very extensive measurements and tests performed in the Polish EPS in the period from 1993 to 1994 in connection with Polish efforts to interconnect the Polish EPS with UCPT showed that the qualities of the Polish system are good and fully satisfy UCPT requirements.

4.7 Security

4.7.1 International

4.7.1.1 Background

The Safety of Programmable Electronic Systems (PES) directly depends on the security of the PES including its environment. Security activities normally start with a Threat Analysis followed by a Risk Analysis. The Risk Analysis determines the security vulnerabilities and recommends security countermeasures. The security countermeasures can be grouped into:

Personnel	Recruitment Screening, Training
Procedural	Information security policies & procedures
Physical	Locks, access control, surveillance cameras, power supplies, cabling
Technical	Cryptographic techniques, Virus Controls, Media protection, Tokens

Physical security measures have a wealth of standards but these dependent on the environment within which the PES is contained and are not considered in this section. The majority of security standards for computer systems have been produced for Information Technology (IT) systems and networks which could be adopted for PES. Also standards are available or being produced for security management both procedural and technical such as the distribution of cryptographic keys. Many countries have schemes in place to evaluate the security functionality and its correctness of both products and systems by licensed third parties. This is normally required for government security applications but could also be used for the security of safety related systems.

Government and military organisations, such as NATO, have their own security standards but these have not been covered. Cryptographic standards are also being developed for sectors not involved in safety related systems but these standards such as those for digital signatures in e-commerce could be used for integrity measures in safety related systems.

Market leaders in IT systems, such as Microsoft, Intel, RSA and Netscape have developed proprietary protocols and interface specifications which are becoming de-facto standards. These proprietary standards have not been covered.

The provision of cryptographic techniques is also subject to legislation and export controls.

International security standards are produced by ISO/IEC 1/SC27 with inputs from National, American and European standards organisations. Work is also undertaken on security of the Global Information Infrastructure (GII) proposed by the G-7 members. OECD have also produced guidelines for cryptographic technology and its legislation.

4.7.1.2 Regulatory Bodies

Nations have their own regulation bodies which form bilateral agreements with other nations for the international acceptance of the accreditation and certification of security products and systems.

4.7.1.3 Standardisation Bodies

The main standardisation body for IT security is ISO/IEC JTC1 SC27. There are many other subcommittees (SCs) where security relevant standardisation is part of their work including:

SC1 Vocabulary

SC6 Telecommunications and Information Exchange Between Systems

SC7 Software Engineering

SC17 Identification Cards and Related Devices

SC18 Document Processing and Related Communications

SC21 Open Systems Interconnection (OSI)

SC22 Programming Languages, Environments and Systems

SC25 Interconnection of Information Technology Equipment

SC28 Office Equipment

SC30 Open EDI

In addition, there are a number of ISO and IEC groups that are also involved with security work including:

ISO/TC68 Banking Systems

IEC/TC65 Safety Related Control Systems

Other groups involved in security related standards activities include:

ATM Forum

IEEE Institute of Electrical and Electronic Engineers

IETF Internet Engineering Task Force

IFIP International Federation of Information Processing

ITU-T International Telecommunication Union formerly CCITT

NIST National Institute of Standards and Technology

Open Group

OMG Object Management Group

4.7.1.4 Recognised User Groups

IT system suppliers have their own trade groups, such as POSIX, defining security recommendations. IT application vendors defining their cryptographic interfaces include:

RSA : Public Key Cryptographic System (PKCS)

Netscape : Secure Sockets Layer (SSL) a standard by for establishing a secure communication link using a public key system.

Internet Engineering Task Force (IETF): S/MIME Secure Multipurpose Internet Mail Extensions; a protocol for sending secure e-mail.

Intel: Common Data Security Architecture (CDSA)

Standards for cryptographic techniques such as algorithms e.g. DES (Data Encryption Standard - the most common encryption algorithm with symmetric keys) and AES (Advanced Encryption Standard), digital signatures e.g. DSA (Digital Signature Algorithm - this algorithm uses a private key to sign a message and a public key to verify the signature. It is a standard proposed by the US government., RSA (Rivest, Shamir, Adleman - a public key cryptosystem invented by Ron Rivest, Adi Shamir, and Leonard Adleman), cryptographic key management are produced in the USA as 'FIPS PUB' documents.

4.7.1.5 Discussion

The Common Criteria (CC) for IT Security Evaluation is an effort by the governments of North American and European Nations to develop a common criteria for developing trusted IT products. CC Version 1.0 is undergoing international review and testing prior to being fully accepted within Europe and North America. When mature enough, the CC will be submitted to ISO SC27 WG3 as a contribution towards an international standard.

For information security management, the British Standard BS7799 has been put forward as an international standard.

4.7.2 European

4.7.2.1 Background

Security work in Europe has been on the European Information Infrastructure (EII) arising from the Bangman Report in the early '90s, the IT Security Evaluation Criteria (ITSEC) and the initiative for Secure Electronic Commerce involving the provision of Trusted Third Parties and Digital Signatures.

The ITSEC was the harmonisation of the criteria from France (Blue-White-Red Book – SCSSI), Germany (ZSIEC), The Netherlands and the UK (DTI Green Books). The criteria cover the requirements for security functions (functionality), the confidence of correctness of the implementation of the security functions (assurance correctness) and the confidence of the effectiveness of the security functions (assurance effectiveness). In October 1997, the UK, Germany and France have signed a Memorandum of Understanding to formally recognise products which have been certified against ITSEC in each country.

4.7.2.2 Regulatory Bodies

Nations have their own regulation bodies which form bilateral agreements with other nations for the international acceptance of the accreditation and certification of security products and systems.

4.7.2.3 Standardisation Bodies

The committees working on European Standards include:

CEN	European Committee for Standardisation
ECMA	European Computer Manufacturers Association
ETSI	European Telecommunications Standards Institute
EWOS	European Workshop on Open Systems
TEN	Trans-European Networks in Telecommunications

4.7.2.4 Recognised User Groups

No recognised user groups have been identified.

4.7.2.5 Discussion

While the signing in October 1997 by the UK, Germany and France of a Memorandum of Understanding to formally recognise products which have been certified against the IT Security Evaluation Criteria (ITSEC) in each country represents a significant move towards European harmonisation, much remains to be done. In particular matters relating to the legal acceptability of digital signatures and the status of trusted third parties are currently the subject of on-going debate.

4.7.3 National

4.7.3.1 Germany

4.7.3.1.1 Background

In Germany the main organisations and institutions involved in the regulation and standardisation are:

Ministry of Interior and German Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik, GISA) for policy and regulations

Ministry of Economics and Federal Office of Economics (Bundesamt für Wirtschaft) for policy and export controls

DIN - Group (Deutsche Industrie Norm)

ZKA (Zentraler Kreditausschuß); Organisation of all banks in Germany

The main areas of work in Germany are:

ITSEC Scheme

Contribution to Common Criteria (CC)

Legal foundation of the Digital Signatures

The Federal German government initiated a Digital Signature Act (SigG) via a cabinet decision at the end of 1996, with the legislation subsequently coming into force on 1st August, 1997.

This Act is intended to prevent a proliferation of uncontrolled standards, to regulate the organisation of the required infrastructure, such as the certification authorities, and in this way to lay down the general conditions for practical introduction of the digital signature on a broad basis. In particular, this legislation establishes the essential basis for safeguarding the rights of individual participants in electronic legal transactions. In a further step, it will then be possible to draw up statutory regulations for legal issues relating to digital signatures.

The present safeguard catalogues for digital signatures have been drafted by the German Information Security Agency. They describe how the individual technical components and the organisational environment are to be configured and structured in order to achieve an overall system in which

digital signatures can be created which possess the necessary degree of security to prevent forgery and manipulation.

4.7.3.1.2 Regulatory Bodies

In Germany Information Security Evaluation is carried out under the ITSEC scheme which is managed by the Bundesamt für Sicherheit in der Informationstechnik (GISA). The scheme was established with the goal of meeting the requirements of government and industry for IT security evaluation and certification and providing a basis for international recognition of evaluation certificates. Evaluations are carried out by independent Evaluation Facilities, accredited by the Certification Body GISA, after undergoing rigorous accreditation procedures. After a successful evaluation, the Certification Body can issue the certificate.

Since the beginning of 1998 private Certification Bodies under ITSEC are recognised officially. Similar to the Evaluation Facilities they have to undergo certain accreditation procedures controlled by GISA.

4.7.3.1.3 Standardisation Bodies

The German national standardisation body is the Deutsche Industrienorm (DIN). DIN is a member of CEN and ISO.

4.7.3.1.4 Recognised User Groups

No recognised user groups have been identified.

4.7.3.1.5 Discussion

The current main activities in Germany are the implementation of the infrastructure for the Digital Signature and the realisation of procedures for the new criteria CC. The Digital Signature Act requires a whole set of certified technical components as well as officially recognised trusted third parties that are allowed to administer keys etc.. The root Trust Centre will be the Regulierungsbehörde für Telekommunikation und Postwesen (RegTP, the successor institution of the Ministry of Post).

4.7.3.2 The United Kingdom

4.7.3.2.1 Background

Within the United Kingdom the organisations involved in the regulation and standardisation include:

Department of Trade & Industry (DTI) for policy and export controls

British Standards Institute (BSI)

Communications Electronics Security Group (CESG) who jointly manage ITSEC

The main activities in the UK are:

UK ITSEC Scheme

BS7799 : The Code of Practice for Information Security Management

DTI Secure Electronic Commerce Statement

A Code of Practice for Information Security Management was developed by the DTI, industry and the BSI. The code of practice was developed as a result of industry, government and commerce demand for a common framework to enable organisations to develop, implement and measure effective security management practice and to provide confidence in inter-company trading. It is based on the best current information security practices of leading British and international businesses and has met with international acclaim. In 1995, the Code of Practice became the UK BS 7799 standard and in 1996, a scheme for certification against BS 7799 was developed by the DTI, industry, the UK Accredited Certification Service (UKAS) and the BSI.

4.7.3.2.2 Regulatory Bodies

Information Security Evaluation in the UK is carried out under the UK ITSEC scheme which is jointly managed by the DTI and CESG. The scheme was established in 1990, with the objectives of meeting the needs of government and industry for IT security evaluation and providing a basis for international recognition of evaluation certificates. Evaluations are carried out by five independent third parties, known as Commercial Licensed Evaluation Facilities (CLEFs), appointed by the Certification Body of the Scheme, after meeting rigorous security and quality standards. After a successful evaluation, the Certification Body can issue the certificate. A Certification

Maintenance Scheme (CMS) enables vendors to maintain the certified status of their products using approved procedures.

The accredited certification scheme for BS 7799, c:cure, was launched on 28th April 1998 and is being developed DISC (Delivering Information Solutions to Customers through International Standards) part of the BSI. DISC provides seminars on BS 7799 and certification and has produced documents to support the scheme. UKAS are developing the criteria, based on ISO/IEC Guide 62, to accredit an organisation to undertake BS 7799 certifications. The scheme to certificate auditors with optional training courses and an examination is presently being developed. The examination will be followed by an interview with a panel. There are three grades of BS 7799 auditor: Provisional BS7799 Auditor, BS 7799 Auditor and Lead BS 7799 Auditor.

4.7.3.2.3 Standardisation Bodies

The national standardisation body for the United Kingdom is the British Standards Institute (BSI). BSI is a member of CEN and ISO.

4.7.3.2.4 Recognised User Groups

A BS 7799 User Club has been set up by the DTI whose aims are to promote the dissemination of good information security management practice, including the use of BS 7799 and the accreditation certification scheme for BS 7799.

4.7.3.2.5 Discussion

BS 7799 is presently being revised and a new version is expected at the end of '98 or early '99. In order to prepare for such a revision the UK held a consultation process to seek a broader opinion on this revision. Proposed new areas for the standard included encryption, firewalls, electronic trading, handling of documents, risk assessment, business continuity planning, owner/user responsibilities, record retention, mobile computing, electronic archiving and third party certified products. Also being considered is a three level hierarchy of documents with a management overview at the top level, BS 7799 at the next level and the lower level being sector specific implementations of BS 7799.

In April '98, the DTI produced the Secure Electronic Statement which proposed the introduction of legislation to licence bodies providing or facilitating the provision of cryptographic services, Trusted Third Parties (TTPs). The legislation is scheduled to start its passage through the UK Parliamentin 1999. The legislation is split into the legal recognition of digital signatures, the voluntary licensing of TTPs and the provision of lawful access to information by law enforcement agencies.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

5.1.1 General

There are many similarities in the regulatory and standardisation environments of the countries included in the study. In all cases the primary responsibility for regulatory control is with internal departments (Ministries or Departments of State) of the government of the country. All regulation is handled nationally. This is also the case within the European Union although all member countries comply with the requirements of relevant European Directives. In the medical device area, a harmonised approach is taken in the EU, with certification being accepted across borders.

The standardisation environment is typically structured with a national standardisation body for each country interfacing with ISO internationally and in the case of European Union countries with CEN, and with a second national body (or a designated body in association with the primary national standardisation body) interfacing with IEC and within the European Union with CENELEC. Additionally national engineering institutes and other professional bodies provide further efforts in the development of national and international standards.

There are also some differences. Within the European Union, Germany delegates responsibility for regulation to the governing bodies of the individual states within Germany with primary responsibility in an overseeing role being retained at the level of the federal government. In the USA which also has a system of federal and state administration more responsibility for regulation is retained at the federal level. The USA has in place a well established legal framework for regulation with the Code of Federal Regulations setting down in considerable detail the legal requirements for regulatory compliance. An adherence to requirements detailed in rules embodied in legal instruments is also a feature of the regulatory environments of Germany and the Netherlands, while in the United Kingdom for example, more emphasis is placed on the strength and legitimacy of a submitted safety case.

In all of the countries, use is made within the regulatory environment of third party independent assessment and testing. There are however differences between the countries on the approach towards certification and of the extent of use of such bodies. In particular the results of a third party assessment or testing activity may not be recognised outside the country or sector originally involved. Within the European Union, the concept of notified bodies is achieving a measure of harmonisation within Europe in this regard.

5.1.2 Medical Devices

Regulation and standardisation of the medical devices sector is still developing both within Europe and worldwide. The international scene is dominated by the USA and the EU. It seems that what receives approval in these countries is also very likely to be approved in other countries worldwide. This is especially true as long as the basis for approval is the international standards from IEC and ISO.

Unlike more established sectors, there was not a strongly national regulatory and standardisation environment in place prior to the establishment of the European Union. The starting point for regulation and standardisation of the medical devices sector within Europe is the issuing of European Directives and the work of CEN/CENELEC. This should lead to a harmonised European approach from the very beginning.

In the USA the regulation of medical devices is the responsibility of the Federal Food and Drugs Administration (FDA). In the USA, a classification of devices is being done in three classes, while in the EU there are four classes. In order to make the exchange of goods easier between the USA and the European Union, it is anticipated that the regulations being outlined in the European Union e.g. in the Medical Device Directive of the EC, will be harmonised with those of the FDA.

5.1.3 Rail Operation

A common theme in the rail sector in all of the countries in the study was that the national rail system had either undergone privatisation or was under notice to do so. This had impacted on both the regulatory and the standardisation environments. Efforts had been made in all cases to keep the two environments as far as possible unchanged through the privatisation process. This had largely been achieved but a process of adaption to meet the changed conditions is in hand.

Modern technological developments have resulted in a close interaction between train control systems and signalling systems. This is particularily true of systems involving the use of computers. Traditionally standards relating to signalling were developed separately to those related to train

control. While harmonisation of standards between countries within the European Union is being pursued within the rail sector through sector specific committees under CEN/CENELEC, there still remains the split of responsibilities separating signalling from train control. This is a problem area which will become more marked as the move to greater automatic control of trains leads to greater interaction and interdependence between the signalling systems and the onboard train controllers.

5.1.4 Nuclear Industry

The nuclear power industry is arguably the most strictly regulated of all industries. The impact of a nuclear accident can cross national boundaries. Since the Chernobyl accident there has been increased international collaboration in the field of nuclear power plant operation and safety. There is however no single international body charged with regulating the safety of nuclear power plants. The United Nations in conjunction with the IAEA maintain a monitoring and regulatory role in relation to the production of fissile materials.

Each of the European countries having operating nuclear power plants has a regulatory organisation to monitor and license its own nuclear plants. At the European level issues such as siting of new nuclear plant and facilities when emissions could cross national boundaries are addressed.

5.1.5 Process Industries

The process industries have always operated in a highly competitive marketplace. The difficulties inherent in reconciling the goal of achieving best economic performance with the need to ensure adequate levels of safety in such a competitive environment have produced individual company internal self-regulatory guidelines which are fiercely defended to ensure continued competitive advantage. Nevertheless, with companies having operating plants spread over a number of countries worldwide coupled with the global nature of the marketplace there is a growing move to support international standard making for this sector.

5.1.6 Electric Power Industry

Safety related application of computer systems in electric power industry concern mainly some applications in power stations and application of computer control systems in substations and in EPS control centres.

Currently there is not any international standards dealing with design of computer-based control systems for EHV or HV substations. The documentation of the existing practices in the field of design and maintenance of the computer-based control systems used in the electric power

industry that can be found in publications is very insufficient to obtain a clear image of these practices.

In many countries, including most European countries, the electric power industry is currently undergoing considerable transformations related to privatisation and transition into the free market of electric power. Under these circumstances guidance on the use of computer based systems in safety related applications is likely to be welcomed by the management of electricity companies. Such a guidance document for the electric power industry would most likely now be based upon the IEC 61508 standard.

5.1.7 Security

Security is, of course, more properly an attribute like safety which would apply across all industrial sectors. Indeed security is a topic area covered in the standardisation and regulatory environments for safety related systems which currently exist in all countries and sectors addressed in this report. However, many of the aspects of standardisation and regulation relating to security matters have historically been addressed by a distinctively separate community of experts. Topics such as cryptographic standards are being developed for sectors not involved in safety related systems but these standards such as those for digital signatures in e-commerce could be used for integrity measures in safety related systems.

The Common Criteria (CC) for IT Security Evaluation is an effort by the governments of North American and European Nations to develop a common criteria for developing trusted IT products. CC Version 1.0 is undergoing international review and testing prior to being fully accepted within Europe and North America. When mature enough, the CC will be submitted to ISO SC27 WG3 as a contribution towards an international standard.

For information security management, the British Standard BS7799 has been put forward as an international standard.

5.2 Recommendations

The study carried out provides a brief outline of the regulatory and standardisation environments relating to the use of computer based systems in safety related applications in a selected number of sectors and countries. The study concludes that there are a great many similarities in the regulatory and standardisation environments in the sectors and countries studied but that differences also exist.

As a result of the outcome of the work carried out under Stage I of Phase II of the Road map project, the following recommendations are made for work to be carried out under Stage II of Phase II:

That confirmation of the correctness of the descriptions of the regulatory and standardisation environments for the selected sectors and countries should be obtained by a direct approach to the relevant regulatory bodies.

That the role of standards in the regulatory process should be studied in collaboration with the relevant regulatory bodies and that, as part of the exercise, the regulatory bodies should be asked to identify those standards and guidance documents that they:

1. Mandate or require compliance with.

2. Recommend or approve or endorse.

3. Consider relevant and informative.

6. APPENDICES

6.1 List of Countries ranked by Gross Domestic Product (GDP)[17]

Country	GDP for 1997 Billion US Dollars
United States of America	7819
Germany	2115
France	1393
United Kingdom	1287
Netherlands	363
Austria	206
Poland	137
Finland	118

[17] Source OECD annual national accounts publication

6.2 List of Sectors

Medical Devices

Rail Transportation

Nuclear Power Industry

Process Industries

Electric Power Industry

Security

6.3 Coverage matrix

	Medical Devices	Rail Transport	Nuclear Power Industry	Process Industries	Electric Power Industry	Security
Austria		X				
Finland			X			
France		X				
Germany	X	X	X	X		X
Netherlands	X	X				
Poland		X			X	
United Kingdom		X	X			X
United States	X		X			

6.4 Details of individual contributions

Section	Sector	Title	Name
		Abstract	Ian Smith
1.		Introduction	Ian Smith
2.		Background	Ian Smith
3.		Scope	Ian Smith
4.1.1	General	International	Ian Smith
4.1.2	General	European	Ian Smith
4.1.3.1	General	Austria	Erwin Schoitsch+Johannes Rainer
4.1.3.2	General	Finland	Jouko Järvi
4.1.3.3	General	France	Ian Smith
4.1.3.4	General	Germany	Wolfgang Ehrenberger
4.1.3.5	General	The Netherlands	Meine van der Meulen
4.1.3.6	General	Poland	Zdzislaw Zurakowski/Janusz Gorski
4.1.3.7	General	The UK	Ian Smith
4.1.3.8	General	The USA	Ian Smith
4.2.1	Medical	International	Udo Voges+Floor Koornneef
4.2.2	Medical	European	Udo Voges+Floor Koornneef
4.2.3.1	Medical	Germany	Udo Voges
4.2.3.2	Medical	The Netherlands	Floor Koornneef
4.2.3.3	Medical	The USA	Udo Voges
4.3.1	Rail	International	Erwin Schoitsch+Johannes Rainer
4.3.2	Rail	European	Erwin Schoitsch+Johannes Rainer

4.3.3.1	Rail	Austria	Erwin Schoitsch+Johannes Rainer
4.3.3.2	Rail	France	Erwin Schoitsch+Johannes Rainer
4.3.3.3	Rail	Germany	Ferdinand Dafelmair
4.3.3.4	Rail	The Netherlands	Meine van der Meulen
4.3.3.5	Rail	Poland	Janusz Gorski
4.3.3.6	Rail	The UK	Robin Bloomfield
4.4.1	Nuclear	International	Ian Smith
4.4.2	Nuclear	European	Ian Smith
4.4.3.1	Nuclear	Finland	Jouko Järvi
4.4.3.2	Nuclear	Germany	Ferdinand Dafelmair
4.4.3.3	Nuclear	The UK	Ian Smith
4.4.3.4	Nuclear	The USA	Ian Smith
4.5.1	Process Ind.	International	Gerd Rabe
4.5.2	Process Ind.	European	Gerd Rabe
4.5.3.1	Process Ind.	Germany	Gerd Rabe
4.6.1	Electric Power	International	Zdzislaw Zurakowski
4.6.2	Electric Power	European	Zdzislaw Zurakowski
4.6.3.1	Electric Power	Poland	Zdzislaw Zurakowski
4.7.1	Security	International	Peter Daniel+Stefan Wittmann
4.7.2	Security	European	Peter Daniel+Stefan Wittmann
4.7.3.1	Security	Germany	Stefan Wittmann
4.7.3.2	Security	The UK	Peter Daniel
5		Conclusions	Ian Smith
6		Appendices	Ian Smith